Algebra I – Commutative Algebra

Lecturer:
Dr. Andreas Mihatsch

Notes by:
Tien Nguyen Thanh

Summer term 2023

Last updated: 9th September 2023

Disclaimer: These are my *personal* notes from the lecture. As I revise my notes based on books, tutorials at university and the internet, my notes may not reflect the exact content of this course taught by the lecturer. All errors and deficiencies in these notes are certainly due to me.

Contents

Usage notes As these notes will be officially made public by the lecturer, I reckon that it might be a good idea to explain some things.

- These are my *personal* notes. The only reader I have in mind is my future self. You might find these notes at multiple times too verbose.

  Nevertheless, I appreciate any feedback about the lecture notes. You can either write me an e-mail at `tien.nguyen@uni-bonn.de` or a chat message on WhatsApp if you have my number.

- These notes should contain all content from the lecture and in the official lecture notes (definitions, propositions, theorems, corollaries, lemmas, examples, and many remarks, although not often declared as such by the lecturer), and maybe a bit more. Many proofs are a lot more detailed. Some proof steps are entirely different compared to the lecture, but hopefully equivalent and more understandable.

- Every now and then, the lecturer gives exercises for the interested, which will be stated as such and might be solved by me. Missing proofs and new remarks I do start with '(From me.)'. But watch out, not everything I add is marked that way.

- There are solutions to many exercises from the weekly exercise sheets. These are not my priority, and please take them with a grain of salt: Some exercises have complete and revised solutions, but more often then not, they are incomplete scratches I take during the tutorials. You will see whether a solution is a readable one if it is listed in Table -1.1. Note that the lecturer did not check the solutions.

- You find date stamps on the right margin. Reading up to '**Peer-reviewed**' in bold is save to do – this part was reviewed by the lecturer. Reading up to '**Reviewed**' is also okay – this part was revised by me. After that, you continue at your own risk.

- There are internal and external hyperlinks in the PDF. All coloured text is clickable. Here a gallery: Observation 4.87, (i), [Sta, 000I], ✓ (the check is an exercise), Wikipedia, the section titles in the table of contents, etc.

Solved exercises Table -1.1 shows all properly formulated solutions to exercises in these notes.

Sheet	Exercise 1	Exercise 2	Exercise 3	Exercise 4
01	✓	✓	✓	✓
02	✓	✓	✓	✓
03	✓	✓	✓	✓
04	✓	✓	✓	✓
05	✓	✓	✓	✓
06	✓	✓	✓	✓
07	✓	✓	✓	✓
08	✓	✓	✓	✓
09	✓	✓	✓	✓
10	✓	✓	✓	✓
11	✓	✓	✓	✓
12	✓	✓	✓	✓

Table -1.1: Properly written solutions in these notes. Horizontal lines act purely as visual guides.

Acknowledgements Many thanks to the lecturer Andreas Mihatsch for proof-reading these notes (it goes without saying that you should look out for errors anyway), and to my tutor Kim Lukas Kiehn for providing solutions to the exercises in my weekly tutorials. Also thanks to everyone who found errata and gave me ideas for improvement, especially (in chronological order) Carolin Hartung, Lars Schmitz, Alexandros Vlachos and Thomas Karamanis.

0 Introduction

Lect. 1
03.04.23

0.1 Motivation

Galois theory considers a single polynomial in a single variable over a field. In that regard, the primitive element theorem states that every separable finite field extension L/K is simple. If we have $L = K(\alpha)$ for an element $\alpha \in L$, we know that $L = K(\alpha) \cong K[T]/(f(T))$, where $f(T) \in K[T]$ is the minimal polynomial of α over K.

Commutative algebra instead considers a system of polynomial equations in several variables with general coefficients. There are mainly two historical origins:

(i) *Algebraic geometry:* Let $T_1, \dots, T_n$ be variables, and let $f_1, \dots f_n \in \mathbb{C}[T_1, \dots, T_n]$ be polynomials. Then we can consider the ring $A = \mathbb{C}[T_1, \dots, T_n]/(f_1, \dots, f_m)$ or the solution set $X = \{t = (t_1, \dots, t_n) \in \mathbb{C}^n \mid f_1(t) = \dots = f_m(t) = 0\}$, which is a set of points in n-dimensional space.

Algebraic geometry recognises that the properties of A and X somewhat match, e. g.

- $\dim(A)$ (the *Krull dimension*) is the $\mathbb{C}$-dimension of X,
- A is regular if and only if X is non-singular, i. e. a manifold.
- The only idempotents in A are 0 and 1 if and only if X is connected.

(ii) *Algebraic number theory:* We are interested in $\mathbb{Z}[T]/(f)$ for some $f \in \mathbb{Z}[T]$. Then we see that e. g. the *Gaussian numbers* $\mathbb{Z}[\mathrm{i}]$ or the *Eisenstein numbers* $\mathbb{Z}[\zeta_3]$ reflect certain classical number-theoretic properties.

This lecture on commutative algebra focuses on commutative rings and modules over them as well as some examples in algebraic geometry and algebraic number theory. Examples for commutative rings include the ring of functions over $\mathbb{C}$ in algebraic geometry, or the ring of algebraic integers over $\mathbb{Q}$ in algebraic number theory. Possible continuations of this lecture are algebraic geometry, algebraic number theory and algebra II. The prerequisite for this course is the course *introduction to algebra*, for example [Sch].

These notes deviate from the intended content structure as envisioned by the lecturer:

(i) Chapter 1, *Rings*, containing everything from ch. 1 and 2.
(ii) Chapter 2, *Modules*, containing everything from ch. 3 and 4.
(iii) Chapter 3, *Geometry and Algebra*, containing everything from ch. 5 and 6.
(iv) Chapter 4, *Number Theory and Algebra*, containing everything from ch. 7.

0.2 References

The main reference for (at least the first half of) this lecture is the following:

[AtMac] Atiyah, Michael F.; MacDonald, Ian G.: *Introduction to commutative algebra.* CRC Press 2018.

Other literature include (in descending importance):

[Sch] Schröer, Jan: *Einführung in die Algebra.* Lecture notes, winter term 22/23. In German. To be found on eCampus.

[Sta] de Jong, Aise J.: *The Stacks project.* Online at https://stacks.math.columbia.edu/.

[Mat] Matsumura, Hideyuki: *Commutative Algebra.* Benjamin 1980, 2nd ed. For a digital version, see: TEXromancers (ed.), 2022: https://aareyanmanzoor.github.io/assets/matsumura-CA.pdf.

[Bos] Bosch, Siegfried: *Algebra.* Springer 2023, 10th ed. In German.

[Cox] Cox, David A.: *Primes of the Form $x^2 + ny^2$.* Wiley 2013.

[LMF] The LMFDB Collaboration: *The L-functions and modular forms database (LMFDB).* Online at https://www.lmfdb.org/.

[Sut] Sutherland, Andrew: *18.785 Number theory I, Lecture #6.* Lecture notes, fall 2015. Online at https://math.mit.edu/classes/18.785/2015fa/LectureNotes6.pdf.

[Mum] Mumford, David: *The Red Book of Varieties and Schemes.* Springer 1999, 2nd ed.

[Leb] Lebruyn, Lieven: *Muford's treasure map.* Online at http://www.neverendingbooks.org/mumfords-treasure-map.

1 Rings and Ideals

This following few subsections will follow [AtMac, ch. 1].

1.1 Rings and Ideals

Definition 1.1. A **ring** A is a set with two binary operations **addition** and **multiplication** $+\colon A \times A \to A$ and $\cdot\colon A \times A \to A$, resp., for which the following hold:

(i) $(A, +)$ is an abelian group.

(ii) Multiplication is associative and distributive over addition (left and right distributive).

Sometimes, a ring A has an **identity element** $1 \in A$ satisfying $x1 = 1x = x$ for all $x \in A$.
We call a ring A **commutative**, if multiplication is commutative.
In this course, a **ring** will always denote a commutative ring with 1.

Definition 1.2. Let A be a ring.

(i) A subset $\mathfrak{a} \subseteq A$ is an **ideal** in A if it is an abelian additive subgroup of A, such that $ax \in \mathfrak{a}$ for all $x \in \mathfrak{a}$ and $a \in A$.

(ii) Let $S \subseteq A$ be a subset. Then the **ideal generated by** S is defined as

$$(S) \coloneqq \bigcap_{\substack{S \subseteq \mathfrak{a} \subseteq A \\ \mathfrak{a} \text{ is ideal}}} \mathfrak{a},$$

which is the smallest ideal containing S.

Note that we are in a commutative ring, so there is no distinction between left- and right-ideals.

Lemma 1.3. *Let A be a ring, and let $S \subseteq A$ be a subset. Then we have*

$$(S) = \sum_{s \in S} As = \left\{ \sum_{s \in S} a_s s \;\middle|\; a_s \in A, a_s \neq 0 \text{ for finitely many} \right\}.$$

Proof. Let $\mathfrak{b}$ be the right hand side. Let $\sum_{s\in S} a_s s, \sum_{s\in S} b_s s \in \mathfrak{b}$, where only finitely many a_s and b_s are not 0. It follows that

$$-\sum_{s\in S} a_s s = \sum_{s\in S}(-a_s)s \in \mathfrak{b} \qquad \text{and} \qquad \sum_{s\in S} a_s s + \sum_{s\in S} b_s s = \sum_{s\in S}(a_s + b_s)s \in \mathfrak{b}.$$

Note that there are only finitely many non-zero $-a_s$ and $a_s + b_s$. Thus $\mathfrak{b}$ is an abelian additive subgroup. We also have

$$a\sum_{s\in S} a_s s = \sum_{s\in S}(aa_s)s \in \mathfrak{b} \qquad \text{for all } a \in A.$$

Again, note that there are only finitely many aa_s not equal 0. Thus $\mathfrak{b}$ is an ideal. Since $1s \in \mathfrak{b}$ for all $s \in S$, it follows that $S \subseteq \mathfrak{b}$ and hence by definition $(S) \subseteq \mathfrak{b}$.

Conversely, let $\mathfrak{a} \subseteq A$ be an ideal such that $S \subseteq \mathfrak{a}$. From the properties of ideals, we get $as \in \mathfrak{a}$ for all $s \in S$ and $a \in A$ and thus $\sum_{s\in S} a_s s \in \mathfrak{a}$ for all finite sums. Therefore $\mathfrak{b} \subseteq \mathfrak{a}$ and finally $\mathfrak{b} \subseteq (S)$. □

How can we construct rings?

(i) We already know some rings, e. g. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, etc.

(ii) Given a ring A, we can form *polynomial rings*.

(iii) Given a ring A and an ideal $\mathfrak{a} \subseteq A$, we can form *quotient rings*.

Definition 1.4. Given any ring A, we can construct **polynomial rings** $A[T]$ over A in a single variable T (which is just a symbol):

$$A[T] \coloneqq \bigoplus_{i=0}^{\infty} AT^i = \left\{ \sum_{i=0}^{n} a_i T^i \;\middle|\; n \geq 0, a_i \in A, a_n \neq 0 \right\}.$$

Remark 1.5. By definition, two polynomials $\sum_{i=0}^{n} a_i T^i$ and $\sum_{i=0}^{m} b_i T^i$ in $A[T]$ are equal (assuming $a_n, b_m \neq 0$) if and only if $n = m$ as well as $a_i = b_i$ for all $i = 0, \ldots, n$.

Definition 1.6. Given a ring A, we can construct a **polynomial ring** over A in several variables $T_1, \ldots, T_n$ by

$$A[T_1, \ldots, T_n] \coloneqq A[T_1, \ldots, T_{n-1}][T_n]$$

inductively. Similarly, if I is any index set, we can form a **polynomial ring** over A in a family of variables $(T_i)_{i \in I}$ by

$$A[T_i, i \in I] \coloneqq \bigcup_{\text{finite } J \subseteq I} A[T_j, j \in J].$$

Definition 1.7. Given a ring A and an ideal $\mathfrak{a} \subseteq A$, the additive abelian quotient group $A/\mathfrak{a}$ endowed with the multiplication

$$(a + \mathfrak{a})(b + \mathfrak{a}) \coloneqq ab + \mathfrak{a} \qquad \text{for all } a, b \in A$$

forms a ring which we call a **quotient (ring)** of A.

Proof. We have to check that this multiplication is well-defined. For all $x, y \in \mathfrak{a}$, we have

$$(a + x + \mathfrak{a})(b + y + \mathfrak{a}) = ab + ay + bx + xy + \mathfrak{a} = ab + \mathfrak{a}$$

since $ay + bx + xy \in \mathfrak{a}$ due to the ideal properties.

All other ring axioms follow directly from those of A. □

Notation 1.8. Let A be a ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let $a, b \in A$. Then we write $a \equiv b \mod \mathfrak{a}$ if $a - b \in \mathfrak{a}$, or equivalently, $a + \mathfrak{a} = b + \mathfrak{a}$. We also write $\bar{a} \in A/\mathfrak{a}$ for the residue class $a + \mathfrak{a}$.

Definition 1.9. Let A and B be rings. We call a map $\varphi \colon A \to B$ a **ring homomorphism** if the following hold:

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in A$.

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in A$.

(iii) $\varphi(1) = 1$.

From now on, we will call ring homomorphisms simply **ring maps**.

Some important properties which are known from the introductory course to algebra.

Theorem 1.10 (**homomorphism theorem for rings**, [Sch, Thm. 5.8])**.** *Let $\varphi \colon A \to B$ be a ring map. Then $\varphi(A)$ is a subring of B and $\ker(\varphi)$ is an ideal of A. Furthermore, we have*

$$A/\ker(\varphi) \xrightarrow{\sim} \varphi(A)$$

Definition 1.11. Especially in the context of category theory, assume that a morphism $f \colon A \to C$ can be written as $f = h \circ g$ with morphism $g \colon A \to B$ and $h \colon B \to C$. Then we will say that f **factors through** any of g, h or B.

Theorem 1.12 (**universal property of polynomial rings**, [Sch, Thm. 5.23])**.** *Let $\varphi\colon A \to B$ be a ring map, and let I be an index set. Then for every map $I \mapsto B$, $i \mapsto b_i$, there is a unique ring map $\psi_{(b_i)}\colon A[T_i, i \in I] \to B$, such that $\psi_{(b_i)}\colon T_i \mapsto b_i$, and such that*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & \nearrow_{\exists!\psi_{(b_i)}} & \\ A[T_i, i \in I] & & \end{array}$$

*commutes, i. e. $\psi_{(b_i)}(a) = \varphi(a)$ for all $a \in A$. We also call $\psi_{(b_i)}$ the **evaluation** of T_i at b_i. Furthermore, there is a bijection between all ψ satisfying the above and $\operatorname{map}(I, B)$ via*

$$\begin{aligned} \psi &\mapsto (i \mapsto \psi(T_i)), \\ (\psi\colon T_i \mapsto b_i) &\leftarrow\!\shortmid (i \mapsto b_i). \end{aligned}$$

Theorem 1.13 (**universal property of quotient rings**, [Sch, Thm. 5.7])**.** *Let $\varphi\colon A \to B$ be a ring map, and let $\mathfrak{a} \subseteq \ker(\varphi)$ be an ideal in A. Then there exists the following unique factorisation of φ:*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & \nearrow_{\exists!} & \\ A/\mathfrak{a} & & \end{array}$$

1.2 Examples of Rings

Example 1.14. Let k be a field, $k[T]$ a polynomial ring and $f = \sum_{i=0}^{n} a_i T^i \in k[T]$ with $a_n \neq 0$. Consider $A = k[T]/(f)$. Then for all $m \geq n$, we have

$$\begin{aligned} T^m &= a_n^{-1} T^{m-n} f - a_n^{-1} \sum_{i=0}^{n-1} a_i T^{m-n+i} \\ \implies T^m &\equiv -a_n^{-1}(a_{n-1}T^{m-1} + a_{n-2}T^{m-2} + \cdots + a_0 T^{m-n}) \mod (f). \end{aligned}$$

This means any residue class of A has a representative $g + (f)$ with $\deg(g) < n$, for we can apply the above iteratively to eliminate the term of highest degree at least n.

Set $t \coloneqq \bar{T} = T + (f)$. The above shows that $1, t, t^2, \ldots, t^{n-1}$ is a k-basis of A. Hence for all $0 \leq i \leq n$,

$$t \cdot t^i = \begin{cases} t^{i+1}, & \text{if } i < n-1, \\ -a_n^{-1}(a_{n-1}t^{n-1} + \cdots + a_1 t + a_0), & \text{if } i = n-1. \end{cases}$$

This multiplication law inductively defines the multiplication of two elements in A completely.

More generally, let A be a ring, and let $f = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in A[T]$ with a_n invertible. Consider $A[T]/(f)$, and set $t \coloneqq T + (f) \in A[T]/(f)$. Then

$$A[T]/(f) \cong \bigoplus_{i=0}^{n-1} A t^i$$

as abelian groups endowed with the same multiplication as before.

Exercise 1.15. Show that this 'minimal' representative g is unique.

Solution. By way of contradiction, suppose that we have $g + (f) = g' + (f)$ with $g \neq g'$ and $\deg(g), \deg(g') < n$. But this implies $f \mid (g - g')$, and hence $n = \deg(f) < \deg(g - g') \leq n - 1$.

Example 1.16. Consider $A \coloneqq \mathbb{Z}[X, Y]/(XY)$. Note that $(XY) = \mathbb{Z}[X, Y] \cdot XY$ is the set of all multiples of XY over $\mathbb{Z}[X, Y]$. We see that every $f \in \mathbb{Z}[X, Y]$ is of the form

$$f = c + \sum_{i=1}^{n} a_i X^i + \sum_{j=1}^{m} b_j Y^j + g \cdot XY$$

with unique $c, a_i, b_j \in \mathbb{Z}$ and $g \in \mathbb{Z}[X,Y]$. Then every residue class in A has a unique representative of the form $c + \sum_{i=1}^{n} a_i X^i + \sum_{j=1}^{m} b_j Y^j$. Let us set $x \coloneqq X + (XY)$ and $y \coloneqq Y + (XY)$. We conclude that

$$A \cong \mathbb{Z} \oplus \bigoplus_{i=1}^{\infty} (\mathbb{Z}x^i \oplus \mathbb{Z}y^i)$$

as abelian groups with multiplication defined by $x^i x^j = x^{i+j}$ and $y^i y^j = y^{i+j}$, but $xy = 0$.

1.3 Basic Properties

Definition 1.17. Let A be a ring.

(i) $x \in A$ is **nilpotent** if $x^n = 0$ for some $n > 0$. A is **reduced** if 0 is the only nilpotent element.

(ii) $x \in A$ is a **zero divisor** if there exists some $0 \neq y \in A$ such that $xy = 0$, otherwise x is **regular**. A is an **integral domain** or just **domain** if $A \neq 0$ and if 0 is the only zero divisor.

(iii) $x \in A$ is a **unit** if there is some $y \in A$ such that $xy = 1$. We denote the set of all units in A by $A^\times$, which forms a multiplicative group.

Remark 1.18. Consider the map $\varphi\colon A \to A$, $a \mapsto xa$ for a given $x \in A$.

(i) φ is injective if and only if x is regular.

Proof: φ is injective as an abelian group map if and only if $\ker(\varphi) = 0$, meaning if $xy = 0$ for some $y \in A$, then $y = 0$. This is the definition of x being regular.

(ii) φ is bijective if and only if φ is surjective if and only if $x \in A^\times$.

Proof: φ being bijective implies φ being surjective. If φ is surjective, then there exists some $a \in A$ with $\varphi(a) = xa = 1$, hence $x \in A^\times$. If $x \in A^\times$, then there exists some $y \in A$ such that $xy = yx = 1$. Hence the inverse map $\varphi^{-1}\colon A \to A$, $a \mapsto ya$ exists, implying that φ is bijective.

Notice that $\mathrm{im}(\varphi) = Ax = (x)$ is the ideal generated by x.

Example 1.19. Let $n \in \mathbb{Z}$ and consider $A \coloneqq \mathbb{Z}[T]/(T^2 - n)$, i. e. we adjoin $\mathbb{Z}$ by the square root of n. Set $t \coloneqq T + (T^2 - n)$, so $t^2 = n$.

(i) If $n = 0$, then $t^2 = 0$ in A. Thus $t \neq 0$ is nilpotent, and A is neither reduced nor an integral domain.

(ii) If $n = m^2$ is a square for $m > 0$, then $(m - t)(m + t) = m^2 - t^2 = n - n = 0$. Both factors are not 0 since $m \in \mathbb{Z}$, but $t \notin \mathbb{Z}$. Thus A is not an integral domain.

(iii) If n is not a square, then $A \cong \mathbb{Z}[\sqrt{n}]$ given by $t \mapsto \sqrt{n}$. So we find an embedding $A \hookrightarrow \mathbb{Q}(\sqrt{n})$ into a field, and A is in particular an integral domain.

Exercise 1.20. Show that if $n \in \mathbb{Z} \setminus \{0\}$, then $A = \mathbb{Z}[T]/(T^2 - n)$ is reduced.

Solution. If $n \neq 0$, we have $A \cong \mathbb{Z} \oplus \mathbb{Z}t$ as an abelian group. Let $a + bt \in A$, and assume that $(a + bt)^k = 0$ for some odd $k > 0$. Expanding yields $0 = aa' + bb't$ for some $a', b' \in \mathbb{Z}$, where each summand in a' or b' is a product of squares and positive integers (more precisely, binomial coefficients). Since $a', b' \geq 0$ and necessarily $aa' = bb' = 0$, we have $a = b = 0$, and hence A is reduced.

Proposition 1.21. *Let A be a reduced ring (resp. an integral domain). Then $A[T_i, i \in I]$ is so as well for any index set I.*

Proof. Let $B \coloneqq A[T_i, i \in I]$. First we assume that $I = \{1, \ldots, n\}$ is finite. Because of $A[T_1, \ldots, T_n] \cong A[T_1, \ldots, T_{n-1}][T_n]$, we can proceed inductively. It suffices to show the inductive step assuming $B = A[T]$.

Let $f = a_n T^n + \cdots + a_0$ and $g = b_m T^m + \cdots + b_0$ be in B with $a_n, b_m \neq 0$. Then $fg = a_n b_m T^{n+m} + \cdots$ and $f^r = a_n^r T^{nr} + \cdots$ for any $r \geq 0$. A being reduced (resp. an integral domain) implies $a_n^r \neq 0$ (resp. $a_n b_m \neq 0$). Thus $f^r \neq 0$ (resp. $fg \neq 0$), and B is reduced (resp. an integral domain.)

Now to the general case. Given any $f, g \in B$, there exists a finite $J \subseteq I$ such that $f, g \in A[T_j, j \in J]$. It follows that $fg, f^r \in A[T_j, j \in J]$ for any $r \geq 0$. Now we proceed similarly as in the finite case and show that $fg \neq 0$ (resp. $f^r \neq 0$ for any $r \geq 0$) in $A[T_j, j \in J]$. By the inclusion $A[T_j, j \in J] \hookrightarrow B$, this also holds in B. □

Definition 1.22. Let A be a ring. We define $\operatorname{nil}(A)$ to be the set of all nilpotent elements in A, called the **nilradical** of A.

Proposition 1.23. *Let A be a ring. Then we have the following:*

(i) $\operatorname{nil}(A)$ *is an ideal.*

(ii) $\bar{A} \coloneqq A/\operatorname{nil}(A)$ *is reduced.*

(iii) ***Universal property of nilradicals**: For any reduced ring B, any ring map $\varphi\colon A \to B$ factorises through $\bar{A}$.*

Proof.

(i) Let $x, y \in \operatorname{nil}(A)$, say $x^n = y^m = 0$. Then $(ax)^n = a^n x^n = 0$ for all $a \in A$. Furthermore,

$$(x+y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^{n+m-1-i} y^i = 0,$$

since we always have either $n+m-1-i \geq n$ or $i \geq m$. Finally, we have $(-x)^n = (-1)^n x^n = 0$. In the end, $-x, x+y, ax \in \operatorname{nil}(A)$ for all $x, y \in \operatorname{nil}(A)$ and $a \in A$.

(ii) Let $\bar{x} = x + \operatorname{nil}(A) \in \bar{A}$ be nilpotent, say $\bar{x}^n = 0$. This means $x^n \in \operatorname{nil}(A)$, i. e. $(x^n)^k = x^{nk} = 0$ for some $k > 0$. Thus $x \in \operatorname{nil}(A)$, hence $\bar{x} = 0$.

(iii) Let B be reduced, and let $\varphi\colon A \to B$ be a ring map. If $x^n = 0$ for $x \in \operatorname{nil}(A)$, then $\varphi(x)^n = \varphi(x^n) = 0$, so $\varphi(x) = 0$ since B is reduced. In other words, $\operatorname{nil}(A) \subseteq \ker(\varphi)$, hence φ factors through $\bar{A}$ according to the universal property of quotients. □

Exercise 1.24. Compute units and the nilradical of the rings $\mathbb{Z}/(n)$ and $\mathbb{C}[\varepsilon]/(\varepsilon^2)[T]$.

1.4 Fields

Lect. 2
06.04.23

Lemma 1.25. *Let A be a ring.*

(i) *Let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a} = A$ if and only if $1 \in \mathfrak{a}$ if and only if $\mathfrak{a}$ contains a unit.*

(ii) *Given $x \in A$, we have $(x) = A$ if and only if $x \in A^\times$.*

Proof.

(i) The only if directions are trivial: If $\mathfrak{a} = A$, then obviously $1 \in \mathfrak{a}$. If $1 \in \mathfrak{a}$, then there is obviously a unit in $\mathfrak{a}$, namely 1.

For the last implication, let $u \in \mathfrak{a}$ be a unit, and let $a \in A$ be arbitrary. By the ideal property, it follows that $a = au^{-1} \cdot u \in \mathfrak{a}$ since $u \in \mathfrak{a}$ and $au^{-1} \in A$. Hence $\mathfrak{a} = A$.

(ii) According to what we just proved, $(x) = A$ if and only if $1 \in (x)$ if and only if $1 = xy$ for some $y \in A$ if and only if $x \in A^\times$. □

Definition 1.26. A ring A is a **field** if $A \neq 0$ and $A^\times = A \setminus \{0\}$.

Lemma 1.27. *Let $A \neq 0$ be a ring. Then A is a field if and only if the only ideals in A are (0) and A.*

Proof. Assume that A is a field, and that $(0) \neq \mathfrak{a} \subseteq A$ is an ideal. Then we pick any $0 \neq x \in \mathfrak{a}$, which is a unit because A is a field. Thus by Lemma 1.25, $A = (x) \subseteq \mathfrak{a}$ and hence $\mathfrak{a} = A$.

Conversely, let $0 \neq x \in A$. By the premise, we have $(x) = A$, and Lemma 1.25 yields $x \in A^\times$. Hence A is a field. □

Definition 1.28. Let A be a ring. An ideal $\mathfrak{m} \subseteq A$ is **maximal**, if $\mathfrak{m} \neq A$ and if there is no ideal $\mathfrak{a} \subseteq A$ with $\mathfrak{m} \subset \mathfrak{a} \subset A$.

Corollary 1.29. *Let A be a ring. An ideal $\mathfrak{m} \subseteq A$ is maximal if and only if $A/\mathfrak{m}$ is a field.*

Proof. We know the following fact from [Sch, Cor. 5.10]: Let $\mathfrak{a} \subseteq A$ be any ideal and $\pi\colon A \to A/\mathfrak{a}$ the canonical projection. Then there is a bijection

$$\{\text{ideals } \bar{\mathfrak{b}} \subseteq A/\mathfrak{a}\} \cong \{\text{ideals } \mathfrak{a} \subseteq \mathfrak{b} \subseteq A\}, \qquad \bar{\mathfrak{b}} \mapsto \pi^{-1}(\bar{\mathfrak{b}}), \qquad \pi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a} \hookleftarrow \mathfrak{b}.$$

Using this fact, we make the following observations: Firstly, $\mathfrak{m} \neq A$ if and only if $A/\mathfrak{m} \neq (0)$. Secondly, for all $\mathfrak{m} \neq A$, there exists no ideal $\mathfrak{m} \subset \mathfrak{a} \subset A$ if and only if there exists no ideal $(0) \subset \bar{\mathfrak{a}} \subset A/\mathfrak{m}$, i. e. (0) and $A/\mathfrak{m}$ are the only ideals of $A/\mathfrak{m}$. By Lemma 1.27, this is equivalent to $A/\mathfrak{m}$ being a field. □

1.5 Principal ideal domains

Definition 1.30. A **principal ideal domain** (PID) is an integral domain A such that every ideal $\mathfrak{a} \subset A$ is **principal**, i. e. of the form $\mathfrak{a} = (f)$ for some $f \in A$.

Example 1.31. $\mathbb{Z}$ and $k[T]$ for any field k are prototypical principal ideal domains.

Example 1.32. $A = \mathbb{C}[\varepsilon]/(\varepsilon^2)$ is not an integral domain, but every ideal is principal, namely $(0), (\bar{\varepsilon}), (\bar{1}) = A$ are the only ideals in A.

To proof that, we can use the correspondence of ideals in the proof of Corollary 1.29. There is a bijection between ideals in A and ideals $(\varepsilon^2) \subseteq \mathfrak{a} \subseteq \mathbb{C}[\varepsilon]$. Since $\mathbb{C}[\varepsilon]$ is a principal ideal domain, the latter set of ideals is $\{(f) \mid f \mid \varepsilon^2\} = \{(1), (\varepsilon), (\varepsilon^2)\}$. After projecting, we obtain the claimed ideals of A.

Alternative: We show that $A^\times = \{a + b\bar{\varepsilon} \in A \mid a \in \mathbb{C}^\times\}$. Let $a + b\bar{\varepsilon} \in A$ with $a \in \mathbb{C}^\times$. Then $a^{-2}(a + b\bar{\varepsilon})(a - b\bar{\varepsilon}) = 1$, so $a + b\bar{\varepsilon} \in A^\times$. Conversely, let $a + b\bar{\varepsilon} \in A^\times$, i. e.

$$1 = (a + b\bar{\varepsilon})(c + d\bar{\varepsilon}) = ac + (ad + bc)\bar{\varepsilon}$$

for some $c + d\bar{\varepsilon} \in A$. This implies $ac = 1$ and $ad + bc = 0$, and in particular, $a \in \mathbb{C}^\times$.

Now we consider some ideal $(0) \neq \mathfrak{a} \subseteq A$. If there exists some $0 \neq a + b\bar{\varepsilon} \in \mathfrak{a}$ with $a \in \mathbb{C}^\times$, then $a + b\bar{\varepsilon} \in A^\times$ and by Lemma 1.25, $\mathfrak{a} = A$. Otherwise, $\mathfrak{a} = \{b\bar{\varepsilon} \mid b \in \mathbb{C}\} = (\bar{\varepsilon})$.

Definition 1.33. A ring is a **principal ideal ring**, if every ideal in it is principal.

In contrast to principal ideal domains, A might have non-zero zero divisors.

Lemma 1.34. *Let A be an integral domain, and let $f, g \in A$. Then $(f) = (g)$ if and only if there exists some $u \in A^\times$ such that $g = uf$.*

Proof. If $g = uf$, then $(g) \subseteq (f)$. Because of $u \in A^\times$, we also have $f = u^{-1}g$, so $(f) \subseteq (g)$.

Conversely, if $(f) = (g)$, we have $f \in (g)$ and $g \in (f)$, i. e. we can write $f = ug$ and $g = vf$ for certain $u, v \in A$. We obtain $f = uvf$, or equivalently $f(1 - uv) = 0$. Since A is an integral domain, $f = 0$ or $uv = 1$.

In the first case $f = 0$, we must have $g = 0$ too, so $g = 1f$ satisfies the assertion. In the second case $uv = 1$, we have $u \in A^\times$ and the assertion is again satisfied. □

Corollary 1.35. *If A is a principal ideal domain, then there is a bijection between ideals in A and the multiplicative group $A/A^\times$, given by $(f) \hookleftarrow f$.*

Example 1.36. In $\mathbb{Z}$, all ideals are exactly $n\mathbb{Z}$ for all $n \geq 0$. In $k[T]$, all ideals are exactly (f) with monic $f \in k[T]$.

Definition 1.37. Let A be an integral domain. Then $p \in A$ is **prime** if $0 \neq p \notin A^\times$, and $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Theorem 1.38. *Let A be a principal ideal domain, but not a field, and let $0 \neq f \in A$. Then there exist $u \in A^\times$, $p_1, \dots, p_r \in A$ prime and $e_1, \dots, e_r \geq 1$ such that*

$$f = u p_1^{e_1} \cdots p_r^{e_r},$$

*which we call a **prime factorisation** of f. Furthermore, we may assume that $p_i \nmid p_j$ for all $i \neq j$. Then (p_i, e_i) are unique up to reordering and up to units, i. e. $p_i \mapsto u_i p_i$ with $u_i \in A^\times$ for all $1 \leq i \leq r$.*

We will prove this theorem in a number of steps, and we will need the following auxiliary statement. Nevertheless, the results on this endeavour are quite interesting in themselves. Besides, we will demonstrate a common technique in commutative algebra: Constructing an ascending chain of ideals.

Lemma 1.39. *Let A be an integral domain, and let $p, q \in A$ be prime. Then $p \mid q$ implies $q \mid p$, i. e. $q = up$ for some $u \in A^\times$.*

Proof. $p \mid q$ implies $q = xp$ for some $x \in A$. The prime property gives $q \mid x$ or $q \mid p$. We now show that $q \mid x$ is impossible.

By way of contradiction, suppose that $x = qy$ for some $y \in A$. Thus $q = qyp$, hence $(1 - yp)q = 0$. Since A is an integral domain and $q \neq 0$, we necessarily have $1 = yp$. But this contradicts $p \notin A^\times$ for prime elements.

Thus $q \mid p$. In particular, $(p) = (q)$. Now, $q = up$ for some $u \in A^\times$ follows from Lemma 1.34. □

Now to the actual proof.

Proof. We will prove a series of claims.

(i) If $f \in A^\times$, then $f = f$ is the 'unique' prime factorisation.

Assume that $p \mid f$ for some $p \in A$. Then $p \mid f f^{-1} = 1$, so $p \in A^\times$ and p cannot be prime. Thus the only factors of f are units, and $f = f$ is a unique prime factorisation.

So from now on, we may assume $f \notin A^\times$.

(ii) For each $f \notin A^\times$, there exists a maximal ideal $\mathfrak{m} \subset A$ with $f \in \mathfrak{m}$.

We define the following chain of ideals: Set $\mathfrak{a}_0 := (f)$. For each $i \geq 0$, if $\mathfrak{a}_i \subset A$ is not maximal, we choose some ideal $\mathfrak{a}_{i+1}$ such that $\mathfrak{a}_i \subset \mathfrak{a}_{i+1} \subset A$. Otherwise we set $\mathfrak{a}_{i+1} := \mathfrak{a}_i$. We obtain the ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$.

The union $\mathfrak{b} := \bigcup_{i \geq 0} \mathfrak{a}_i$ is again an ideal. (For all $f, g \in \mathfrak{b}$, there is some i with $f, g \in \mathfrak{a}_i$. Now, all ideal properties hold in $\mathfrak{a}_i$.) As A is a principal ideal domain, we can write $\mathfrak{b} = (g)$ for some $g \in \mathfrak{b}$. Then we must have $g \in \mathfrak{a}_i$ for some i, giving $(g) \subseteq \mathfrak{a}_i \subseteq \mathfrak{b} = (g)$. So this chain stabilises at $\mathfrak{a}_i = \mathfrak{a}_{i+1} = \cdots$ and $\mathfrak{a}_i$ must be maximal.

(iii) Let $(0) \neq \mathfrak{m} = (p)$ be an ideal in A (recall that A is not a field and Lemma 1.27). Then $\mathfrak{m}$ is maximal if and only if p is prime. (We actually only need the 'only if' direction.)

Let $(0) \subset \mathfrak{m} \subset A$ be maximal, thus $0 \neq p \notin A^\times$ due to Lemma 1.25. Assume that $p \mid ab$, i. e. $ab \in \mathfrak{m}$. This implies $\bar{a} \cdot \bar{b} = 0$ in $A/\mathfrak{m}$, which is a field by Corollary 1.29. Thus we have $\bar{a} = 0$ or $\bar{b} = 0$, hence $a \in \mathfrak{m}$ or $b \in \mathfrak{m}$. This means $p \mid a$ or $p \mid b$, and hence p is prime.

Conversely, let p be prime. As $p \notin A^\times$, by (ii), there exists some maximal ideal $\mathfrak{n} \subset A$ such that $(p) \subseteq \mathfrak{n}$. We want to show that $\mathfrak{m} = (p) = \mathfrak{n}$.

Since A is a principal ideal domain, we can write $\mathfrak{n} = (q)$ for some $q \in A$. This implies $q \mid p$ According to the 'if' direction we just showed, q is prime. Thus by Lemma 1.39, we also have $p \mid q$ and hence $\mathfrak{m} = (p) = (q) = \mathfrak{n}$.

(iv) Any $0 \neq f \in A \setminus A^\times$ has a prime factorisation as asserted.

We define the following sequence inductively: Set $f_0 := f$. For $i \geq 0$, we set $f_{i+1} := f_i$ if $f_i \in A^\times$, and $f_{i+1} := f_i / p_i$ otherwise, where $(p_i) \subset A$ is a maximal ideal with $f_i \in (p_i)$ (notice that in this case, $p_i \mid f_i$ and thus $f_i / p_i \in A$). We obtain the ascending chain $(f_0) \subseteq (f_1) \subseteq \cdots$. By the exact same argument as in (ii), this chain becomes stationary at some point, say $(f_{n-1}) \subset (f_n) = (f_{n+1}) = \cdots$.

By (iii), the p_i are all prime. Furthermore, we have $f_n \in A^\times$: Otherwise by Lemma 1.34, we would have $f_n/p_n = f_{n+1} = f_n u$ for some $u \in A^\times$. This implies $f_n(1 - p_n u) = 0$. As A is an integral domain and $f_n \neq 0$, we would obtain $p_n u = 1$ and thus $p_n \in A^\times$, contradicting p_n being prime.

This yields $f = f_n p_0 \cdots p_{n-1}$ by construction (we continuously factor out prime elements from $f_0 = f$). Using Lemma 1.39, we can collect the p_is w. r. t. to the equivalence relation $p_i \sim p_j$ if $p_i = u p_j$ for some $u \in A^\times$. This finally yields the prime factorisation $f = u'(p_1')^{e_1} \cdots (p_r')^{e_r}$ with $u' \in A^\times$ and $p_i' \nmid p_j'$ for all $i \neq j$.

(v) The prime factorisation as claimed in the theorem is unique.

Assume that $u p_1^{e_1} \cdots p_r^{e_r} = v q_1^{f_1} \cdots q_s^{f_s}$ are two prime factorisations as claimed in the theorem. As p_1 is prime, by the prime property, $p_1 \mid q_j$ for some $1 \leq j \leq s$ ($p_1 \mid v$ is impossible since $p_1 \notin A^\times$). Then Lemma 1.39 implies $q_j = w p_1$ for some $w \in A^\times$. As A is an integral domain and $p_1 \neq 0$, we may divide this equation by p_1 and obtain

$$u p_1^{e_1 - 1} p_2^{e_2} \cdots p_r^{e_r} = v' q_1^{f_1} \cdots q_j^{f_j - 1} \cdots q_s^{f_s} \qquad \text{with} \qquad v' \coloneqq vw \in A^\times.$$

By induction over $\sum_{i=1}^r e_i$, we may assume that $u = v q_1^{f_1} \cdots q_s^{f_s}$. Thus all factors on the right hand side must be units and no prime can exist, i. e. $s = 0$.

We conclude that in our initial assumption, $\sum_{i=1}^r e_i = \sum_{j=1}^s f_j$. More precisely, we have $e_i = f_j$ for corresponding prime elements p_i and q_j, as we cancel prime elements one by one. Notice that in the induction step, if $p_1 \mid q_j$, then $p_i \nmid q_j$ for all $i \neq 1$. Otherwise we would have $w p_1 = q_j = w' p_i$ with $w, w' \in A^\times$ for some i and hence $p_1 \mid p_i$, contradicting the premise. □

Corollary 1.40. *Let A be a principal ideal domain, but not a field. Then there exists a bijection between the maximal ideals of A and the prime elements of A modulo $A^\times$ via $(p) \leftrightarrow p$. (That means we do not differentiate between primes which are different up to a unit.)*

In a principal ideal domain, we can obtain notions of a greatest common divisor or the least common multiple by the prime factorisation.

Definition 1.41. Let A be a ring and $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideals. Then the **sum** and the **product** of $\mathfrak{a}$ and $\mathfrak{b}$ are, resp., defined as

$$\mathfrak{a} + \mathfrak{b} \coloneqq \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} = (\mathfrak{a} \cup \mathfrak{b}) \qquad \text{and} \qquad \mathfrak{a}\mathfrak{b} \coloneqq (ab, a \in \mathfrak{a}, b \in \mathfrak{b}).$$

Corollary 1.42. *Let A be a principal ideal domain. Then we have a well-defined notion of the **greatest common divisor** $\gcd(f, g)$ and **least common multiple** $\operatorname{lcm}(f, g)$ for any $0 \neq f, g \in A$ ('greatest' in the sense that any other common divisor divides $\gcd(f, g)$, 'least' in the sense that any other common multiple is a multiple of $\operatorname{lcm}(f, g)$). Moreover, we have the following properties:*

(i) $(f)(g) = (fg)$ *(actually true in any ring A).*

(ii) $(f) + (g) = (\gcd(f, g))$.

(iii) $(f) \cap (g) = (\operatorname{lcm}(f, g))$.

Proof. (From me.) As f and g have unique prime factorisations, any common divisor and common multiple must be a product of prime elements (and units). In particular, the $\gcd(f, g)$ (resp. $\operatorname{lcm}(f, g)$) must have each prime divisor of maximal (resp. minimal) common multiplicity, and is thus unique up to units.

(i) By definition, $(f)(g) = (afbg, a, b \in A) = (afg, a \in A) = (fg)$.

(ii) Since A is a principal ideal domain, there is some $d \in A$ such that $(f) + (g) = (d)$. We have $f, g \in (d)$, so $d \mid f, g$. For every $e \in A$ with $e \mid f, g$, we have $f, g \in (e)$ and hence $(d) = (f, g) \subseteq (e)$, thus $e \mid d$. In the end, $d = \gcd(f, g)$.

(iii) Since A is a principal ideal domain, there is some $m \in A$ such that $(f) \cap (g) = (m)$. We have $m \in (f), (g)$, so $f, g \mid m$. For every $n \in A$ with $f, g \mid n$, we have $n \in (f) \cap (g)$ and hence $(n) \subseteq (f) \cap (g) = (m)$, thus $m \mid n$. In the end, $m = \operatorname{lcm}(f, g)$. □

1.6 Power series

Definition 1.43. Let A be a ring. Then we call

$$A[\![T]\!] \coloneqq \left\{ \text{infinite series } \sum_{i=0}^{\infty} a_i T^i \;\middle|\; a_i \in A \right\} \cong \prod_{i=0}^{\infty} AT^i = A^{\mathbb{Z}_{\geq 0}}$$

the **power series ring** over A. The standard multiplication law on polynomial rings also applies to $A[\![T]\!]$.

Remark 1.44. We observe that only finitely many summands contribute to a coefficient in a product (namely the ones of lower degree), so there is no need to define convergence of series.

Remark 1.45. The difference between the infinite direct sum $\bigoplus_{i=0}^{\infty} AT^i$ and the infinite product $\prod_{i=0}^{\infty} AT^i$ is that in the former, all but finitely many coefficients are required to vanish. But in the case of finite direct sums and products, both coincide.

Remark 1.46. Some properties of $A[T]$ carry over.

(i) We can define $A[\![T_1, \dots, T_{n-1}, T_n]\!] \coloneqq A[\![T_1, \dots, T_{n-1}]\!][\![T_n]\!]$.

(ii) If A is reduced (resp. an integral domain), then $A[\![T_i, i \in I]\!]$ is so as well.

The proof is completely analogous to Proposition 1.21, but this time, we have to consider the non-zero coefficients of lowest degree.

Proposition 1.47. *Let A be a ring. Then $f = \sum_{i=0}^{\infty} a_i T^i \in A[\![T]\!]^\times$ if and only if $a_0 \in A^\times$.*

Proof. We have a ring map

$$A[\![T]\!] \to A, \qquad \sum_{i=0}^{\infty} a_i T^i \mapsto a_0.$$

Indeed, this map preserves multiplication since

$$(a_0 + a_1 T + a_2 T^2 + \cdots)(b_0 + b_1 T + b_2 T^2 + \cdots) = a_0 b_0 + \cdots \mapsto a_0 b_0.$$

Since any ring map maps units to units, if $f \in A[\![T]\!]^\times$, then $a_0 \in A^\times$.

Conversely, suppose that $a_0 \in A^\times$. We want to show $f \in A[\![T]\!]^\times$, or equivalently $a_0^{-1} f \in A[\![T]\!]^\times$. So w. l. o. g. we may assume f to be of the form $f = 1 - gT$ with $g \in A[\![T]\!]$.

For all $n \geq 0$, let $h_n \coloneqq \sum_{i=0}^{n} (gT)^i \in A[\![T]\!]$. These have the following properties:

(i) $h_n \equiv h_{n+1} \mod (T^{n+1})$, or in other words, the coefficients of degree smaller $n+1$ are equal.

(ii) $h_n f = 1 - (gT)^{n+1}$, a quite known factorisation.

Now set h_∞ as the unique power series such that $h_\infty \equiv h_n \mod (T^{n+1})$ for all $n \geq 0$, or informally $h_\infty \coloneqq \lim_{n \to \infty} h_n$. We claim that $h_\infty f = 1$. For any $n \geq 0$, we can write $h_\infty = h_n + \varepsilon_n T^{n+1}$ with $\varepsilon_n \in A[\![T]\!]$ (here we used the first property). Therefore

$$h_\infty f = (h_n + \varepsilon_n T^{n+1}) f = 1 - (gT)^{n+1} + \varepsilon_n f T^{n+1} \equiv 1 \mod (T^{n+1}) \implies h_\infty f - 1 \in \bigcap_{n \geq 1} (T^n) = (0).$$

Thus $h_\infty f = 1$, and hence $f \in A[\![T]\!]^\times$. □

Example 1.48. Let us consider $\mathbb{Z}[\![T]\!]$. Then we have the following (as only finitely many summands contribute to a coefficient of a product, we could show the following by induction):

- $(1 - T)^{-1} = 1 + T + T^2 + T^3 + \cdots$.
  This holds since for $n \geq 1$, the nth coefficient of $(1 - T)(1 + T + T^2 + \cdots)$ is $T^n - TT^{n-1} = 0$.
- $(1 + T)^{-1} = 1 - T + T^2 - T^3 + \cdots$.
  This holds since for $n \geq 1$, the nth coefficient of $(1 + T)(1 - T + T^2 - \cdots)$ is $(-T)^n + T(-T)^{n-1} = 0$.

- $(1-T-T^2)^{-1} = F(T) \coloneqq 1+T+2T^2+3T^3+5T^4+\cdots$, i. e. the coefficients are the Fibonacci sequence. This follows from $F(T) = TF(T)+T^2F(T)+1$.

Exercise 1.49. Prove that $1+T \in \mathbb{Q}[\![T]\!]^\times$ has a square root.

Solution. We construct the square root $f \coloneqq \sum_{i=0}^\infty a_i T^i$ recursively as follows: Set $a_0 \coloneqq 1$ and $a_1 \coloneqq \frac{1}{2}$. Then for all $i \geq 1$, set $a_{i+1} \coloneqq -\frac{1}{2}\sum_{k=0}^i a_k a_{i-k} \in \mathbb{Q}$. The coefficients are chosen in such a way that if $f^2 = \sum_{i=0}^\infty b_i T^i$, we have $b_0 = 1$, $b_1 = \frac{1}{2}+\frac{1}{2} = 1$ and $b_{i+1} = \sum_{k=0}^i a_k a_{i-k} + 2a_0 a_{i+1} = 0$ for all $i \geq 1$. Hence $f^2 = 1+T$.

Proposition 1.50. *Let k be a field. Then the ideals of $k[\![T]\!]$ are precisely (0) and (T^n) for all $n \geq 0$. In particular, $k[\![T]\!]$ is a principal ideal domain, and there exists a unique maximal ideal, namely (T). In this case, T is up to units the only prime element.*

Proof. Let $(0) \neq \mathfrak{a} \subseteq k[\![T]\!]$ be an ideal. We pick $0 \neq f = \sum_{i=n}^\infty a_i T^i \in \mathfrak{a}$ with $a_n \neq 0$ such that n is minimal. As $a_n \in k^\times$, we can factor out T^n from f and obtain a unit in $k[\![T]\!]^\times$ by Proposition 1.47, i. e. $f = uT^n$ with $u \in k[\![T]\!]^\times$. By minimality of n, we must have $T^n \mid g$ for all $g \in \mathfrak{a}$ (g has infinitely many summands of degree at least n), hence $\mathfrak{a} = (f) = (T^n)$.

In particular, since $(0), (T^n) \subseteq (T) \neq k[\![T]\!]$ for all $n \geq 1$, (T) is maximal. From the proof of Theorem 1.38, step (iii), T is the only prime element. □

Definition 1.51. Let A be any ring. Then the **Jacobson radical** is defined as

$$\operatorname{jac}(A) \coloneqq \bigcap_{\text{maximal } \mathfrak{m} \subset A} \mathfrak{m}.$$

Example 1.52.

(i) $\operatorname{jac}(k[\![T]\!]) = (T)$ (we just proved this).

(ii) $\operatorname{jac}(\mathbb{Z}) = (0)$, as by the proof of Theorem 1.38, part (iii), the maximal ideals are (p) with primes $p \in \mathbb{Z}$ (recall that $\mathbb{Z}$ is a principal ideal domain). The only number divisible by all primes is 0.

(iii) $\operatorname{jac}(k[T]) = (0)$ (Exercise 8.3).

(iv) $\operatorname{jac}(\mathbb{C}[\varepsilon]/(\varepsilon^2)) = (\varepsilon)$ (Exercise 8.3).

1.7 Euclidean Rings

Lect. 3
13.04.23

We want to find a criterion for rings being a principal ideal domain.

Definition 1.53. A ring A is **euclidean** if A is an integral domain, and if there exists a **degree function**

$$\deg\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

such that for all $a, b \in A \setminus \{0\}$, there exist some $q, r \in A$ with $a = qb + r$ and either $r = 0$ or $\deg(r) < \deg(b)$.

Proposition 1.54. *Every euclidean ring is a principal ideal domain.*

Proof. The proof is based on the **Euclidean algorithm**. Let A be a euclidean ring w. r. t. deg and $\mathfrak{a} \subseteq A$ any ideal. If $\mathfrak{a} = (0)$, then we are done. Otherwise, pick any $0 \neq b \in \mathfrak{a}$ such that $\deg(b) = \min\{\deg(a) \mid 0 \neq a \in \mathfrak{a}\}$.

We claim that $\mathfrak{a} = (b)$. $(b) \subseteq \mathfrak{a}$ is obvious. Take an arbitrary $0 \neq a \in \mathfrak{a}$. By definition of euclidean rings, there are $q, r \in A$ such that $a = qb + r$ with either $r = 0$ or $\deg(r) < \deg(b)$. $r \neq 0$ cannot occur, as otherwise $\deg(r) < \deg(b)$ and $r = a - qb \in \mathfrak{a}$, which violates the minimality of $\deg(b)$. Thus $r = 0$ and $a = qb \in (b)$, hence $\mathfrak{a} \subseteq (b)$. □

Now we consider some specific examples from number theory. These properties are not that common among rings over $\mathbb{Z}$.

Proposition 1.55. *Let A be one of the rings $\mathbb{Z}[\mathrm{i}]$ (**Gaussian integers**), $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_6]$ (**Eisenstein integers**). (The minimal polynomial of $\frac{1}{2}(1+\sqrt{-3}) = \zeta_6$ is $T^2 - T + 1$, thus $\mathbb{Z}[\zeta_6] \cong \mathbb{Z}[T]/(T^2 - T + 1)$.) We can understand A as a subring of k, where k is $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$, resp. In particular, A is an integral domain.*

*For $d = -1, -2, -3$, we define the **norm***

$$N\colon k \to \mathbb{Q}, \qquad a + b\sqrt{-d} \mapsto a^2 + db^2$$

which restricts to a function $N\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Then A is euclidean w. r. t. N.

Proof. Pick any field embedding $\varphi\colon k \hookrightarrow \mathbb{C}$ (e. g. the canonical inclusion). Then $\varphi(A)$ is a lattice generated by 1 and resp. i, $\mathrm{i}\sqrt{2}$ or $\frac{1}{2}(1 + \mathrm{i}\sqrt{3})$ (see Figure 1.1). Now we make the following observations:

(i) For all $a \in A$, we have $N(a) = \|\varphi(a)\|^2$, where $\|\cdot\|$ is the absolute value of complex numbers.

(ii) For each $z \in \mathbb{C}$, there exists some lattice point $z_0 \in \varphi(A)$ such that $\|z - z_0\|^2 < 1$. This geometric property holds specifically for these lattices: We can subdivide the lattice into cells. Then z must land in one of these cells. z achieves the largest distance to a closest lattice point z_0 in this cell if it lies at the centre of the cell. Thus $\|z - z_0\|^2$ is at most

$$\frac{1^2 + 1^2}{2^2} = \frac{1}{2}, \qquad \frac{1^2 + \sqrt{2}^2}{2^2} = \frac{3}{4}, \qquad \left(\frac{2}{3} \cdot \frac{\sqrt{3}}{2}\right)^2 = \frac{1}{3},$$

resp.

Now we have to show the euclidean property. For any $a, b \in A \setminus \{0\}$ set $z := \varphi(a)/\varphi(b)$. We choose $z_0 \in \varphi(A)$ such that $\|z - z_0\|^2 < 1$. Now set $q := \varphi^{-1}(z_0) \in A$ and $r := a - qb \in A$. Then we obtain

$$N(r) = N(a - qb) = \|\varphi(a - qb)\|^2 = \|\varphi(a) - \varphi(q)\varphi(b)\|^2 = \|\varphi(b)\|^2 \|z - z_0\|^2 < \|\varphi(b)\|^2 = N(b). \qquad \square$$

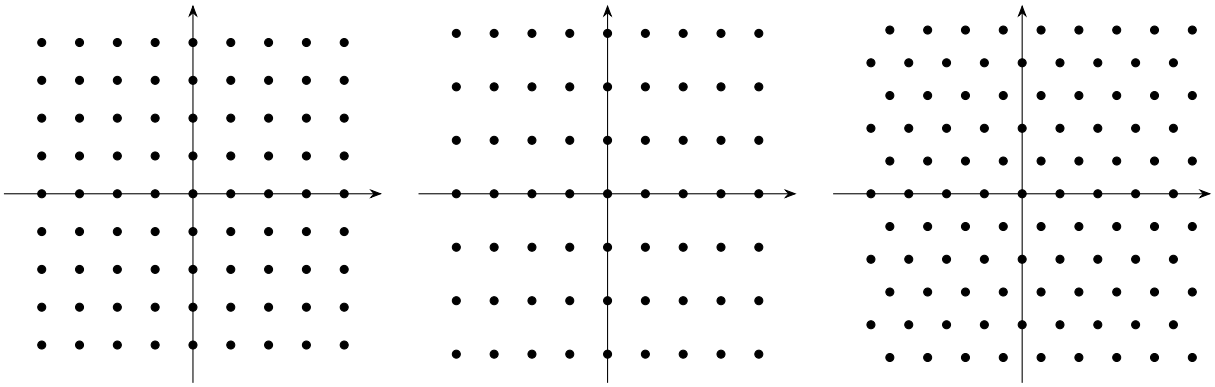


Figure 1.1: Lattices in the Gaussian plane. Left: $a + b\mathrm{i}$. Middle: $a + b\sqrt{-2}$. Right: $a + b\zeta_6 + c\zeta_6^2$.

A ring being euclidean is a very strong condition, which is only satisfied by some principal ideal domains.

Corollary 1.56. *$\mathbb{Z}[\mathrm{i}]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_6]$ are principal ideal domains and thus **unique factorisation domains**, i. e. they have unique prime factorisations.*

2 Computing Spectra

An important process in algebraic geometry and number theory is to determine the set of all prime ideals of a ring, the so-called *spectrum*.

2.1 Computing Maximal Ideals

Before we come to prime ideals, we will compute maximal ideals first.

Problem 2.1. Let $A = \mathbb{Z}[T]/(f)$, where $1 \neq f \in \mathbb{Z}[T]$ is monic. Our aim is to determine $\mathrm{MaxSpec}(A)$, the set of all maximal ideals of A.

Lemma 2.2. *Let $A \coloneqq \mathbb{Z}[T]/(f)$ and $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. Then $\mathfrak{m} \cap \mathbb{Z} = (p)$ for some prime number $p \in \mathbb{Z}$.*

Proof. From Example 1.14 we know that $A \cong \bigoplus_{i=0}^{\deg(f)-1} \mathbb{Z}$ as an abelian group, which is finitely generated. Under the canonical projection $A \twoheadrightarrow A/\mathfrak{m}$, we see that $A/\mathfrak{m}$ must be finitely generated as an abelian group too. By Corollary 1.29, $A/\mathfrak{m}$ is a field.

Recall from [Sch, Lem. 5.12, 5.13] that for any field k, there exists a unique ring map $\varphi\colon \mathbb{Z} \to k$, and $\ker(\varphi) = (\operatorname{char}(k))$. Thus φ is either injective (if $\operatorname{char}(k) = 0$) or $\varphi(\mathbb{Z}) \cong \mathbb{F}_p$ for some prime p (if $\operatorname{char}(k) = p$). In the first case, k contains a subfield isomorphic to $\mathbb{Q}$, as $\varphi(n)^{-1} \in k$ corresponds to $\frac{1}{n} \in \mathbb{Q}$ for all $n \in \mathbb{Z} \setminus \{0\}$.

Now back to our original task. Consider $\varphi\colon \mathbb{Z} \to A/\mathfrak{m}$. Since $\mathbb{Q}$ is not finitely generated as an additive abelian group (namely $\mathbb{Q} = \langle \frac{1}{n}, n \geq 1 \rangle$), there is no embedding $\mathbb{Q} \hookrightarrow A/\mathfrak{m}$. Therefore we must have $\operatorname{char}(A/\mathfrak{m}) = p$ for some prime p. If we look more closely, φ is actually $\mathbb{Z} \hookrightarrow A \twoheadrightarrow A/\mathfrak{m}$. This implies $(p) = \ker(\varphi) = \mathfrak{m} \cap \mathbb{Z}$. □

Thus we can refine our problem: Given a prime p, what are all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$ such that $\mathfrak{m} \cap \mathbb{Z} = (p)$?

Remark 2.3. Some general facts for any ring A.

(i) Let $\mathfrak{a} \subseteq A$ be an ideal. Then there is a bijection (the same as in Corollary 1.29)

$$\begin{aligned} \operatorname{MaxSpec}(A/\mathfrak{a}) &\leftrightarrow \{\mathfrak{m} \in \operatorname{MaxSpec}(A) \mid \mathfrak{a} \subseteq \mathfrak{m}\}, \\ \bar{\mathfrak{m}} &\mapsto \pi^{-1}(\bar{\mathfrak{m}}), \\ \pi(\mathfrak{m}) = \mathfrak{m}/\mathfrak{a} &\mapsfrom \mathfrak{m}. \end{aligned}$$

(ii) Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be arbitrary ideals. Then we already know $\mathfrak{a} + \mathfrak{b} \coloneqq (\mathfrak{a} \cup \mathfrak{b})$. In particular, we have

$$(f_1, \dots, f_n) + (g_1, \dots, g_m) = (f_1, \dots, f_n, g_1, \dots, g_m).$$

Set $\bar{\mathfrak{a}} = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b} \subseteq A/\mathfrak{b}$ and $\bar{\mathfrak{b}} = (\mathfrak{a} + \mathfrak{b})/\mathfrak{a} \subseteq A/\mathfrak{a}$. By Noether's isomorphism theorem, we obtain

$$(A/\mathfrak{b})/\bar{\mathfrak{a}} \cong A/\mathfrak{a} + \mathfrak{b} \cong (A/\mathfrak{a})/\bar{\mathfrak{b}}.$$

(iii) Let $\mathfrak{a} \subseteq A$ be an ideal and $\bar{\mathfrak{b}} = (g_1, \dots, g_m) \subseteq A/\mathfrak{a}$. Pick any lift $\tilde{g}_i$ of g_i to A for all $1 \leq i \leq m$, i. e. any $\tilde{g}_i \in A$ such that $\pi(\tilde{g}_i) = g_i$. Then by the well-known bijection between ideals,

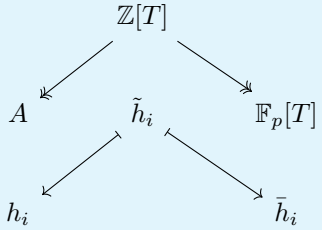
$$\pi^{-1}(\bar{\mathfrak{b}}) = \mathfrak{a} + (\tilde{g}_1, \dots, \tilde{g}_m).$$

Observation 2.4. Back to $A = \mathbb{Z}[T]/(f)$. With $\bar{f} \coloneqq f \bmod (p)$ we obtain

$$\begin{aligned} \{\mathfrak{m} \subset A \mid \mathfrak{m} \cap \mathbb{Z} = (p)\} &\overset{2.2}{=} \{\mathfrak{m} \subset A \mid (p) \subseteq \mathfrak{m}\} \overset{\text{(i)}}{=} \operatorname{MaxSpec}(A/pA) \overset{\text{(ii)}}{=} \operatorname{MaxSpec}(\mathbb{Z}[T]/(p, f)) \\ &\overset{\text{(ii)}}{=} \operatorname{MaxSpec}((\mathbb{Z}[T]/p\mathbb{Z}[T])/(\bar{f})) \overset{\text{(i)}}{=} \operatorname{MaxSpec}(\mathbb{F}_p[T]/(\bar{f})) \\ &\overset{\text{(i)}}{=} \{(\bar{h}_i) \mid \text{irreducible factors } \bar{h}_i \in \mathbb{F}_p[T] \text{ of } \bar{f}\} \\ &\overset{\text{(ii)},\text{(iii)}}{=} \{(p, h_i) \mid h_i \in A \text{ is image of any lift } \tilde{h}_i \in \mathbb{Z}[T] \text{ of } \bar{h}_i \text{ to } \mathbb{Z}[T]\}. \end{aligned}$$

The second to last equality follows from properties of $\mathbb{F}_p[T]$ being a principal ideal domain (irreducible elements generate maximal ideals, and $(f) \subseteq (g)$ if and only if $g \mid f$).

Annotation to the lift: For any irreducible factor $\bar{h}_i \in \mathbb{F}_p[T]$ of $\bar{f}$, we pick a pre-image $\tilde{h}_i \in \mathbb{Z}[T]$ under the projection $\mathbb{Z}[T] \to \mathbb{F}_p[T]$, $\tilde{h}_i \mapsto \tilde{h}_i \bmod (p) = \bar{h}_i$. After that, we take the image of $\tilde{h}_i$ under the projection $\mathbb{Z}[T] \to A$, $\tilde{h}_i \mapsto \tilde{h}_i + (f) = h_i$.



2.2 Sum of Squares

Theorem 2.5 (Fermat, Euler 1758)**.** *Let $p \in \mathbb{Z}_{\geq 0}$ be a prime. Then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 2 \mod 4$.*

Before we start, we need the following.

Lemma 2.6. *$T^2 + 1 \in \mathbb{F}_p[T]$ is either*

- *$(T+1)^2$, if $p = 2$,*
- *$(T-\alpha)(T+\alpha)$, if $p \equiv 1 \mod (4)$, where $\alpha \in \mathbb{F}_p^\times$ such that $\alpha^2 = -1$,*
- *irreducible, if $p \equiv 3 \mod (4)$.*

Proof. The case $p = 2$ is correct. Assume that $p \neq 2$.

We know that $\mathbb{F}_p^\times$ is a cyclic group of even order $p-1$. Then there exists some $\zeta \in \mathbb{F}_p^\times$ such that $\operatorname{ord}(\zeta) = p-1$, hence $\zeta^{(p-1)/2} \neq 1$ and $(\zeta^{(p-1)/2})^2 = 1$. We conclude that $\zeta^{(p-1)/2} = -1$ (if $\operatorname{char}(k) \neq 2$, then $T^2 - 1$ has precisely the roots ± 1).

Now $T^2 + 1$ has root $\alpha \in \mathbb{F}_p$ (i. e. $\alpha^2 = -1$) if and only if we can write $\zeta^{(p-1)/2} = (\zeta^k)^2$ for some $k \geq 0$ if and only if $\frac{1}{2}(p-1)$ is even. This is only possible if and only if $p \equiv 1 \mod (4)$ (in both cases $\frac{1}{2}(p-1) \equiv 0, 2 \mod (4)$). □

Now to the actual proof.

Proof. Firstly, the easier 'only if' implication: The quadratic residue classes are $0^2 \equiv 2^2 \equiv 0$ and $1^2 \equiv 3^2 \equiv 1 \mod (4)$. Therefore $x^2 + y^2 \equiv 0, 1, 2 \mod (4)$ for any $x, y \in \mathbb{Z}$. Thus $p \equiv 1, 2 \mod (4)$ (no prime is divisible by 4).

Now to the converse. This implication is far more difficult and we will exhaust the fact that $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain.

(i) Let $p \in \mathbb{Z}$ be a prime. As we have seen in Observation 2.4, we have

$$\mathbb{Z}[\mathrm{i}]/(p) \cong \mathbb{Z}[T]/(p, T^2+1) \cong \mathbb{F}_p[T]/(T^2+1).$$

According to Observation 2.4 in combination with Lemma 2.2, we have

$$\operatorname{MaxSpec}(\mathbb{Z}[\mathrm{i}]) = \coprod_{p \text{ prime}} \begin{cases} (2, \mathrm{i}+1), & \text{if } p = 2, \\ (p, \mathrm{i}-\alpha), (p, \mathrm{i}+\alpha) \text{ with } \alpha^2 \equiv -1 \mod (p), & \text{if } p \equiv 1 \mod (4), \\ (p), & \text{if } p \equiv 3 \mod (4). \end{cases}$$

(ii) Since $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain (Corollary 1.56), every $\mathfrak{m} \in \operatorname{MaxSpec}(\mathbb{Z}[\mathrm{i}])$ has the form $\mathfrak{m} = (\pi)$ for some prime element $\pi \in \mathbb{Z}[\mathrm{i}]$ (see the proof of Theorem 1.38 (iii)).

Assume that $(\pi) \cap \mathbb{Z} = (p)$ with $p \equiv 1, 2 \mod (4)$, according to Lemma 2.2. Then $(p) \neq (\pi)$ because $\pi \neq 0$ in $\mathbb{F}_p[T]/(T^2+1) \cong \mathbb{Z}[\mathrm{i}]/(p)$ (we saw that $(\pi) = (p, \mathrm{i}+a)$ corresponds to some ideal $(0) \neq (T+a) \subseteq \mathbb{F}_p[T]/(T^2+1)$ with $(T+a) \mid (T^2+1)$ in $\mathbb{F}_p[T]$) and thus $p \nmid \pi$ in $\mathbb{Z}[\mathrm{i}]$. Therefore by Lemma 1.34, π is a proper divisor of p in $\mathbb{Z}[\mathrm{i}]$, i. e. $\frac{p}{\pi} \notin \mathbb{Z}[\mathrm{i}]^\times$.

Let us write $\pi = x + \mathrm{i}y \in \mathbb{Z}[\mathrm{i}]$. We claim that $N(\pi) := x^2 + y^2 = p$. Proving this finishes the whole proof.

Since the norm is multiplicative, we have $N(\pi)N(\frac{p}{\pi}) = N(p) = p^2$, hence $N(\pi) \in \{1, p, p^2\}$. Again by multiplicativity and $N(\mathbb{Z}[\mathrm{i}]) \subseteq \mathbb{Z}_{\geq 0}$, we observe that $u \in \mathbb{Z}[\mathrm{i}]^\times$ if and only if $N(u) = 1 = N(1)$. Since $\pi, \frac{p}{\pi} \notin \mathbb{Z}[\mathrm{i}]^\times$ (π is prime), we have $N(\pi) \neq 1 \neq N(\frac{p}{\pi})$, thus $N(\pi) = N(\frac{p}{\pi}) = p$. □

Exercise 2.7. Use the fact that $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain to prove that for $n \in \mathbb{Z}_{>0}$, the following are equivalent:

(i) $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

(ii) Let $n = p_1^{e_1} \cdots p_r^{e_r}$ with $p_i \neq p_j$ for all $i \neq j$ be the prime factorisation of n. If $p_i \equiv 3 \mod (4)$, then e_i is even.

Remark 2.8. There exists analogue statements for $\mathbb{Z}[\zeta_6] = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$ (Exercise 8.8) and $\mathbb{Z}[\sqrt{-2}]$. For $\mathbb{Z}[\sqrt{-2}]$, we have $p = x^2 + 2y^2$ if and only if $p \equiv 1, 2, 3 \mod 8$. In these cases, we can factorise p in the respective rings, see e. g. sec. 2.2. In all other cases, p is indeed a prime element.

prime $p \in \mathbb{Z}_{>0}$	in $\mathbb{Z}[\mathrm{i}]$	in $\mathbb{Z}[\sqrt{-2}]$
2	$-\mathrm{i}(1+\mathrm{i})^2$	$-(\sqrt{-2})^2$
3	prime	$(1+\sqrt{-2})(1-\sqrt{-2})$
5	$(1+2\mathrm{i})(1-2\mathrm{i})$	prime
7	prime	prime

Remark 2.9. Historically, these specific examples and other generalisations in number theory were an important driver in the development of commutative algebra.

However, solving $p = x^2 + ny^2$ with primes $p \in \mathbb{Z}_{>0}$ or, more generally, $m = x^2 + ny^2$ with $m \in \mathbb{Z}_{>0}$ for large n is far more difficult and requires *class field theory*, which will be a topic in algebra II. As a reference, there is the nice book [Cox].

2.3 The Spectrum

Lect. 4
17.04.23

Definition 2.10. Let A be a ring. An ideal $\mathfrak{p} \subseteq A$ is **prime** if $\mathfrak{p} \neq A$ and if $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Lemma 2.11. *Let A be a ring. Then an ideal $\mathfrak{p} \subseteq A$ is prime if and only if $A/\mathfrak{p}$ is an integral domain.*

Proof. (From me.) Suppose that $(a+\mathfrak{p})(b+\mathfrak{p}) = 0$ in $A/\mathfrak{p}$. By definition, $A/\mathfrak{p}$ is an integral domain if and only if $a+\mathfrak{p} = 0$ or $b+\mathfrak{p} = 0$. This means $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. As $ab \in \mathfrak{p}$, this is equivalent to $\mathfrak{p}$ being prime. □

Lemma 2.12. *Let $\varphi\colon A \to B$ be a ring map and $\mathfrak{q} \subset B$ be a prime ideal. Then $\varphi^{-1}(\mathfrak{q}) \subset A$ is a prime ideal, i. e.* pullbacks *are prime ideals.*

Proof. Preimages of ideals are again ideals ($\mathfrak{q}$ is an abelian group, so $\varphi^{-1}(\mathfrak{q})$ is an abelian group too; for all $a \in A$ and $x \in \varphi^{-1}(\mathfrak{q})$ we have $\varphi(ax) = \varphi(a)\varphi(x) \in \mathfrak{q}$ since $\varphi(a) \in B$ and $\varphi(x) \in \mathfrak{q}$).

By Lemma 1.25 and $\mathfrak{q} \neq B$, we have $1_B \notin \mathfrak{q}$. Thus $1_A \notin \varphi^{-1}(\mathfrak{q})$ and hence $\varphi^{-1}(\mathfrak{q}) \neq A$. Moreover, suppose that $xy \in \varphi^{-1}(\mathfrak{q})$, then $\varphi(xy) = \varphi(x)\varphi(y) \in \mathfrak{q}$. Since $\mathfrak{q}$ is prime, it follows that $\varphi(x) \in \mathfrak{q}$ or $\varphi(y) \in \mathfrak{q}$, thus $x \in \varphi^{-1}(\mathfrak{q})$ or $y \in \varphi^{-1}(\mathfrak{q})$. □

Definition 2.13. The **spectrum** $\operatorname{Spec}(A)$ of a ring A is the set of all prime ideals $\mathfrak{p} \subset A$.

Let $\varphi\colon A \to B$ be a ring map. Then we define

$$\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A), \qquad \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q}).$$

Example 2.14. Let $\pi\colon A \twoheadrightarrow A/\mathfrak{a}$ be the canonical projection map. Then, as in Observation 2.4,

$$\operatorname{Spec}(\pi)\colon \operatorname{Spec}(A/\mathfrak{a}) \to \operatorname{Spec}(A)$$

is obviously injective, where the image is the set of all prime ideals $\mathfrak{a} \subseteq \mathfrak{p} \subset A$.

Example 2.15. Let $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[\mathrm{i}]$ be the canonical inclusion map. Then consider

$$\operatorname{Spec}(\iota)\colon \operatorname{Spec}(\mathbb{Z}[\mathrm{i}]) \to \operatorname{Spec}(\mathbb{Z}), \qquad \mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{Z}.$$

Some general facts known from the introduction to algebra: Through the combination of Corollary 1.29 and Lemma 2.11, we conclude that maximal ideals are prime. Furthermore, directly by definition, an ideal $(p) \neq (0)$ is prime if and only if p is a prime element. So specifically in principal ideal domains, due to Theorem 1.38 (iii), we conclude that all non-zero prime ideals are maximal.

Thus $\operatorname{Spec}(\iota)$ is (almost) identical to the map $\operatorname{MaxSpec}(\mathbb{Z}[\mathrm{i}]) \to \operatorname{MaxSpec}(\mathbb{Z})$ from the previous subsection with the addition of $(0) \mapsto (0)$. As we have seen in the proof of Theorem 2.5, each fibre (i. e. a preimage of an element) contains either one or two elements.

Example 2.16. $\operatorname{Spec}(\mathbb{Z} \hookrightarrow \mathbb{Q})\colon \operatorname{Spec}(\mathbb{Q}) \to \operatorname{Spec}(\mathbb{Z})$ maps $(0) \mapsto (0)$. Since $\mathbb{Q}$ is a field, by Lemma 1.27, (0) is the only maximal ideal in $\mathbb{Q}$. On the other hand, (0) is not maximal in $\mathbb{Z}$. Here we see that preimages of maximal ideals need not to be maximal, but prime ideals do. This is the reason why we consider Spec more naturally than MaxSpec.

Remark 2.17. Apparently $\operatorname{Spec}(0) = \varnothing$. On the other hand, for all rings $A \neq 0$, we have $\operatorname{Spec}(A) \neq \varnothing$ due to the following theorem.

Theorem 2.18 (Krull's theorem). *Every ring $A \neq 0$ has a maximal ideal.*

Proof. This is an application of Zorn's lemma. Let Σ be the set of all ideals $\mathfrak{a} \subset A$. We can partially order Σ w. r. t. inclusion. As $A \neq 0$, we have $(0) \in \Sigma \neq \varnothing$.

Let $S \subseteq \Sigma$ be a *chain*, i. e. we can order any two elements (in this case $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$ for all $\mathfrak{a}, \mathfrak{b} \in S$). Then $\mathfrak{c} \coloneqq \bigcup_{\mathfrak{a} \in S} \mathfrak{a}$ is again an ideal. (By the definition of a chain, we can literally order all elements of S into an ascending chain. Then for finitely many elements in $\mathfrak{c}$, we find an $\mathfrak{a} \in S$ containing them. Then all rules of ideals apply to $\mathfrak{a}$.) By Lemma 1.25 and $\mathfrak{a} \neq A$ for all $\mathfrak{a} \in S$, it follows that $1 \notin \mathfrak{a}$ and thus $1 \notin \mathfrak{c}$, implying $\mathfrak{c} \neq A$. Hence $\mathfrak{c} \in \Sigma$ is an upper bound of S.

Finishing with Zorn's lemma, there exist maximal elements in Σ. □

Corollary 2.19. *Let $A \neq 0$ be a ring, and let $\mathfrak{a} \subset A$ be an ideal. Then there exists a maximal ideal $\mathfrak{m} \subset A$ such that $\mathfrak{a} \subseteq \mathfrak{m}$.*

Proof. We can apply the previous theorem to $A/\mathfrak{a} \neq 0$. The result follows from Remark 2.3 (i). □

Corollary 2.20. *Let $A \neq 0$ be a ring. Then $x \in A^\times$ if and only if $x \notin \mathfrak{m}$ for all maximal ideals $\mathfrak{m} \subset A$.*

Proof. This follows from Lemma 1.25: We have $x \in A^\times$ if and only if $(x) = A$. $(x) = A$ implies $x \notin \mathfrak{m}$ for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. If $x \notin \mathfrak{m}$ for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$, there is no $\mathfrak{m}$ that contains (x). By Corollary 2.19, we must have $(x) = A$. □

Example 2.21. Let $A \neq 0$ be a ring with a unique maximal ideal $\mathfrak{m}$. Then $A = A^\times \sqcup \mathfrak{m}$. (For example, $A = k[\![T_1, \dots, T_n]\!]$ has the unique maximal ideal $\mathfrak{m} = (T_1, \dots, T_n)$.) Conversely, if $A \setminus A^\times =: \mathfrak{m}$ is a maximal ideal in $A \neq 0$, then $\mathfrak{m}$ is the only maximal ideal (another maximal ideal would contain a unit, which is impossible). We will later call such a ring *local*.

Recall: The *nilradical* $\operatorname{nil}(A)$ of a ring A is the set of all nilpotent elements in A.

Proposition 2.22. *For any ring A, we have*

$$\operatorname{nil}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}.$$

Proof. Let $x \in \operatorname{nil}(A)$, say $x^n = 0$. Then $x^n = 0 \in \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, thus $x \in \mathfrak{p}$ by definition of prime ideals. So $\operatorname{nil}(A) \subseteq \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$.

The converse inclusion is again an application of Zorn's lemma. Let $f \notin \operatorname{nil}(A)$, and let Σ be the set of all ideals $\mathfrak{a} \subseteq A$ with $f^n \notin \mathfrak{a}$ for all $n \geq 0$. We can partially order Σ by inclusion. Since $f^n \neq 0$ for all $n \geq 0$, we have $(0) \in \Sigma \neq \varnothing$.

Let $S \subseteq \Sigma$ be a chain. For all $n \geq 0$ and $\mathfrak{a} \in S$, we have $f^n \notin \mathfrak{a}$ and thus $f^n \notin \mathfrak{c} \coloneqq \bigcup_{\mathfrak{a} \in S} \mathfrak{a}$. Hence $\mathfrak{c} \in \Sigma$ is an upper bound of S.

By Zorn's Lemma, there exists a maximal element in Σ, say $\mathfrak{p} \in \Sigma$. We claim that $\mathfrak{p}$ is prime. Firstly, note that $\mathfrak{p} \neq A$ as $f \notin \mathfrak{p}$. Let $x, y \notin \mathfrak{p}$. Then $(x) + \mathfrak{p}, (y) + \mathfrak{p} \notin \Sigma$ by maximality of $\mathfrak{p}$. This means there is some $n \geq 0$ such that $f^n \in (x) + \mathfrak{p}, (y) + \mathfrak{p}$, say $f^n = ax + p_1 = by + p_2$ with $a, b \in A$ and $p_1, p_2 \in \mathfrak{p}$. Then

$$f^{2n} = abxy + byp_1 + axp_2 + p_1p_2 \in (abxy) + \mathfrak{p}.$$

Thus $(abxy) + \mathfrak{p} \notin \Sigma$, and hence $xy \notin \mathfrak{p}$ (otherwise $(abxy) + \mathfrak{p} = \mathfrak{p} \in \Sigma$), so $\mathfrak{p}$ is prime. In particular, $f \notin \bigcap_{\mathfrak{q} \in \operatorname{Spec}(A)} \mathfrak{q}$. □

Corollary 2.23. *Let A be a ring, and let $\pi\colon A \to A/\operatorname{nil}(A)$ be the canonical projection. Then the induced map*

$$\operatorname{Spec}(\pi)\colon \operatorname{Spec}(A/\operatorname{nil}(A)) \to \operatorname{Spec}(A).$$

on spectra is a bijection.

Proof. (From me.) We already have a bijection between ideals $\bar{\mathfrak{a}} = \pi(\mathfrak{a}) \subseteq A/\operatorname{nil}(A)$ and ideals $\operatorname{nil}(A) \subseteq \mathfrak{a} \subseteq A$.

We claim that if $\mathfrak{p} \in \operatorname{Spec}(A)$, then $\pi(\mathfrak{p}) = \bar{\mathfrak{p}} \in \operatorname{Spec}(A/\operatorname{nil}(A))$. By Noether's isomorphism theorem, we have $(A/\operatorname{nil}(A))/\bar{\mathfrak{p}} \cong A/\mathfrak{p}$, which is an integral domain due to Lemma 2.11. Thus $\bar{\mathfrak{p}} \in \operatorname{Spec}(A/\operatorname{nil}(A))$.

Together with Lemma 2.12, π and π^{-1} retain primality of ideals. Therefore the bijection between ideals actually restricts to a bijection between prime ideals (notice that all prime ideals contain $\operatorname{nil}(A)$). □

Problem 2.24. We want to develop techniques to study spectra in order to generalise and conceptualise the map $\operatorname{MaxSpec}(\mathbb{Z}[T]/(f)) \to \operatorname{MaxSpec}(\mathbb{Z})$ for monic $1 \neq f \in \mathbb{Z}[T]$ from previous sections. As we have argued before, it is more natural to generalise

$$\operatorname{Spec}(\mathbb{Z}[T]/(f)) \to \operatorname{Spec}(\mathbb{Z}).$$

2.4 Example: Spec($\mathbb{Z}[T]$)

To motivate this question, we will consider a non-trivial example.

Remark 2.25. For any ring A, $\operatorname{Spec}(A)$ naturally forms a partially ordered set w. r. t. inclusion. E. g. for $\operatorname{Spec}(\mathbb{Z})$, although relatively boring, we have $(0) \subset (2), (3), (5), \ldots$

Definition 2.26. Let A be a ring.

(i) The **height** $\operatorname{ht}(\mathfrak{p})$ of $\mathfrak{p} \in \operatorname{Spec}(A)$ is defined as the supremum over all $n \geq 0$ such that there exist $\mathfrak{p}_0, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(A)$ with

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}.$$

(ii) The **Krull dimension** of A is

$$\dim(A) \coloneqq \sup_{\mathfrak{p} \in \operatorname{Spec}(A)} \operatorname{ht}(\mathfrak{p}).$$

Remark 2.27. In general, the height of any specific maximal ideal is in general not the Krull dimension of the ring. Instead, the Krull dimension is the supremum of the heights of all maximal ideals.

The reason is that different maximal ideals can have different heights. For example, take rings A_1, A_2 with maximal ideals $\mathfrak{m}_1 \subset A_1$ and $\mathfrak{m}_2 \subset A_2$ such that $\operatorname{ht}(\mathfrak{m}_1) \neq \operatorname{ht}(\mathfrak{m}_2)$. Then $\mathfrak{m}_1 \times A_2$ and $A_1 \times \mathfrak{m}_2$ are maximal ideals in $A_1 \times A_2$ with different heights (the ideals $A_1 \times \mathfrak{p}_2$ and $\mathfrak{p}_1 \times A_2$ with $\mathfrak{p}_i \in \operatorname{Spec}(A_i)$ for $i = 1, 2$ are the only prime ideals).

Proposition 2.28. *We have* $\dim(\mathbb{Z}[T]) = 2$. *Furthermore,* $\operatorname{Spec}(\mathbb{Z}[T])$ *consists of the following elements:*

(i) (0) *(of height 0).*

(ii) (f) *with irreducible* $f \in \mathbb{Z}[T]$ *(of height 1).*

(iii) (p, f) *with prime* $p \in \mathbb{Z}$ *and* $f \in \mathbb{Z}[T]$ *such that* $f \bmod (p)$ *is irreducible (of height 2).*

Moreover, every prime ideal of height 1 is contained in a prime ideal of height 2, meaning only prime ideals of height 2 are maximal.

Proof. The proof follows a common strategy: We compute all fibres of $\operatorname{Spec}(\mathbb{Z}[T]) \to \operatorname{Spec}(\mathbb{Z})$, $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{Z}$ (this map originates from the canonical inclusion). Let $0 \neq \mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[T]$. Recall that the prime ideals in $\mathbb{Z}$ are (p) and (0) for all primes $p \in \mathbb{Z}$.

(i) Assume that $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime $p \in \mathbb{Z}$. Then $\bar{\mathfrak{p}} \coloneqq \mathfrak{p}/p\mathbb{Z}[T]$ is a prime ideal of $\mathbb{F}_p[T] \cong \mathbb{Z}[T]/p\mathbb{Z}[T]$ (this follows from Noether's isomorphism theorem with Lemma 2.11). Since $\mathbb{F}_p[T]$ is a principal ideal domain, every non-zero prime ideal is generated by an irreducible $\bar{f} \in \mathbb{F}_p[T]$. Hence we have $\mathfrak{p} = (p)$ if $\bar{\mathfrak{p}} = (0)$ or $\mathfrak{p} = (p, f)$ if $\bar{\mathfrak{p}} = (\bar{f})$, where $f \in \mathbb{Z}[T]$ is any lift of an irreducible $\bar{f} = f \bmod p$ in $\mathbb{F}_p[T]$.

(ii) Assume that $\mathfrak{p} \cap \mathbb{Z} = (0)$. Here we need a new technique called *localisation* (we will later introduce this in more generality). Consider $\mathfrak{q} \coloneqq \mathfrak{p}\mathbb{Q}[T]$, i. e. the ideal in $\mathbb{Q}[T]$ generated by elements in $\mathfrak{p}$. We claim that $\mathfrak{q}$ is a prime ideal of $\mathbb{Q}[T]$.

If $1 \in \mathfrak{q}$, then we can write $1 = \sum_{i=1}^{n} f_i a_i$ with $f_i \in \mathbb{Q}[T]$ and $a_i \in \mathfrak{p}$. Let $0 \neq m \in \mathbb{Z}$ be the common denominator of all coefficients of all f_i. Then $mf_i \in \mathbb{Z}[T]$ for all $i = 1, \dots, n$, hence $m = \sum_{i=1}^{n} (mf_i)a_i \in \mathfrak{p}$, which yields the contradiction $0 \neq m \in \mathfrak{p} \cap \mathbb{Z} = (0)$. We conclude $1 \notin \mathfrak{q}$ and, by Lemma 1.25, $\mathfrak{q} \neq \mathbb{Q}[T]$.

Next let $gh \in \mathfrak{q}$ for some $g, h \in \mathbb{Q}[T]$. Then we can write $gh = \sum_{i=1}^{n} f_i a_i$ with $f_i \in \mathbb{Q}[T]$ and $a_i \in \mathfrak{p}$. Now we choose a common denominator $0 \neq m \in \mathbb{Z}$ such that $mg, mh, mf_i \in \mathbb{Z}[T]$ for all $i = 1, \dots, n$. Then $mf \cdot mg = m \sum_{i=1}^{n} (mf_i)a_i \in \mathfrak{p}$ and by the prime ideal property, $mf \in \mathfrak{p}$ or $mg \in \mathfrak{p}$. Thus $f \in \mathfrak{q}$ or $g \in \mathfrak{q}$ as $m^{-1} \in \mathbb{Q}$, and we proved that $\mathfrak{q}$ is prime.

Since $\mathbb{Q}[T]$ is a principal ideal domain, we can write $\mathfrak{q} = (h)$ for some irreducible $h \in \mathbb{Q}[T]$. Multiplying with the common denominator of all coefficients, we may assume that $h \in \mathbb{Z}[T]$. Further factoring out the greatest common divisor of all coefficients, we may assume that h is primitive, i. e. that the greatest common divisor of all coefficients of h is 1.

With *Gauss's lemma*, we can prove the following: If $h \in \mathbb{Z}[T]$ is primitive and $f \in \mathbb{Z}[T]$, then $h \mid f$ in $\mathbb{Z}[T]$ if and only if $h \mid f$ in $\mathbb{Q}[T]$. (A proof: Let $f = hg$ for some $g \in \mathbb{Q}[T]$. Then there exists a $c \in \mathbb{Q}$ such that $g = cg'$ and $g' \in \mathbb{Z}[T]$ is primitive. By Gauss's lemma, $hg' \in \mathbb{Z}[T]$ is primitive. Since $chg' = f \in \mathbb{Z}[T]$, we must have $c \in \mathbb{Z}$; otherwise the denominator would divide all coefficients of hg'. Hence $g = cg' \in \mathbb{Z}[T]$ and $h \mid f$ in $\mathbb{Z}[T]$.)

As a consequence, we have $\mathfrak{q} \cap \mathbb{Z}[T] = (h)$ in $\mathbb{Z}[T]$ with irreducible and primitive h. We will later show that $\mathfrak{q} \cap \mathbb{Z}[T] = \mathfrak{p}$ (see Lemma 2.52). The claim about the heights is Exercise 8.13. □

Definition 2.29. A ring A is a **unique factorisation domain** (UFD), if A is an integral domain, and if every $f \in A \setminus \{0\}$ has a prime factorisation. Similar to Theorem 1.38, it must be unique up to permutation and units.

Proposition 2.30. *A is a unique factorisation domain if and only if $A[T]$ is a unique factorisation domain.*

Proof. (From me.) We know the 'only if' implication from the introduction to algebra, see Gauss's theorem ([Sch, Thm. 5.50]). For the converse, notice that, due to $A \hookrightarrow A[T]$, there is a prime factorisation in $A[T]$ for each element in A. By considering the degree of the factors, it follows that this prime factorisation is actually in A. □

Proposition 2.31. *Let A be a unique factorisation domain. Then we have the following:*

(i) *A prime ideal $\mathfrak{p} \subseteq A$ is of height 1 if and only if there exists a prime element $\pi \in A$ such that $\mathfrak{p} = (\pi)$.*

(ii) *A is a principal ideal domain if $\dim(A) \leq 1$.*

Proof. Exercise 8.11. □

2.5 Localisation

The following on localisations will partly be treated in [AtMac, ch. 3].

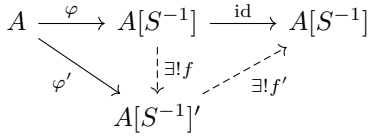
Definition 2.32. Let A be a ring and $S \subseteq A$ a subset. Then the **localisation** of A in S is a ring map $\varphi\colon A \to A[S^{-1}]$ (here, $A[S^{-1}]$ is just notation for some ring which we are characterising) such that:

(i) $\varphi(S) \subseteq A[S^{-1}]^\times$.

(ii) **Universal property of localisations**: For all ring maps $\psi\colon A \to B$ such that $\psi(S) \subseteq B^\times$, there is a unique factorisation

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A[S^{-1}] \\ & \searrow^{\psi} & \downarrow{\scriptstyle \exists!} \\ & & B \end{array}$$

Remark 2.33. Because of the universal property, the localisation is unique up to unique isomorphism. (Consider



where φ and φ' are two localisations of A in S. Then there are unique ring maps f and f' such that $f \circ \varphi = \varphi'$ and $f' \circ \varphi' = \varphi$. Hence $f' \circ f \circ \varphi = \varphi$. But by the universal property, the only ring map $g\colon A[S^{-1}] \to A[S^{-1}]$ with $g \circ \varphi = \varphi$ is id. Thus $f' \circ f = \mathrm{id}$. Similarly $f \circ f' = \mathrm{id}$, so f is a unique isomorphism.)

Proposition 2.34. *Localisations exist.*

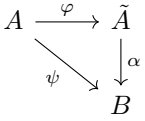
Proof. For all $s \in S$, let T_s be a variable. Consider the canonical map

$$\varphi\colon A \to \tilde{A} \coloneqq A[T_s, s \in S]/(sT_s - 1, s \in S) \tag{2.35}$$

(which might not be injective).

(i) Then $\varphi(s)T_s = sT_s = 1$ in $\tilde{A}$, meaning $\varphi(S) \subseteq \tilde{A}^\times$.

(ii) Let $\psi\colon A \to B$ be any ring map with $\psi(S) \subseteq B^\times$. Then there is at most one factorisation



through φ: α must map $\alpha(sT_s - 1) = \alpha(s)\alpha(T_s) - 1 = 0$ for all $s \in S$. Noticing $\psi(s) = \alpha(\varphi(s)) = \alpha(s)$, this is equivalent to $\psi(s)\alpha(T_s) = 1$, meaning $\alpha(T_s) = \psi(s)^{-1}$. Thus α is uniquely defined by $\alpha(T_s) = \psi(s)^{-1}$ for all $s \in S$ and $\alpha|_A = \psi$.

For the existence, consider $\beta\colon A[T_s, s \in S] \to B$ given by $\beta(T_s) = \psi(s)^{-1}$ and $\beta|_A = \psi$. Then $\psi = \beta \circ \varphi$. Furthermore, $\beta(sT_s - 1) = 0$, so β factors through $\tilde{A}$ according to the homomorphism theorem. □

Now we will give a more explicit construction of localisations, known from [Sch, sec. 5.17].

Definition 2.36. Let A be a ring and $S \subseteq A$ a subset.

(i) S is **multiplicative**, if $1 \in S$ and $a, b \in S$ implies $ab \in S$.

(ii) S is **saturated**, if S is multiplicative, and $ab \in S$ implies $a, b \in S$.

Saturated subsets are thus closed under taking divisors.

Remark 2.37. Every subset $S \subseteq A$ has a **multiplicative closure** S^{mult} and a **saturated hull** S^{sat}. We observe: For all $x, y \in B$ in a ring B, we have $xy \in B^\times$ if and only if $x, y \in B^\times$. So if $\varphi\colon A \to B$ is a ring map and $S \subseteq A$, then $\varphi(S) \subseteq B^\times$ if and only if $\varphi(S^{\mathrm{mult}}) \subseteq B^\times$ if and only if $\varphi(S^{\mathrm{sat}}) \subseteq B^\times$. If we consider B to be $A[S^{-1}]$, $A[S^{\mathrm{mult},-1}]$ or $A[S^{\mathrm{sat},-1}]$, we see through the universal property that

$$A[S^{-1}] \cong A[S^{\mathrm{mult},-1}] \cong A[S^{\mathrm{sat},-1}].$$

So w. l. o. g. we may require S to be multiplicative.

Example 2.38. Let $S = \{8\} \subset \mathbb{Z}$. Then $S^{\mathrm{mult}} = \{8^n \mid n \geq 1\}$ and $S^{\mathrm{sat}} = \{\pm 2^n \mid n \geq 0\}$.

Notation 2.39. For a subset S of a ring A, we will denote $\overline{S} \coloneqq S^{\mathrm{mult}}$.

Definition 2.40. Let A be a ring and $S \subseteq A$ be multiplicative. Then we define an equivalence relation on $S \times A$ by the following:

$$\frac{a_1}{s_1} \sim \frac{a_2}{s_2}$$

if there exists some $s_3 \in S$ such that $s_3(s_1a_2 - s_2a_1) = 0$. We denote the set of all equivalence classes by

$$S^{-1}A \coloneqq \left\{ \frac{a}{s} \;\middle|\; a \in A, s \in S \right\} / \sim,$$

which forms a ring with the usual addition and multiplication rules we know for fractions in $\mathbb{Q}$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Proposition 2.41. *Let A be a ring, and let $S \subseteq A$ be multiplicative. Then $S^{-1}A$ together with the map $A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ forms a localisation of A in S, i. e. $S^{-1}A \cong A[S^{-1}]$.*

Remark 2.42. If A is an integral domain and if $0 \notin S$, then we could equivalently require $a_1/s_1 \sim a_2/s_2$ if $a_1s_2 = a_2s_1$.

Definition 2.43. Let A be an integral domain and $S = A \setminus \{0\}$. We then call $\mathrm{Quot}(A) \coloneqq A[S^{-1}]$ the **quotient field** or **field of fractions** of A.

Example 2.44. We have $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ and $\mathrm{Quot}(\mathbb{Z}[\mathrm{i}]) = \mathbb{Q}(\mathrm{i})$.

If k is a field, then $\mathrm{Quot}(k[T]) = \{\frac{f}{g} \mid f, g \in k[T], g \neq 0\} =: k(T)$, and similarly $\mathrm{Quot}(k[T_1, \dots, T_n]) =: k(T_1, \dots, T_n)$.

Problem 2.45. We want to study

Lect. 5
20.04.23

$$\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(A[S^{-1}]) \to \mathrm{Spec}(A), \qquad \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q}).$$

Lemma 2.46. *Let A be a ring and $S \subseteq A$. Then*

$$\ker(A \to A[S^{-1}]) = \{a \in A \mid \textit{there exists } s \in \overline{S} \textit{ such that } sa = 0\}.$$

Proof. $\frac{a}{1} \sim 0$ means $s_1(s_2a - 0 \cdot 1) = 0$, so the condition $sa = 0$ for some $s \in \overline{S}$ is equivalent to $\frac{a}{1} \sim 0$. Since $A[S^{-1}] \cong \overline{S}^{-1}A$, the result follows (the kernel of the map is precisely the equivalence class of 0). □

Recall: $s \in A$ is a *zero divisor* if there exists some $0 \neq a \in A$ such that $sa = 0$. Otherwise it is *regular*.

Corollary 2.47. *Let A be a ring and $S \subseteq A$. Then the localisation $A \to A[S^{-1}]$ is injective if and only if all elements of S are regular.*

Remark 2.48. For integral domains A, we have $\mathrm{Quot}(A) \coloneqq S^{-1}A$ with $S = A \setminus \{0\}$.

But in the case of general rings A which are not integral domains, we can choose S to be the set of all regular elements of A, which is multiplicative. Then $A \hookrightarrow A[S^{-1}]$ is the best replacement for quotient fields, called the **total ring of fractions**.

Example 2.49. Let A be an integral domain and $S \subseteq A \setminus \{0\}$. Then $A[S^{-1}] \subseteq \mathrm{Quot}(A)$ is a subring, which is generated by A and new elements $\{\frac{1}{s} \mid s \in S\}$ (which behave in the usual way as inverses). E. g. $\mathbb{Z}[\frac{1}{6}] = \mathbb{Z}[\frac{1}{2}, \frac{1}{3}] \subset \mathbb{Q}$ and

$$k\left[X, \frac{1}{X(X+1)}\right] \subset k(X).$$

Example 2.50. Let A be a ring, and let $S \subseteq A$ be a multiplicative subset with a nilpotent $\varepsilon \in S$. Then $0 \in S$ and, by Lemma 2.46, $A[S^{-1}] = 0$ (we have $\ker(A \to A[S^{-1}]) = A$, and $A[S^{-1}]$ is unique up to isomorphism).

We can also derive $A[S^{-1}] = 0$ differently: Say $\varepsilon^{n+1} = 0$. Then we have, in the notion of (2.35),

$$1 = 1 - (\varepsilon T_\varepsilon)^{n+1} = (1 - \varepsilon T_\varepsilon)(1 + \varepsilon T_\varepsilon + \dots + (\varepsilon T_\varepsilon)^n).$$

By Lemma 1.25, this gives $(sT_s - 1, s \in S) = A[T_s, s \in S]$, and hence $A[S^{-1}] \cong A[T_s, s \in S]/(sT_s - 1, s \in S) = 0$.

Example 2.51. A more sophisticated example: By construction of localisations (and Noether's isomorphism theorem), we have

$$\mathbb{C}[X,Y]/(XY)[X^{-1}] \cong \mathbb{C}[X,Y,T]/(XY, XT-1).$$

The ideal $(XY, XT-1)$ contains the element $T \cdot XY - Y(XT-1) = Y$. So we can simplify to

$$\mathbb{C}[X,Y]/(XY)[X^{-1}] \cong \mathbb{C}[X,T]/(XT-1) \cong \mathbb{C}[X,X^{-1}] \subset \mathbb{C}(X)$$

(we map $T \mapsto X^{-1}$).

2.6 Localisation and Ideals

We consider the maps between ideals of A and ideals of $A[S^{-1}]$ via $\mathfrak{a} \mapsto \varphi(\mathfrak{a})A[S^{-1}]$ and $\varphi^{-1}(\mathfrak{b}) \hookleftarrow \mathfrak{b}$.

Lemma 2.52. *Let A be a ring and $S \subseteq A$. Let $\varphi\colon A \to A[S^{-1}]$ be the localisation. We define the maps*

$$\{\text{ideals of } A\} \leftrightarrow \{\text{ideals of } A[S^{-1}]\}, \qquad \mathfrak{a} \mapsto \varphi(\mathfrak{a})A[S^{-1}], \qquad \varphi^{-1}(\mathfrak{b}) \hookleftarrow \mathfrak{b},$$

where $\varphi(\mathfrak{a})A[S^{-1}] = \varphi(\mathfrak{a}) \cdot A[S^{-1}]$ denotes the ideal generated by $\varphi(\mathfrak{a})$ in $A[S^{-1}]$.

Then $\mathfrak{b} \mapsto \varphi^{-1}(\mathfrak{b})$ is injective. More precisely, this map is the right inverse of $\mathfrak{a} \mapsto \varphi(\mathfrak{a})A[S^{-1}]$, i. e.

$$\mathfrak{b} = \varphi(\varphi^{-1}(\mathfrak{b}))A[S^{-1}].$$

Proof. We will show the equality, for injectivity follows from $\varphi \circ \varphi^{-1} = \mathrm{id}$. From a set-theoretic perspective, $\varphi(\varphi^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$ always holds true. For the converse inclusion, if $\frac{a}{s} \in \mathfrak{b}$ with $a \in A$ and $s \in \overline{S}$, then $\frac{a}{1} = s\frac{a}{s} \in \mathfrak{b}$ and thus $a = \varphi^{-1}(\frac{a}{1}) \in \varphi^{-1}(\mathfrak{b})$, hence $\frac{a}{s} = \frac{1}{s} \cdot \frac{a}{1} = \frac{1}{s}\varphi(a) \in \varphi(\varphi^{-1}(\mathfrak{b}))A[S^{-1}]$. □

Example 2.53. In general, the ideals of $A[S^{-1}]$ will always be 'simpler' then those of A.

We will show that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. By way of contradiction, assume that it is. We compute the fibre of (3) w. r. t. $\mathrm{Spec}(\mathbb{Z}[\sqrt{-5}]) \to \mathrm{Spec}(\mathbb{Z})$.

Let $\mathfrak{p} \subseteq \mathbb{Z}[\sqrt{-5}]$ be a prime ideal with $\mathfrak{p} \cap \mathbb{Z} = (3)$. By Noether's isomorphism theorem, $\mathfrak{p}/(3\mathbb{Z}[\sqrt{-5}])$ is a prime ideal of $\mathbb{Z}[\sqrt{-5}]/(3) \cong \mathbb{F}_3[T]/(T^2+5)$. As $\mathbb{F}_3[T]$ is a principal ideal domain, the prime ideals of $\mathbb{F}_3[T]/(T^2+5)$ are generated by irreducible factors of T^2+5 mod (3). We have

$$T^2 + 5 \equiv T^2 - 1 = (T+1)(T-1) \mod (3).$$

After lifting to $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[T]/(T^2+5)$, there are exactly two prime ideals above (3), namely $\mathfrak{p}_\pm = (3, 1 \pm \sqrt{-5})$.

If $\mathfrak{p}_\pm$ would be principal, then the principal generator must divide both 3 and $1 \pm \sqrt{-5}$. As the norm is multiplicative, the norm of the principal generator must divide

$$\gcd(N(3), N(1 \pm \sqrt{-5})) = \gcd(9, 6) = 3.$$

Since

$$N(x + y\sqrt{-5}) = x^2 + 5y^2 = 3 \qquad \text{for } x, y \in \mathbb{Z}$$

has no solutions, $\mathfrak{p}_\pm$ cannot be principal.

But

$$\frac{3}{1 \pm \sqrt{-5}} = \frac{3}{(1 \pm \sqrt{-5})(1 \mp \sqrt{-5})}(1 \mp \sqrt{-5}) = \frac{1 \mp \sqrt{-5}}{2}.$$

Thus if we consider the localised ideal $\mathfrak{p}\mathbb{Z}[\sqrt{-5}, \frac{1}{2}] = (1 \mp \sqrt{-5})$, then it is principal. In fact, one can show that $\mathbb{Z}[\sqrt{-5}, \frac{1}{2}]$ is a principal ideal domain.

Remark: In general, for all square-free $d \in \mathbb{Z}$, there exists some $s \in \mathbb{Z}$ such that $\mathbb{Z}[\sqrt{d}, \frac{1}{s}]$ is a principal ideal domain, which we will show later.

Lemma 2.54. *Let A be a ring, let $\mathfrak{a} \subseteq A$ be an ideal, and let $S \subseteq A$ be a subset. Let $\varphi\colon A \to A[S^{-1}]$ be the localisation, and let $\pi\colon A \to A/\mathfrak{a}$ be the canonical projection map. Then*

$$A/\mathfrak{a}[\pi(S)^{-1}] \cong A[S^{-1}]/\varphi(\mathfrak{a})A[S^{-1}].$$

A common convention is to just write $A[S^{-1}]/\varphi(\mathfrak{a})$ instead of $A[S^{-1}]/\varphi(\mathfrak{a})A[S^{-1}]$ in these situations since it is clear that we mean the ideal in $A[S^{-1}]$ generated by $\varphi(\mathfrak{a})$. One could further drop φ to arrive at $A[S^{-1}]/\mathfrak{a}$.

Proof. Let $\alpha\colon A \to \tilde{A}$ be either of the two ring maps

$$A \to A/\mathfrak{a} \to A/\mathfrak{a}[\pi(S)^{-1}] \qquad \text{or} \qquad A \to A[S^{-1}] \to A[S^{-1}]/\varphi(\mathfrak{a})A[S^{-1}].$$

We observe that $\alpha(\mathfrak{a}) = 0$ and $\alpha(S) \subseteq \tilde{A}^\times$. Furthermore, α has the following universal property: Any ring map $\psi\colon A \to B$ with $\psi(\mathfrak{a}) = 0$ and $\psi(S) \subseteq B^\times$ factors uniquely through α. This follows from applying the universal properties of projections and localisations in the respective order. Hence $\tilde{A}$ is uniquely determined up to unique isomorphism and we obtain the proposed isomorphism.

Alternatively, we could argue more explicitly:

$$\begin{aligned} A/\mathfrak{a}[\pi(S)^{-1}] &= A/\mathfrak{a}[T_{\pi(s)}, \pi(s) \in \pi(S)]/(\pi(s)T_{\pi(s)} - 1, \pi(s) \in \pi(S)) \\ &= A/\mathfrak{a}[T_s, s \in S]/(\pi(s)T_s - 1, s \in S) \\ &\cong A[T_s, s \in S]/((\mathfrak{a}) + (sT_s - 1, s \in S)) \\ &\cong (A[T_s, s \in S]/(sT_s - 1, s \in S))/\varphi(\mathfrak{a})A[S^{-1}] = A[S^{-1}]/\varphi(\mathfrak{a})A[S^{-1}]. \end{aligned}$$

The second line just introduces more variables, if at all, without making more elements invertible. The third and fourth line follow from Noether's isomorphism theorem, noticing

$$\begin{aligned} (\pi(s)T_s - 1, s \in S) &\cong ((\mathfrak{a}) + (sT_s - 1, s \in S))/(\mathfrak{a}), \\ ((\mathfrak{a}) + (sT_s - 1, s \in S))/(sT_s - 1, s \in S) &\cong \varphi(\mathfrak{a})A[S^{-1}]. \end{aligned}$$

□

Proposition 2.55. *Let A be a ring, let $S \subseteq A$ be a subset, and let $\varphi\colon A \to A[S^{-1}]$ be the localisation. Then the following hold:*

(i) $\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(A[S^{-1}]) \to \operatorname{Spec}(A)$ *is injective.*

(ii) *Its image is* $\{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}$.

(iii) *If* $\mathfrak{p} \cap S = \varnothing$, *then* $\operatorname{Spec}(\varphi)^{-1}(\mathfrak{p}) = \varphi(\mathfrak{p})A[S^{-1}]$.

Proof.

(i) We already proved this in Lemma 2.52.

(ii) Let $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ for some $\mathfrak{q} \in \operatorname{Spec}(A[S^{-1}])$. Then $\varphi(\mathfrak{p}) \cap A[S^{-1}]^\times \subseteq \mathfrak{q} \cap A[S^{-1}]^\times = \varnothing$ since prime ideals do not contain units (Lemma 1.25). With $S \subseteq A[S^{-1}]^\times$, it follows that $\mathfrak{p} \cap S = \varnothing$. This shows that the image is in $\{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}$.

Conversely, let $\mathfrak{p} \in \operatorname{Spec}(A)$ with $\mathfrak{p} \cap S = \varnothing$. By Lemma 2.54, we have $A[S^{-1}]/\varphi(\mathfrak{p})A[S^{-1}] \cong A/\mathfrak{p}[\pi(S)^{-1}]$. Since $\mathfrak{p} \cap S = \varnothing$, we have $0 \notin \pi(S)$. Moreover, $A/\mathfrak{p}$ is a domain since $\mathfrak{p}$ is prime (Lemma 2.11). Thus $A/\mathfrak{p}[\pi(S)^{-1}]$ is a subring of $\operatorname{Quot}(A/\mathfrak{p})$, and in particular an integral domain (cf. Example 2.49). Hence $\varphi(\mathfrak{p})A[S^{-1}]$ is a prime ideal.

We now prove that it is a preimage of $\mathfrak{p}$. As $A/\mathfrak{p}$ is an integral domain and $0 \notin \pi(S)$, $\pi(S)$ contains no zero divisor. Hence by Corollary 2.47, $A/\mathfrak{p} \to A/\mathfrak{p}[\pi(S)^{-1}] \cong A[S^{-1}]/\varphi(\mathfrak{p})A[S^{-1}]$ is injective. So we obtain

$$\varphi^{-1}(\varphi(\mathfrak{p})A[S^{-1}]) = \ker(A \to A/\mathfrak{p} \to A[S^{-1}]/\varphi(\mathfrak{p})A[S^{-1}]) = \ker(A \to A/\mathfrak{p}) = \mathfrak{p},$$

i. e. $\varphi(\mathfrak{p}A[S^{-1}])$ is a preimage of $\mathfrak{p}$ under $\operatorname{Spec}(\varphi)$.

(iii) We just showed this. □

Remark 2.56. If $\mathfrak{p} \cap S \neq \varnothing$, then $\varnothing \neq \varphi(\mathfrak{p} \cap S) \subseteq \varphi(S) \subseteq A[S^{-1}]^\times$, hence $\varphi(\mathfrak{p})A[S^{-1}] = A[S^{-1}]$ due to Lemma 1.25 (which is clearly not prime).

The two most common forms of localisation are localising at an element and localising at a prime ideal.

Example 2.57. Let A be a ring, and let $f \in A$ be any element. Applying Proposition 2.55 to the localisation $A \to A[f^{-1}]$ yields

$$\operatorname{Spec}(A[f^{-1}]) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid f \notin \mathfrak{p}\}.$$

Example 2.58. We have

$$\operatorname{Spec}\left(\mathbb{Z}\left[\frac{1}{3 \cdot 5 \cdot 11}\right]\right) = \{(0), (2), (7), (13), (17), (19), \ldots\} = \operatorname{Spec}(\mathbb{Z}) \setminus \{(3), (5), (11)\}.$$

Example 2.59. We have

$$\operatorname{Spec}(\mathbb{C}[X,Y]/(XY)) = \{(X-x,Y),(X,Y-y),(X),(Y) \mid x,y \in \mathbb{C}\}.$$

This can be proved as follows: According to Exercise 8.13, as $\mathbb{C}[X]$ is a principal ideal domain, $\operatorname{Spec}(\mathbb{C}[X,Y]) = \operatorname{Spec}(\mathbb{C}[X][Y])$ consists of

$$\operatorname{Spec}(\mathbb{C}[X,Y]) = \{(0)\} \sqcup \{(f) \mid f \in \mathbb{C}[X,Y] \text{ irreducible}\} \sqcup \{(X-x,Y-y) \mid x,y \in \mathbb{C}\}.$$

The third set above is $\operatorname{MaxSpec}(\mathbb{C}[X,Y])$ according to Exercise 8.14. Due to Example 2.14, $\operatorname{Spec}(\mathbb{C}[X,Y]/(XY))$ consists of all elements in $\operatorname{Spec}(\mathbb{C}[X,Y])$ containing (XY).

We can visualise the situation by Figure 2.1. The prime ideals $(X-x,Y)$ and $(X,Y-y)$ correspond the points $(x,0)$ and $(0,y)$ in $\mathbb{C}^2$, resp. The prime ideals (X) and (Y) are generic points, 'fat' points which are 'smeared' over the whole vertical and horizontal axes, resp.

Passing to $\mathbb{C}[X,Y]/(XY)[X^{-1}]$, we obtain

$$\operatorname{Spec}(\mathbb{C}[X,Y]/(XY)[X^{-1}]) = \{(X-x,Y),(Y) \mid 0 \neq x \in \mathbb{C}\}.$$

This corresponds to deleting the whole vertical axis in Figure 2.1. Conincidentally due to Example 2.51, this spectrum has a one-to-one correspondence with

$$\operatorname{Spec}(\mathbb{C}[X,X^{-1}]) = \{(0),(X-x) \mid 0 \neq x \in \mathbb{C}\}.$$

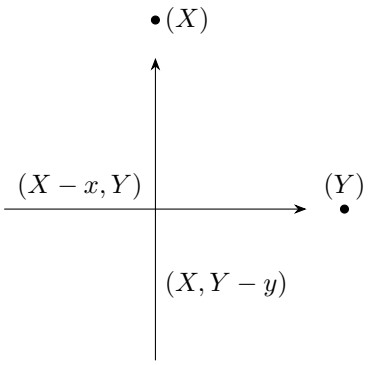


Figure 2.1: Visualisation of $\operatorname{Spec}(\mathbb{C}[X,Y]/(XY))$.

Remark 2.60. Let A be a ring and $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $A \setminus \mathfrak{p}$ is a multiplicative set, as $A/\mathfrak{p}$ is an integral domain (Lemma 2.11).

Definition 2.61. Let A be a ring and $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $A_\mathfrak{p} \coloneqq (A \setminus \mathfrak{p})^{-1}A$ is the **localisation** of A at $\mathfrak{p}$.

Remark 2.62. By Proposition 2.55, we have a bijection

$$\operatorname{Spec}(A_\mathfrak{p}) \leftrightarrow \{\mathfrak{q} \in \operatorname{Spec}(A) \mid \mathfrak{q} \subseteq \mathfrak{p}\}.$$

In particular, $A_\mathfrak{p}$ has a *unique* maximal ideal, namely $\mathfrak{p}A_\mathfrak{p}$, the prime ideal corresponding to $\mathfrak{p} \in \operatorname{Spec}(A)$.

Definition 2.63. A ring A with a unique maximal ideal $\mathfrak{m} \subset A$ is a **local ring**. We call $A/\mathfrak{m}$ the **residue field** of $\mathfrak{m}$.

Notation 2.64. Let A be a ring and $\mathfrak{p} \in \operatorname{Spec}(A)$. We write $\kappa(\mathfrak{p}) \coloneqq A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ for the residue field of $\mathfrak{p}$.

Remark 2.65. By Lemma 2.54, we have $\kappa(\mathfrak{p}) \cong \operatorname{Quot}(A/\mathfrak{p})$, noticing that $\pi(A \setminus \mathfrak{p}) = A/\mathfrak{p} \setminus \{0\}$.

Example 2.66. Consider $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ for some prime $p \in \mathbb{Z}$. Then we have $\kappa(p) = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \operatorname{Quot}(\mathbb{Z}/p) \cong \mathbb{F}_p$ via $\frac{a}{b} \mapsto b^{-1}a$. This map is well defined since $p \nmid b$ for $\frac{a}{b} \in \kappa(p)$ and hence $b^{-1} \in \mathbb{F}_p^\times$.

2.7 Application to Spectra

Problem 2.67. Given a ring map $\varphi\colon A \to B$ and $\operatorname{Spec}(A)$, how do we describe $\operatorname{Spec}(B)$?

Observation 2.68. Our strategy is to consider $\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ and to compute the fibre $\operatorname{Spec}(\varphi)^{-1}(\mathfrak{p})$ for each $\mathfrak{p} \in \operatorname{Spec}(A)$. Then

$$\begin{aligned}\operatorname{Spec}(\varphi)^{-1}(\mathfrak{p}) &= \{\mathfrak{q} \in \operatorname{Spec}(B) \mid \varphi(\mathfrak{p}) \subseteq \mathfrak{q}, \varphi(A \setminus \mathfrak{p}) \cap \mathfrak{q} = \varnothing\} \\ &\cong \{\bar{\mathfrak{q}} \in \operatorname{Spec}(B/(\varphi(\mathfrak{p}))) \mid (\varphi(A \setminus \mathfrak{p})) \cap \bar{\mathfrak{q}} = \varnothing\} \cong \operatorname{Spec}(B/(\varphi(\mathfrak{p}))[\varphi(A \setminus \mathfrak{p})^{-1}]).\end{aligned}$$

The first equality is the set-theoretic condition for $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ to hold. The second equality uses Example 2.14. Note that $\varphi(A\setminus\mathfrak{p})$ and $\mathfrak{q}$ are still disjoint after passing to quotients, for otherwise $\overline{\varphi(s)} = \bar{q}$ with $\varphi(s) \in \varphi(A\setminus\mathfrak{p})$ and $q \in \mathfrak{q}$ implies $\varphi(s) - q \in \varphi(\mathfrak{p})B \subseteq \mathfrak{q}$, so $\varphi(s) \in \mathfrak{q}$, a contradiction. The last equality uses Proposition 2.55.

The bijection is given by the canonical map

$$\pi\colon B \to B/(\varphi(\mathfrak{p})) \to B/(\varphi(\mathfrak{p}))[\varphi(A \setminus \mathfrak{p})^{-1}], \qquad \pi^{-1}(\bar{\mathfrak{q}}) \hookleftarrow \bar{\mathfrak{q}}.$$

Assume for example $B = A[T_1, \dots, T_n]/(f_1, \dots, f_m)$ with $\varphi\colon A \to B$ being the composition of projection after inclusion. Then

$$B/(\varphi(\mathfrak{p}))[\varphi(A \setminus \mathfrak{p})^{-1}] \cong \kappa(\mathfrak{p})[T_1, \dots, T_n]/(f_1, \dots, f_m).$$

(We have $\kappa(\mathfrak{p}) \cong A/\mathfrak{p}[(A\setminus\mathfrak{p})^{-1}]$ via Lemma 2.54. The isomorphism follows from the homomorphism theorem.)

Example 2.69. Our above discussion on $\operatorname{Spec}(B)$ generalises the argument we gave for Proposition 2.28, part (ii) of the proof. There we considered $\varphi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[T]$ and wanted to compute $\operatorname{Spec}(\varphi)^{-1}((0))$. With our new tool applied to $(0) \in \operatorname{Spec}(\mathbb{Z})$, we have $\kappa((0)) \cong \mathbb{Q}$ and thus

$$\operatorname{Spec}(\varphi)^{-1}((0)) = \operatorname{Spec}(\mathbb{Q}[T]) \qquad \text{via} \qquad \mathfrak{q} \cap \mathbb{Z}[T] \hookleftarrow \mathfrak{q}.$$

Similarly for $(p) \in \operatorname{Spec}(\mathbb{Z})$. This gives in total

$$\operatorname{Spec}(\mathbb{Z}[T]) = \operatorname{Spec}(\mathbb{Q}[T]) \sqcup \coprod_{p \text{ prime}} \operatorname{Spec}(\mathbb{F}_p[T]), \qquad \mathfrak{q} \cap \mathbb{Z}[T] \hookleftarrow \mathfrak{q}.$$

In general for any ring A, we have in fact the full description

$$\operatorname{Spec}(A[T]) = \coprod_{\mathfrak{p} \in \operatorname{Spec}(A)} \operatorname{Spec}(\kappa(\mathfrak{p})[T]).$$

Remark 2.70. Caveat: In practice, it might be algorithmically very difficult to compute $\pi^{-1}(\bar{\mathfrak{q}})$ for the map π in Observation 2.68. In the above example and Proposition 2.28, it was quite simple since we had Gauss's lemma, whereas in Example 2.53, what is $(1 \mp \sqrt{-5}) \cdot \mathbb{Z}[\sqrt{-5}, \frac{1}{2}] \cap \mathbb{Z}[\sqrt{-5}]$?

2.8 Appendix: Geometric Intuition

All of this theory in commutative algebra is the entry point to algebraic geometry.

Observation 2.71. Let $X := \mathbb{R}^n$ be the standard euclidean vector space, and let $A := \mathcal{C}^\infty(X, \mathbb{R})$ be the space of all smooth functions on X (a ring with pointwise multiplication). Then we have the map

$$X \to \operatorname{MaxSpec}(A), \qquad x \mapsto \mathfrak{m}_x := \{f \in A \mid f(x) = 0\}.$$

Indeed, $\mathfrak{m}_x$ is maximal since $\kappa(\mathfrak{m}_x) = A/\mathfrak{m}_x \cong \mathbb{R}$ via the ring map $A \to \mathbb{R}$, $f \mapsto f(x)$ and the homomorphism theorem.

Let $f_1, \dots, f_m \in A$. Then we have two operations:

(i) We can take the *vanishing set* $V(f_1, \dots, f_m) = \{x \in X \mid f_1(x) = \cdots = f_m(x) = 0\} =: V$. This is closed since the functions are continuous (every convergent series in V has its limit point in V, as under each f_i, this series converges to 0).

For any $\bar{g} \in A/(f_1, \dots, f_m)$ and $x \in V$, the value $\bar{g}(x) \in \mathbb{R}$ is well-defined: If $\bar{g} = \bar{h}$, then $\bar{g} - \bar{h} \in (f_1, \dots, f_m)$ and thus $(\bar{g} - \bar{h})(x) = \bar{g}(x) - \bar{h}(x) = 0$. Thus $A/(f_1, \dots, f_m)$ forms a ring of functions on V.

(ii) We can take the *does-not-vanish set* $D(f_1, \dots, f_m) = \{x \in X \mid (f_1 \cdots f_m)(x) \neq 0\} =: D$. This is open since the finitely many functions are continuous ($D(f_i) = f_i^{-1}(X \setminus \{0\})$ is open and thus $D = \bigcap_{i=1}^m D(f_i)$).

Since $f_i(x) \neq 0$ for all i and $x \in D$, $A[f_1^{-1}, \dots, f_m^{-1}]$ forms a ring of functions on D.

In general, if A is a ring and $X = \operatorname{Spec}(A)$, we have the same geometric intuition with only two differences:

(i) For each $\mathfrak{p} \in X$, we interpret the 'value of a function' $f \in A$ as its image f mod $\mathfrak{p}$ in $\kappa(\mathfrak{p})$. Of course, $\kappa(\mathfrak{p})$ varies with $\mathfrak{p}$.

(ii) We define X, $V(f_1, \dots, f_m)$ and $D(f_1, \dots, f_m)$ instead by

$$X \coloneqq \operatorname{Spec}(A), \quad V(f_1, \dots, f_m) \coloneqq \operatorname{Spec}(A/(f_1, \dots, f_m)), \quad D(f_1, \dots, f_m) \coloneqq \operatorname{Spec}(A[f_1^{-1}, \dots, f_m^{-1}]).$$

3 Modules

Lect. 6
24.04.23

We introduce *modules*, which serve as a generalisation of vector spaces. As they are defined over a ring as opposed to over a field, they have much more applications in commutative algebra and in other algebraic disciplines.

3.1 Definition and Examples

For this subsection, see [AtMac, ch. 2].

Definition 3.1. Let A be a ring. An **A-module** is an (additive) abelian group M together with a ring homomorphism $A \to \operatorname{End}_{\mathrm{AbGrp}}(M)$.

Or equivalently (and more intuitively), we have an A-action $\bullet\colon A \times M \to M$ on M such that for all $a, b \in A$ and $x, y \in M$, the following laws hold:

(i) $a \bullet (x + y) = a \bullet x + a \bullet y$.

(ii) $(a + b) \bullet x = a \bullet x + b \bullet x$.

(iii) $(ab) \bullet x = a \bullet (b \bullet x)$.

(iv) $1 \bullet x = x$.

Remark 3.2. Let $\varphi\colon A \to \operatorname{End}_{\mathrm{AbGrp}}(M)$. The first law originates from the images of φ being group homomorphisms. The other laws are the additivity, multiplicativity and identity of φ.

Example 3.3.

(i) For fields k, the k-modules are precisely the k-vector spaces because their definitions are identical.

(ii) Definition 3.1 (ii) and (iv) imply that $n \bullet x = (1 + \cdots + 1) \bullet x = x + \cdots + x$ for all $n \geq 1$ and $x \in M$. Similar to vector spaces, we have $0 \bullet x = 0$ and $-1 \bullet x = -x$, thus $-n \bullet x = -x + \cdots + (-x)$ for all $n \geq 1$ and $x \in M$.

With the above definition, the $\mathbb{Z}$-modules are precisely all abelian groups. Furthermore, since there always exists a ring map $\mathbb{Z} \to A$ for any ring A, every A-module M is naturally also a $\mathbb{Z}$-module.

Definition 3.4.

(i) A **A-submodule** of an A-module M is a subgroup $N \subseteq M$ such that

$$a \bullet x \in N \qquad \text{for all } a \in A \text{ and } x \in N.$$

(ii) If $N \subseteq M$ is a submodule, the quotient group M/N becomes an A-module via

$$a \bullet (x + N) \coloneqq a \bullet x + N \qquad \text{for all } a \in A \text{ and } x \in M,$$

the so called **quotient A-module** of M over N.

Remark 3.5. Notice that we do not have to require that N is a normal subgroup of M since M is abelian, so any subgroup is already normal.

Furthermore, the multiplication in the quotient module is well-defined: For $x + N = y + N$, we have $x - y \in N$. Thus $a(x - y) = ax - ay \in N$ and hence $ax + N = ay + N$ for all $a \in A$.

Example 3.6.

(i) Trivially, any ring A is itself an A-module via its left-multiplication $a \bullet b \coloneqq ab$. The submodules of A are precisely the ideals of A. For ideals $\mathfrak{a} \subseteq A$, the quotient ring $A/\mathfrak{a}$ is also the A-quotient module.

(ii) If $\varphi\colon A \to B$ is a ring map, then B becomes an A-module via $a \bullet b \coloneqq \varphi(a)b$.

Definition 3.7. Let M and N be two A-modules.

(i) An **A-module map** (or **A-module homomorphism** or **A-linear map**) from M to N is a group homomorphism $f\colon M \to N$ such that

$$f(a \bullet x) = a \bullet f(x) \qquad \text{for all } a \in A \text{ and } x \in M.$$

We call f an **A-module isomorphism** if f is bijective. In this case, we write $M \cong N$.

(ii) We denote the set of all A-module maps $f\colon M \to N$ as $\mathrm{Hom}_A(M, N)$, which is again an A-module via $(a \bullet f)(x) \coloneqq a \bullet f(x)$.

(iii) Let $f \in \mathrm{Hom}_A(M, N)$. Then the subgroups $\ker(f) \subseteq M$ and $\mathrm{im}(f) \subseteq N$ are submodules. The **cokernel**

$$\mathrm{coker}(f) \coloneqq N/\mathrm{im}(f)$$

is a quotient module.

Definition 3.8. Let I be an arbitrary index set and $(M_i)_{i\in I}$ a tuple of A-modules. Then the abelian groups

$$\bigoplus_{i\in I} M \qquad \text{and} \qquad \prod_{i\in I} M_i$$

form A-modules via

$$a \bullet (x_i)_{i\in I} \coloneqq (a \bullet x_i)_{i\in I} \qquad \text{for all } a \in A \text{ and } (x_i)_{i\in I}.$$

Notation 3.9. From now on, we will drop the multiplication sign $\bullet$ if it is clear which multiplication we mean. Sometimes, we will also write $\cdot$ instead of $\bullet$.

The following concept is the analogue to basis in vector spaces.

Definition 3.10.

(i) An A-module M is called **free** if there exists a set I and an isomorphism

$$M \cong A^{\oplus I} \coloneqq \bigoplus_{i\in I} A.$$

(ii) A tuple $(m_i)_{i\in I} \in \prod_{i\in I} M$ is a **basis** of M if there exists an isomorphism $A^{\oplus I} \to M$, $e_i \mapsto m_i$.

Or equivalently, every $x \in M$ is a *unique* A-linear combination of the $(m_i)_{i\in I}$, i. e. there exists a *unique* $(a_i)_{i\in I} \in \bigoplus_{i\in I} A$ such that

$$x = \sum_{i\in I} a_i x_i.$$

Remark 3.11. Let M be any A-module. Then

$$\mathrm{Hom}_A(A^{\oplus I}, M) \cong \prod_{i\in I} M, \qquad f \mapsto (f(e_i))_{i\in I},$$

where $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ has 1 at the ith position. The e_i form a basis of $A^{\oplus I}$. (This is clearly A-linear, and we have $f((a_i)_{i\in I}) = \sum_{i\in I} a_i f(e_i) \in M$, i. e. f is uniquely determined by $(f(e_i))_{i\in I}$. Notice in the sum that $a_i \neq 0$ for only finitely many $i \in I$.)

Remark 3.12. By generalising to A-modules, we lose some nice properties of bases in k-vector spaces.

(i) Every vector space has a basis.

For example, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ with $n \geq 1$ is not free: If e_1 corresponds to $x \in \mathbb{Z}/n\mathbb{Z}$, then $ne_1 \neq 0 = nx$. But $\mathbb{Z}/n\mathbb{Z}$ would be trivially free as a $\mathbb{Z}/n\mathbb{Z}$-module.

(ii) In any vector space, every maximal set of linearly independent elements forms a basis.

For example in the $\mathbb{Z}$-module $\mathbb{Z}$, the element $2 \in \mathbb{Z}$ is maximal linearly independent since for any $a \in \mathbb{Z}$, the set $\{2, a\}$ is linearly dependent as $a \bullet 2 - 2 \bullet a = 0$. But 2 does not generate $\mathbb{Z}$.

(iii) In any vector space, every minimal set of generating elements forms a basis.

For example in the $\mathbb{Z}$-module $\mathbb{Z}$, $\{2, 3\}$ is a minimal generating set since $-1 \bullet 2 + 1 \bullet 3 = 1$ and neither 2 nor 3 generate $\mathbb{Z}$. But $\{2, 3\}$ is not linearly independent as $3 \bullet 2 + (-2) \bullet 3 = 0$.

Remark 3.13. Similar to vector spaces, we can express any map between free modules as a matrix. For any ring A, it is true that

$$\operatorname{Hom}_A(A^{\oplus m}, A^{\oplus n}) \cong M_{n\times m}(A), \qquad \left[e_j \mapsto \sum_{i=1}^{n} a_{ij} e_i\right] \leftarrow\!\shortmid (a_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,m}}.$$

The composition of A-linear maps $A^{\oplus m} \to A^{\oplus n}$ is the usual product of matrices.

Example 3.14. Consider $A = k[X, Y]$ and the ideal $M \coloneqq (X, Y) \subseteq A$. Then $A/M \cong k$. We consider the surjective A-module map

$$\begin{pmatrix} X & Y \end{pmatrix} \colon A^{\oplus 2} \to M, \qquad \begin{pmatrix} f \\ g \end{pmatrix} \mapsto \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = Xf + Yg.$$

What is its kernel? For that we need to solve $Xf + Yg = 0$ with $f, g \in A$. Since X and Y are prime elements and $X \nmid Y$, $Y \nmid X$, we need $f = Yf'$ and $g = Xg'$ for some $f', g' \in A$. This yields $XY(f' + g') = 0$, or equivalently $f' = -g'$ since $XY \neq 0$ in the integral domain A. In conclusion, we have the surjective A-module map

$$\begin{pmatrix} -Y \\ X \end{pmatrix} \colon A \to \ker(\begin{pmatrix} X & Y \end{pmatrix}), \qquad f \mapsto \begin{pmatrix} -Yf \\ Xf \end{pmatrix}.$$

Since X and Y not zero divisors, this map is injective. Hence the $\ker(\begin{pmatrix} X & Y \end{pmatrix}) \cong A$ is a free A-module of rank 1 (*rank* is the cardinality of the basis of a free module).

Example 3.15. Let A be a ring and $0 \neq \mathfrak{a} \subset A$ an ideal. Then $A/\mathfrak{a}$ is never a free A-module: Let $0 \neq a \in \mathfrak{a}$. Then $a \bullet A/\mathfrak{a} = 0$, but $a \bullet (A^{\oplus I}) = (a \bullet A)^{\oplus I} \neq 0$ for any set I.

3.2 Finiteness Properties

See [AtMac, ch. 6].

Definition 3.16. Let M be an A-module, and let $U \subseteq M$ be a subset. Then the **submodule generated by** U is

$$(U) \coloneqq \bigcap_{\substack{U\subseteq N\subseteq M \\ N \text{ submodule}}} N.$$

(U) consists of A-linear combinations of elements from U, i. e. $(U) = \operatorname{im}(A^{\oplus U} \to M, e_u \mapsto u)$.

Definition 3.17. Let M be an A-module.

(i) M is of **finite type** or **finitely generated**, if $M = (x_1, \dots, x_n)$ for some $n \geq 0$ and $x_1, \dots, x_n \in M$.
Or equivalently, there exists some $n \geq 0$ and an A-linear surjection $\varphi \colon A^{\oplus n} \to M$.

(ii) If M is finitely generated with an A-linear surjection $\varphi\colon A^{\oplus n} \to M$ such that $\ker(\varphi) \subseteq A^{\oplus n}$ is also finitely generated, then M is of **finite presentation** or **finitely presented**.

Or equivalently, any module M is of finite presentation if there exist $m, n \geq 0$ and an A-module map $f\colon A^{\oplus m} \to A^{\oplus n}$ such that $M \cong \operatorname{coker}(f)$.

Remark 3.18. (From me.) The definitions for finite presentation are indeed equivalent.

Given the surjection $\varphi\colon A^{\oplus n} \to M$ with finitely generated $\ker(\varphi) = (x_1, \dots, x_m)$, we can naturally define $f\colon A^{\oplus m} \to A^{\oplus n}$, $e_i \mapsto x_i$. Then $\operatorname{im}(f) = \ker(\varphi)$ and thus by the homomorphism theorem for groups, $\operatorname{coker}(f) = A^{\oplus n}/\ker(\varphi) \cong M$, which also induces an isomorphism between A-modules.

Conversely, given $f\colon A^{\oplus m} \to A^{\oplus n}$ such that $M \cong \operatorname{coker}(f)$, we define the canonical projection map $\varphi\colon A^{\oplus n} \to \operatorname{coker}(f) \cong M$. This is surjective, thus M is finitely generated. Furthermore, we have the surjective restriction $f\colon A^{\oplus m} \to \operatorname{im}(f) = \ker(\varphi)$, hence $\ker(\varphi)$ is finitely generated.

Remark 3.19. A-modules M of finite presentation are the modules we may study by their map $f\colon A^{\oplus m} \to A^{\oplus n}$, which is in fact a finite matrix $f \in M_{n\times m}(A)$. This makes them much more accessible.

Example 3.20. As we showed in Example 3.14, (X, Y) is a finitely presented $k[X, Y]$-module, since the kernel of the A-linear surjection $\begin{pmatrix} X & Y \end{pmatrix}\colon A^{\oplus 2} \to M$ is finitely generated. More precisely, we showed $(X, Y) \cong \operatorname{coker}(\begin{pmatrix} -Y \\ X \end{pmatrix}\colon A \to A^{\oplus 2})$.

Example 3.21. Let A be a ring, which is a finitely generated A-module. If an ideal $\mathfrak{a} \subset A$ is not finitely generated, then the A-module $A/\mathfrak{a}$ is finitely generated, but not of finite presentation. E. g. take $\mathfrak{a} = (T_1, T_2, \dots) \subseteq A = k[T_1, T_2, \dots]$. Then $A/\mathfrak{a}$ is finitely generated via the A-module map $A \twoheadrightarrow A/\mathfrak{a}$, but its kernel $\mathfrak{a}$ is not finitely generated (no variable can be expressed as an A-linear combination of the other variables as $1 \notin \mathfrak{a}$).

Definition 3.22. An A-module M is **noetherian**, if one of the following two equivalent conditions are satisfied:

(i) Any ascending chain of submodules $N_1 \subseteq N_2 \subseteq \cdots \subseteq M$ becomes stationary.

(ii) Any submodule $N \subseteq M$ is finitely generated.

Proof. Let $N \subseteq M$ be an arbitrary submodule. We define an ascending chain of submodules in N by $N_0 \coloneqq 0$, and $N_i \coloneqq N_{i-1} + (x_i)$ if $x_i \in N \setminus N_{i-1}$ exists, and $N_i \coloneqq N_{i-1}$ otherwise. By assumption, $N_0 \subseteq N_1 \subseteq \cdots \subseteq N$ stabilises. We choose k to be minimal with $N_k = N_{k+1} = \cdots = N$. Then $N = (x_1, \dots, x_k)$.

Conversely, let $N_1 \subseteq N_2 \subseteq \cdots$ be any chain. By assumption, the submodule $N \coloneqq \bigcup_{i\geq 1} N_i$ is finitely generated, say by $x_1, \dots, x_r$. We choose k such that $x_1, \dots, x_r \in N_k$. Then we have $N_k = N_{k+1} = \cdots = N$. □

Definition 3.23. A ring A is **noetherian** if it is noetherian viewed as an A-module. This means that every ideal $\mathfrak{a} \subseteq A$ is finitely generated, or equivalently, any chain of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A$ stabilises.

Proposition 3.24. *Let M be an A-module, $K \subseteq M$ a submodule and $Q \coloneqq M/K$ a quotient. Then we have:*

(i) *If M is noetherian, then K and Q are noetherian.*

(ii) *If K and Q are noetherian, then M is noetherian.*

Proof.

(i) For K, any submodule of K is a submodule of M, which is finitely generated by definition.

For Q, let $N \subseteq Q$ be any submodule. Let $q\colon M \twoheadrightarrow Q$ be the canonical projection. By assumption, $q^{-1}(N)$, which is a submodule, is finitely generated by say $x_1, \dots, x_r$, and we have $N = (q(x_1), \dots, q(x_r))$ (note that q is surjective).

(ii) Let $N \subseteq M$ be any submodule. By assumption, $K \cap N$ and $q(N)$, which are submodules, are finitely generated, say $K \cap N = (x_1, \dots, x_r)$ and $q(N) = (y_1, \dots, y_s)$. Now we choose any lifts $\tilde{y}_1, \dots, \tilde{y}_s \in N$ of the $y_1, \dots, y_s$. We claim that $N = (x_1, \dots, x_r, \tilde{y}_1, \dots, \tilde{y}_s)$.

Let $z \in N$ be arbitrary. Then we can write $q(z) = a_1 y_1 + \cdots + a_s y_s$ with $a_1, \dots, a_s \in A$. This means $z' \coloneqq z - \sum_{i=1}^{s} a_i \tilde{y}_i \in \ker(q) \cap N = K \cap N$. Then we can write $z' = b_1 x_1 + \cdots + b_r x_r$ for some $b_1, \dots, b_r \in A$ and we are done. □

Corollary 3.25. *Let A be a noetherian ring and M an A-module of finite type. Then M is noetherian.*

Proof. For any $n \geq 1$, $A^{\oplus n-1} \cong A^{\oplus n}/(0^{n-1} \oplus A)$ generally holds. By Proposition 3.24 and induction ($0^{n-1} \oplus A$ and $A^{\oplus n-1}$ are noetherian), $A^{\oplus n}$ is a noetherian A-module for all $n \geq 0$. As M is finitely generated, there exists some n and an A-linear surjection $\varphi\colon A^{\oplus n} \twoheadrightarrow M$. Again by Proposition 3.24, $M \cong A^{\oplus n}/\ker(\varphi)$ is noetherian, using the homomorphism theorem for A-modules. □

Corollary 3.26. *Let A be a noetherian ring and M an A-module. Then M is finitely generated if and only if M is finitely presented.*

Proof. If M is finitely generated, choose any A-linear surjection $f\colon A^{\oplus n} \twoheadrightarrow M$. Since $A^{\oplus n}$ is noetherian, $\ker(f)$ is finitely generated and M is finitely presented. □

Example 3.27. Some examples of non-noetherian rings.

(i) $k[T_1, T_2, \dots]$ is not noetherian, as $(T_1, T_2, \dots)$ is not finitely generated.

(ii) Consider $\mathbb{Z}[p^{1/2}, p^{1/4}, p^{1/8}, p^{1/16}, \dots] \subseteq \mathbb{R}$ for some prime $p \in \mathbb{Z}$. Then $(p^{1/2}) \subset (p^{1/4}) \subset (p^{1/8}) \subset \cdots$ does not stabilize, so this ring is not noetherian. In particular, $(p^{1/2}, p^{1/4}, p^{1/8}, \dots)$ is not finitely generated.

(iii) Consider $A = \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$, the ring of smooth functions. Then $\mathfrak{a}_n = \{f \in A \mid f|_{[-1/n,1/n]} \equiv 0\}$ for all $n \geq 1$ are ideals. Thus $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ does not stabilise, and A is not noetherian. In particular, $\mathfrak{a} = \bigcup_{n\geq 1} \mathfrak{a}_n$ is not finitely generated.

3.3 Noetherian Rings

Lect. 7
27.04.23

See [AtMac, ch. 7].

Proposition 3.28. *Let A be a noetherian ring. Then the following hold:*

(i) *Any quotient ring $A/\mathfrak{a}$ with an ideal $\mathfrak{a} \subseteq A$ is noetherian.*

(ii) *Any localisation $A[S^{-1}]$ with a subset $S \subseteq A$ is noetherian.*

Proof. Any ideal in $A/\mathfrak{a}$ (resp. $A[S^{-1}]$) is of the form $\mathfrak{b}/\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$ (resp. $\mathfrak{b}A[S^{-1}]$ for some ideal $\mathfrak{b} \subseteq A$, since $\mathfrak{b} \mapsto \mathfrak{b}A[S^{-1}]$ is surjective, see Lemma 2.52). Since $\mathfrak{b}$ is finitely generated by assumption, $\mathfrak{b}/\mathfrak{a}$ (resp. $\mathfrak{b}A[S^{-1}]$) is finitely generated. Hence $A/\mathfrak{a}$ (resp. $A[S^{-1}]$) is noetherian. □

Example 3.29. Let A be non-noetherian, and $\mathfrak{a} \subseteq A$ be non-finitely generated. This defies our intuition about vector spaces: $\mathfrak{a}$ is not finitely generated, but $A = (1)$ is.

Theorem 3.30 (Hilbert's basis theorem). *If A is a noetherian ring, then $A[T]$ is also noetherian.*

This applies in particular to principal ideal domains A.

Proof. Let $\mathfrak{a} \subseteq A[T]$ be any ideal. Then consider the ideal

$$\mathfrak{b} \coloneqq \{a \in A \mid \text{there exists } f = aT^n + \cdots \in \mathfrak{a}\} \subseteq A,$$

which is finitely generated by assumption, say $\mathfrak{b} = (a_1, \dots, a_r)$. For each $i = 1, \dots, r$, we pick $f_i = a_i T^{n_i} + \cdots \in \mathfrak{a}$. Put $n \coloneqq \max\{n_1, \dots, n_r\}$. We claim that for every $g \in \mathfrak{a}$, there exist $h, h_1, \dots, h_r \in A[T]$ such that $g = h_1 f_1 + \cdots + h_r f_r + h$ and $\deg(h) < n$.

If $\deg(g) < n$, we can put $h_1 = \cdots = h_r = 0$ and $h = g$. Otherwise, let $g = bT^m + \cdots$. Since $b \in \mathfrak{b}$, we can write $b = x_1 a_1 + \cdots + x_r a_r$ with $x_i \in A$. Then set $g' \coloneqq g - \sum_{i=1}^r x_i T^{m-n_i} f_i$, which satisfies $g' \in \mathfrak{a}$ and $\deg(g') < \deg(g)$. Now we continue with g', i. e. the claim follows by induction on $\deg(g)$.

Now consider the A-submodule $M = \bigoplus_{i=0}^{n-1} AT^i \subseteq A[T]$. It is apparently finitely generated (we even have $M \cong A^{\oplus n}$). The claim shows that $\mathfrak{a} = (f_1, \dots, f_r) + (M \cap \mathfrak{a})$ holds true. As A is noetherian, $M \cap \mathfrak{a} = (g_1, \dots, g_s)$ is finitely generated as an A-module (Corollary 3.25). Finally, $\mathfrak{a} = (f_1, \dots, f_r, g_1, \dots, g_s)$. □

Corollary 3.31. *Let A be a noetherian ring. Then any ring of the form $A[T_1, \dots, T_n]/\mathfrak{a}$ with any ideal $\mathfrak{a} \subseteq A[T_1, \dots, T_n]$ is noetherian. Moreover, $\mathfrak{a}$ is finitely generated.*

Proof. Using $A[T_1, \dots, T_n] \cong A[T_1, \dots, T_{n-1}][T_n]$ and induction, Hilbert's basis theorem 3.30 says that $A[T_1, \dots, T_n]$ is noetherian. Thus $\mathfrak{a}$ is finitely generated. By Proposition 3.28, $A[T_1, \dots, T_n]/\mathfrak{a}$ is also noetherian. □

Remark 3.32. The argument in Hilbert's basis theorem 3.30 also shows that if A is noetherian, then $A[\![T]\!]$ is noetherian (Exercise 8.17).

3.4 Matrices

Recall: For any ring A, it is true that

$$\mathrm{Hom}_A(A^m, A^n) \cong M_{n\times m}(A), \qquad f \mapsto (f(e_1), \dots, f(e_m)),$$

where the $f(e_i) \in A^n$ are column vectors. In particular, $\mathrm{End}_A(A^n) \cong M_n(A)$.

Definition 3.33. Let A be a ring. Then

$$\mathrm{GL}_n(A) \coloneqq M_n(A)^\times = \{S \in M_n(A) \mid \text{there exists } T \in M_n(A) \text{ such that } ST = 1_n\} = \mathrm{Aut}_{A\text{-Mod}}(A^n)$$

is the **general linear group** over A of degree n.

Definition 3.34. Using identical definitions as in linear algebra, for any $S \in M_n(A)$, we define the **determinant**, **trace** and **characteristic polynomial** as

$$\det(S) \in A, \qquad \mathrm{tr}(S) \in A, \qquad \mathrm{char}(S, X) \coloneqq \det(X1_n - S) \in A[X].$$

Furthermore, these are $\mathrm{GL}_n(A)$-conjugation invariant, i. e. for all $S \in M_n(A)$ and $T \in \mathrm{GL}_n(A)$, we have

$$\det(TST^{-1}) = \det(S), \qquad \mathrm{tr}(TST^{-1}) = \mathrm{tr}(S), \qquad \mathrm{char}(TST^{-1}, X) = \mathrm{char}(S, X).$$

This is identical to matrices over fields $A = k$, since $\mathrm{GL}_n(A)$-conjugation is essentially a change of basis.

Lemma 3.35. *Let A be a ring. Then $S \in M_n(A)$ is invertible if and only if $\det(S) \in A^\times$.*

Proof. This proof works identical to the proof for fields. We observe that the only difference between rings and fields is that not every non-zero element is invertible.

Suppose that $S \in M_n(A)^\times$, i. e. $ST = 1_n$ for some $T \in M_n(A)$, then $\det(S)\det(T) = \det(1_n) = 1$.

(Here a proof for why the determinant is multiplicative over any ring. Our strategy is similar to the strategy for the Cayley-Hamilton theorem 8.19 over any ring.

Let $n \geq 1$, let $B = \mathbb{Z}[S_{ij}, T_{ij} \mid 1 \leq i, j \leq n]$, and define $S' \coloneqq (S_{ij})_{ij}, T' \coloneqq (T_{ij})_{ij} \in M_n(B)$. Since B is an integral domain, there exists the canonical embedding $B \hookrightarrow \mathrm{Quot}(B)$. We know from liner algebra that $\det(S'T') = \det(S')\det(T')$ holds in the field $\mathrm{Quot}(B)$. But this calculation does not involve fractions (the embedding maps $S' \mapsto S'$ and $T' \mapsto T'$), so this also holds in B.

Now let $S = (s_{ij})_{ij}, T = (t_{ij})_{ij} \in M_n(A)$. There always exists a ring map $\mathbb{Z} \to A$. Thus by the universal property of polynomial rings, there exists the evaluation map $B \to A$ given by $S_{ij} \mapsto s_{ij}$ and $T_{ij} \mapsto t_{ij}$. Evaluating $\det(S'T') = \det(S')\det(T')$ in B gives $\det(ST) = \det(S)\det(T)$ in A.)

For the converse, we construct the **adjoint matrix** $\hat{S} = (t_{ij})$ through $t_{ij} \coloneqq (-1)^{i+j}\det(S_{ji})$, where S_{ji} arises from S by cancelling the jth row and ith column. The point is that the definition of $\hat{S}$ does not involve any inverses of elements. Then we can check that $\hat{S}S = \det(S)1_n$, which requires purely algebraic manipulation. Thus if $\det(S) \in A^\times$, then $\det(S)^{-1}\hat{S} \in M_n(A)^\times$ is the inverse of S. □

Remark 3.36. For an ideal $\mathfrak{a} \subseteq A$ and an A-module M, we define the submodule

$$\mathfrak{a}M \coloneqq (am \mid a \in \mathfrak{a}, m \in M) \subseteq M.$$

If $f\colon N \to M$ is an A-linear map, then it restricts to $f|_{\mathfrak{a}N}\colon \mathfrak{a}N \to \mathfrak{a}M$ since $f(an) = af(n) \in \mathfrak{a}M$ for all $an \in \mathfrak{a}N$. So this construction is compatible with any f. Therefore if f is surjective, then we obtain the following commutative diagram:

$$\begin{array}{ccc} N & \xrightarrow{f} & M \\ \downarrow & & \downarrow \\ N/\mathfrak{a}N & \xrightarrow{\bar{f}} & M/\mathfrak{a}M \end{array}$$

Hence $\bar{f}\colon n + \mathfrak{a}N \mapsto f(n) + \mathfrak{a}M$ is also surjective. ($\bar{f}$ is well-defined since $f|_{\mathfrak{a}N}(\mathfrak{a}N) \subseteq \mathfrak{a}M$.)

Corollary 3.37. *Let $A \neq 0$ be a ring and $f\colon A^m \twoheadrightarrow A^n$ an A-linear surjection. Then $m \geq n$. In particular, we have $A^m \cong A^n$ if and only if $m = n$.*

Proof. Let $\mathfrak{m} \subset A$ be a maximal ideal, which exists due to Krull's theorem 2.18, and set $\kappa(\mathfrak{m}) \coloneqq A/\mathfrak{m}$ to be its residue field. Then $\mathfrak{m}^m \subseteq A^m$ is a submodule, and $A^m/\mathfrak{m}^m = \kappa(\mathfrak{m})^m$. The same applies to $A^n/\mathfrak{m}^n$. Set $\bar{f} \coloneqq f \bmod \mathfrak{m}\colon \kappa(\mathfrak{m})^m \to \kappa(\mathfrak{m})^n$. By Remark 3.36, $\bar{f}$ is a surjective map of $\kappa(\mathfrak{m})$-vector spaces, and thus $m \geq n$ according to linear algebra.

The second claim assumes that $f\colon A^m \to A^n$ is an isomorphism. Applying the above result to $f^{-1}\colon A^n \to A^m$ additionally yields $n \geq m$. □

Recall the following definition from linear algebra.

Definition 3.38. An **$(k \times k)$-minor** of $S \in M_{n\times m}(A)$ is a $(k \times k)$-matrix which is obtained by deleting $n - k$ rows and $m - k$ columns. We denote the $(k \times k)$-minor $(s_{ij})_{i\in I, j\in J}$ with rows $I \subseteq \{1, \dots, n\}$ and columns $J \subseteq \{1, \dots, m\}$ by $S_{I,J}$, where $|I| = |J| = k$.

Corollary 3.39. *Let $S\colon A^m \to A^n$ be an A-linear map and $I(S) \coloneqq (\det(S_{I,J}) \mid |I| = |J| = n)$. If S is surjective, then $I(S) = A$.*

Proof. As $A = 0$ is trivial, let $A \neq 0$. Similar to Corollary 3.37, let $\mathfrak{m} \subset A$ be a maximal ideal so that $\bar{S} \coloneqq S \bmod \mathfrak{m}\colon \kappa(\mathfrak{m})^m \to \kappa(\mathfrak{m})^n$ is a surjective map of $\kappa(\mathfrak{m})$-vector spaces, which gives $m \geq n$. From linear algebra, we know that $\operatorname{im}(\bar{S})$ contains a basis of $\kappa(\mathfrak{m})^n$. Thus there exists an $(n \times n)$-minor $S_{I,J}$ of $\bar{S} \in M_{n\times m}(\kappa(\mathfrak{m}))$ which is invertible. By Lemmas 3.35 and 1.25, it follows that $\det(S_{I,J}) \notin \mathfrak{m}$ and thus $I(S) \not\subset \mathfrak{m}$. Since this holds for any $\mathfrak{m}$, it must be $I(S) = A$ by Corollary 2.19. □

Remark 3.40. The converse also holds true: If $I(S) = A$, then A is surjective. We will discuss this in Corollary 4.62.

Example 3.41. This holds in the special case $n = 1$: Let $f\colon A^m \to A$, $e_i \mapsto f_i$ be an A-linear map. Then f is surjective if and only if $(f_1, \dots, f_m) = A$.

3.5 The Elementary Divisor Theorem

Lemma 3.42. *Let A be a ring, and let $S, T \in M_{n\times m}(A)$. Assume that there are $L \in \mathrm{GL}_n(A)$, $R \in \mathrm{GL}_m(A)$ such that $LSR = T$. Then L and R induce isomorphisms*

$$R|_{\ker(T)}\colon \ker(T) \to \ker(S) \qquad \text{and} \qquad \bar{L} \coloneqq L \bmod \operatorname{im}(T)\colon \operatorname{coker}(S) \to \operatorname{coker}(T).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccc} M_1 & \xrightarrow{f_1} & N_1 \\ {\scriptstyle g_1}\downarrow & & \downarrow{\scriptstyle g_2} \\ M_2 & \xrightarrow{f_2} & N_2 \end{array}$$

Necessarily by commutativity, $g_1(\ker(f_1)) \subseteq \ker(f_2)$ and $g_2(\operatorname{im}(f_1)) \subseteq \operatorname{im}(f_2)$. (For all $x \in \ker(f_1)$, we have $(g_2 \circ f_1)(x) = 0 = (f_2 \circ g_1)(x)$ and thus $g_1(x) \in \ker(f_2)$. For all $x \in M_1$, we have $(g_2 \circ f_1)(x) = (f_2 \circ g_1)(x)$ and

thus $(g_2 \circ f_1)(x) \in \operatorname{im}(f_2)$.) Thus we can extend the above commutative diagram by the following maps, which are well-defined (they are actually unique):

$$\begin{array}{ccccccc} & & \ker(f_1) & \longrightarrow & M_1 & \xrightarrow{f_1} & N_1 & \longrightarrow & \operatorname{coker}(f_1) \\ & & \downarrow{\scriptstyle g_1|_{\ker(f_1)}} & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_2 \bmod \operatorname{im}(f_1)} \\ & & \ker(f_2) & \longrightarrow & M_2 & \xrightarrow{f_2} & N_2 & \longrightarrow & \operatorname{coker}(f_2) \end{array}$$

If g_1 and g_2 are isomorphisms, we can do the same in the other direction with g_1^{-1} and g_2^{-1}. This yields

$$\begin{array}{ccccccc} & & \ker(f_1) & \longrightarrow & M_1 & \xrightarrow{f_1} & N_1 & \longrightarrow & \operatorname{coker}(f_1) \\ & & \uparrow{\scriptstyle g_1^{-1}|_{\ker(f_2)}} & & \uparrow{\scriptstyle g_1^{-1}} & & \uparrow{\scriptstyle g_2^{-1}} & & \uparrow{\scriptstyle g_2^{-1} \bmod \operatorname{im}(f_2)} \\ & & \ker(f_2) & \longrightarrow & M_2 & \xrightarrow{f_2} & N_2 & \longrightarrow & \operatorname{coker}(f_2) \end{array}$$

Thus $g_1|_{\ker(f_1)}$ and $g_2 \bmod \operatorname{im}(f_1)$ are isomorphisms.

Now we apply this to

$$\begin{array}{ccc} A^m & \xrightarrow{S} & A^n \\ {\scriptstyle R^{-1}}\downarrow & & \downarrow{\scriptstyle L} \\ A^m & \xrightarrow{T} & A^n \end{array}$$

(From me.) An alternative: We shall call $\iota_S \colon \ker(S) \to A^m$ and $\iota_T \colon \ker(T) \to A^m$.

By definition of the kernel, $T \circ \iota_T$ is a zero map, i. e. prepending (resp. appending) $T \circ \iota_T$ with two different maps yields the same map 0. Thus $L^{-1} \circ T \circ \iota_T$ is a zero map. Since the middle square commutes, $S \circ R \circ \iota_T$ is also a zero map. But ι_S is the kernel of S, hence by the universal property of the kernel, there is a unique map $f \colon \ker(T) \to \ker(S)$ such that the left square commutes.

By a similar argument, we obtain another map $g \colon \ker(S) \to \ker(T)$. As the left square commutes, it is true that $\iota_S = R \circ \iota_T \circ g = R \circ (R^{-1} \circ \iota_S \circ f) \circ g = \iota_S \circ f \circ g$. Since ι_S is a monomorphism, we have $f \circ g = \mathrm{id}_{\ker(S)}$. We obtain $g \circ f = \mathrm{id}_{\ker(T)}$ in a similar way, thus $g = f^{-1}$ are isomorphisms. Finally, $f = R|_{\ker(T)}$ as f is unique.

The isomorphism $\bar{L}$ in the right square follows dually.

(Also from me.) Alternatively, we observe that $\ker(T) = \ker(L^{-1}T) = \ker(SR) \cong \ker(S)$ since L and R are isomorphisms and $LSR = T$. Similarly, $\operatorname{coker}(T) = \operatorname{coker}(TR^{-1}) = \operatorname{coker}(LS) \cong \operatorname{coker}(S)$. Looking at the isomorphisms, we immediately see that they are induced by R and L, resp. □

Thus to a degree, we can classify finitely presented A-modules up to isomorphism by classifying the double cosets

$$\mathrm{GL}_n(A) \backslash M_{n \times m}(A) / \mathrm{GL}_m(A)$$

for given $m, n \geq 0$.

Definition 3.43. Let A be a ring. We call two matrices $S, S' \in M_{n \times m}(A)$ **equivalent** if there exist $L \in \mathrm{GL}_n(A)$ and $R \in \mathrm{GL}_m(A)$ such that $S' = LSR$. In this case, we write $S \sim S'$.

Before we come to the main part of this subsection, we should discuss some properties of the greatest common divisor.

Remark 3.44. A reformulation of Theorem 1.38: Let A be a principal ideal domain and $0 \neq a \in A$ arbitrary. For each prime $\pi \in A$, we define the **π-adic valuation** $\nu_\pi(a) := \sup\{n \geq 0 \mid \pi^n \mid a\}$ of a over A. Let $\mathrm{PI}/\!\sim \; := \{\text{primes } \pi \in A\}/A^\times$ (prime ideals up to units), and further choose representatives π for each equivalence class. Then

$$a = u \prod_{\pi \in \mathrm{PI}/\sim} \pi^{\nu_\pi(a)} \qquad \text{with } u \in A^\times$$

is the *literally* unique prime factorisation of a.

Lemma 3.45. *Let A be a principal ideal domain and $a, b \in A$. Then the following three definitions of the **greatest common divisor** $g_1(a,b)$, $g_2(a,b)$ and $g_3(a,b)$ are equal up to units:*

(i) $g_1(a,b) \in A$ *such that* $(a,b) = (g_1(a,b))$.

(ii) $g_2(a,b) \coloneqq \prod_{\pi \in \mathrm{PI}/\sim} \pi^{\min\{\nu_\pi(a),\nu_\pi(b)\}}$.

(iii) $g_3(a,b) \mid a,b$ *such that if* $c \mid a,b$ *for any* $c \in A$, *then* $c \mid g_3(a,b)$.

Proof. We abbreviate $g_i \coloneqq g_i(a,b)$ for $i = 1,2,3$.

(i) g_3 satisfies the definition of g_2: By the uniqueness of prime factorisations, if $x \mid y$, then $\nu_\pi(x) \leq \nu_\pi(y)$ for all $\pi \in \mathrm{PI}/\sim$. This implies that for common divisors $c \mid a,b$, we must have $\nu_\pi(c) \leq \min\{\nu_\pi(a), \nu_\pi(b)\}$. We reach maximality in the sense of g_3 if $\nu_\pi(g_3) = \min\{\nu_\pi(a), \nu_\pi(b)\}$.

(ii) g_2 satisfies the definition of g_1: By the definition of g_2, a/g_2 and b/g_2 cannot have any common prime factor. Recall that in principal ideal domains, all prime ideals are generated by prime elements. Hence there is no prime ideal $\mathfrak{p} \subset A$ with $a/g_2, b/g_2 \in \mathfrak{p}$. Recall that in principal ideal domains, maximal ideals are precisely all non-zero prime ideals. Hence $(a/g_2, b/g_2) = A$. Thus $(a,b) = g_2 \cdot (a/g_2, b/g_2) = g_2 A = (g_2)$.

(iii) g_1 satisfies the definition of g_3: By definition of g_1, we have $g_1 \mid a,b$. If $c \mid a,b$ for some $c \in A$, then $(a,b) \subseteq (c)$ and thus $c \mid g_1$. □

Theorem 3.46 (elementary divisor theorem). *Let A be a principal ideal domain and $S \in M_{n\times m}(A)$. Then there exists a (up to units) unique ascending chain of divisors $a_1 \mid a_2 \mid \cdots \mid a_k \in A$ with $k = \min\{m,n\}$ such that*

$$S \sim \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ & 0_{(n-k)\times m} & \end{pmatrix} \quad \text{or resp.} \quad S \sim \begin{pmatrix} a_1 & & & \\ & \ddots & & 0_{n\times(m-k)} \\ & & a_k & \end{pmatrix}.$$

*(The chain of divisors might become stationary at 0 as $0 \mid 0$ makes sense.) We call these equivalent matrices the **Smith normal form** of S.*

We will prove this through an algorithm. But in order to do this, we need many auxiliary statements.

For the remaining subsection, let $g \coloneqq \gcd$. For $S \in M_{n\times m}(A)$, let $g(S)$ be the greatest common divisor of all entries.

Lemma 3.47. *Let A be a principal ideal domain, and let $a,b \in A$. Then there is some $X \in \mathrm{GL}_2(A)$ such that*

$$X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g(a,b) \\ c \end{pmatrix} \qquad \text{for some } c \in A.$$

Proof. If $a = b = 0$, we can choose $X = 1_2$. From now on, we may assume $g(a,b) \neq 0$.

Since $(a,b) = (g(a,b))$ by Lemma 3.45, there exists $r,s \in A$ such that $g(a,b) = ra + sb$. Then necessarily, we have $g(r,s) = 1$ (up to units) because $g(r,s)g(a,b) \mid g(a,b)$ and the prime factorisation of $g(a,b)$ is unique. So there are $u,v \in A$ such that $ur + vs = 1$, and hence $X = \left(\begin{smallmatrix} r & s \\ -v & u \end{smallmatrix}\right) \in \mathrm{GL}_2(A)$ by Lemma 3.35 (the determinant is 1). We obtain

$$X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g(a,b) \\ -va + ub \end{pmatrix}.$$ □

Corollary 3.48. *Let A be a principal ideal domain, and let $S \in M_{n\times m}(A)$. Then for each $2 \leq i \leq n$, there is an $L \in \mathrm{GL}_n(A)$ such that*

$$LS = \begin{pmatrix} g(s_{11}, s_{i1}) & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{pmatrix}.$$

Proof. Let $Y \in \mathrm{GL}_n(A)$ be the permutation matrix that swaps the second and ith row (in fact $Y^{-1} = Y$). According to Lemma 3.47, we can find an $X \in \mathrm{GL}_2(A)$ such that

$$X\begin{pmatrix} s_{11} \\ s_{i1} \end{pmatrix} = \begin{pmatrix} g(s_{11}, s_{i1}) \\ c \end{pmatrix}.$$

To obtain the result, set

$$L \coloneqq Y^{-1}\begin{pmatrix} X & \\ & 1_{n-2} \end{pmatrix} Y. \qquad \square$$

Remark 3.49. We can apply the above analogously to the first row instead of the first column: For each $2 \leq j \leq m$, there is an $R \in \mathrm{GL}_m(A)$ such that

$$SR = \begin{pmatrix} g(s_{11}, s_{1j}) & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{pmatrix}$$

This follows from Corollary 3.48 by transposing X.

Lemma 3.50. *Let A be a principal ideal domain, and let $S \in M_{n\times m}(A)$. If $s_{11} \mid s_{i1}, s_{1j}$ for all $2 \leq i \leq n$ and $2 \leq j \leq m$, then there are $L \in \mathrm{GL}_n(A)$ and $R \in \mathrm{GL}_m(A)$ such that*

$$LSR = \begin{pmatrix} s_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \tilde{S} & \\ 0 & & & \end{pmatrix}$$

Proof. These are well-known elementary row and column operations: We take

$$L = \begin{pmatrix} 1 & & & \\ l_2 & 1 & & \\ \vdots & & \ddots & \\ l_n & & & 1 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 1 & r_2 & \cdots & r_m \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

with $l_i \coloneqq -s_{i1}/s_{11}$ and $r_j \coloneqq -s_{1j}/s_{11}$. $\square$

Definition 3.51. For an element $a \in A$ of a principal ideal domain, we define its **size** by

$$\sigma(a) = \begin{cases} \infty, & \text{if } a = 0, \\ e_1 + \cdots + e_r, & \text{if } 0 \neq a = \pi_1^{e_1} \cdots \pi_r^{e_r} \text{ is the prime factorisation.} \end{cases}$$

Now to the actual proof of the elementary divisor theorem.

Proof. Our aim is to show this claim: Let $a_1 \coloneqq g(S)$. Then there is an $S_1 \in M_{(n-1)\times(m-1)}(A)$ such that

$$S \sim \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & S_1 & \\ 0 & & & \end{pmatrix}$$

This claim proves the theorem, since:

- For any $L \in M_n(A)$ and $R \in M_m(A)$, each entry of LSR is a linear combination of entries of S, hence $g(S) \mid g(LSR)$. If $L \in \mathrm{GL}_n(A)$ and $R \in \mathrm{GL}_m(A)$, then we also have $g(LSR) \mid g(L^{-1}LSRR^{-1}) = g(S)$, thus $g(S) = g(LSR)$ up to units.

  Therefore if $S \sim \left(\begin{smallmatrix} a_1 & \\ & S_1 \end{smallmatrix}\right)$, then $a_1 \coloneqq g(S) = g\left(\begin{smallmatrix} a_1 & \\ & S_1 \end{smallmatrix}\right) \mid g(S_1) =: a_2$. By induction on (n, m), we obtain a chain $a_1 \mid a_2 \mid \cdots \mid a_k$ as required. Notice that the base cases for $(n \times 1)$- and $(1 \times m)$-matrices are already covered by the claim.

- We can also show uniqueness with the observation $g(S) = g(LSR)$ for $L \in \mathrm{GL}_n(A)$ and $R \in \mathrm{GL}_m(A)$: Assume that S is equivalent to a matrix as in the theorem with $a_1 \mid a_2 \mid \cdots \mid a_k$. Then $g(S) = g(a_1, \ldots, a_k) = a_1$, so a_1 is uniquely determined up to units. Furthermore, if $\begin{pmatrix} a & \\ & S_1 \end{pmatrix} \sim \begin{pmatrix} a & \\ & \tilde{S}_1 \end{pmatrix}$, then $S_1 \sim \tilde{S}_1$. Hence by induction on (n, m), the $a_2 \mid \cdots \mid a_k$ are unique as well.

Now to the proof of the claim. We will show an algorithm which transforms S into equivalent matrices.

If $S = 0$, then we are done. Otherwise, we swap rows and columns such that $s_{11} \neq 0$. We will proceed by descending induction on $\sigma(s_{11}/g(S)) \geq 0$ (notice that $g(S) \mid s_{11}$). In particular, there can only be finitely many steps.

(i) If $\sigma(s_{11}/g(S)) = 0$, i. e. $s_{11} = g(S)$ up to units, then in particular $s_{11} \mid s_{i1}, s_{1j}$ for all $2 \leq i \leq n$ and $2 \leq j \leq m$. We finish with Lemma 3.50.

(ii) Otherwise, it is $\sigma(s_{11}/g(S)) \geq 1$. We distinguish between two cases:

(a) If there is some $2 \leq i \leq n$ or $2 \leq j \leq m$ with $s_{11} \nmid s_{i1}$ or $s_{11} \nmid s_{1j}$, then we can use Corollary 3.48 to obtain

$$S \sim \begin{pmatrix} \tilde{s}_{11} & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{pmatrix}$$

with $\tilde{s}_{11} = g(s_{11}, s_{i1})$ or $\tilde{s}_{11} = g(s_{11}, s_{j1})$, resp. Then by assumption, $\tilde{s}_{11} \mid s_{11}$ properly, and thus $\sigma(\tilde{s}_{11}/g(S)) < \sigma(s_{11}/g(S))$ (recall that $g(S) = g(\tilde{S})$ for $S \sim \tilde{S}$). Now we can start anew and proceed by induction.

(b) If $s_{11} \mid s_{i1}, s_{1j}$ for all $2 \leq i \leq n$ and $2 \leq j \leq m$, then we do the following: Firstly, we apply Lemma 3.50 to obtain

$$S \sim \begin{pmatrix} s_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \tilde{S} & \\ 0 & & & \end{pmatrix}$$

Then, since $\sigma(s_{11}/g(S)) \geq 1$, we have $g(S) \mid s_{11}$ properly. Therefore there is some entry $\tilde{s}_{ij}$ with $2 \leq i \leq n$ and $2 \leq j \leq m$ such that $s_{11} \nmid \tilde{s}_{ij}$. We add the ith row to the first row, and now we are in case (ii)a. □

Theorem 3.52 (structure theorem for finitely generated modules over principal ideal domains). *Let A be a principal ideal domain, and let M be a finitely generated A-module. Then there are unique $l, r \geq 0$ and a (up to units) unique ascending chain of* elementary divisors $a_1 \mid a_2 \mid \cdots \mid a_l \neq 0$ *such that*

$$M \cong A/(a_1) \oplus \cdots \oplus A/(a_l) \oplus A^r.$$

Example 3.53. Let $A = \mathbb{Z}$. Any finitely generated abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}/n_1 \oplus \cdots \oplus \mathbb{Z}/n_l \oplus \mathbb{Z}^r$$

with unique $n_1 \mid \cdots \mid n_l \neq 0$ and $r \geq 0$.

Proof. As M is finitely generated, there is an A-linear surjection $\varphi\colon A^n \twoheadrightarrow M$. A is a principal ideal domain, thus noetherian. With Corollary 3.25, A^n is noetherian, hence $\ker(\varphi) \subseteq A^n$ is finitely generated and there exists an A-linear surjection $S\colon A^m \twoheadrightarrow \ker(\varphi)$. This means $M \cong \mathrm{coker}(S)$ is of finite presentation.

Because of Lemma 3.42, we may choose any equivalent matrix $S' \sim S$ and $M \cong \mathrm{coker}(S')$ still holds. So by the elementary divisor theorem 3.46, we may assume

$$S = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ & 0_{(n-k)\times m} & \end{pmatrix} \quad \text{or} \quad S = \begin{pmatrix} a_1 & & & \\ & \ddots & & 0_{n\times(m-k)} \\ & & a_k & \end{pmatrix}$$

with elementary divisors $a_1 \mid a_2 \mid \cdots \mid a_l \neq 0$ and $a_{l+1} = \cdots = a_k = 0$. Then

$$\operatorname{im}(S) \cong (a_1) \oplus \cdots \oplus (a_l) \oplus 0^{\max\{0,n-l\}} \implies M \cong A/(a_1) \oplus \cdots \oplus A/(a_l) \oplus A^{\max\{0,n-l\}}.$$

Uniqueness will be shown in Exercise 8.20. □

Example 3.54. Consider

$$\begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \in M_{3\times 2}(\mathbb{Z}).$$

By subtracting the first row two times from the third, we obtain

$$\begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ & 3 \\ & 5 \end{pmatrix}$$

As $\gcd(2,3,5) = 1 \neq 2$, we have to continue with the upper left corner. Adding the second column to the first, we have

$$\begin{pmatrix} 2 & \\ & 3 \\ & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ 3 & 3 \\ 5 & 5 \end{pmatrix}.$$

Using $T = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and eliminating the first column and first row yields

$$\begin{pmatrix} 2 & \\ 3 & 3 \\ 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ -2 & \\ 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ & 6 \\ 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ & 6 \\ & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 6 \\ & -10 \end{pmatrix}.$$

Since $\gcd(6,-10) = 2$, we can use $T = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ to get

$$\begin{pmatrix} 1 & \\ & 6 \\ & -10 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 2 \\ & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 2 \\ 0 & 0 \end{pmatrix}.$$

In particular,

$$\operatorname{coker} \begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \cong \mathbb{Z}/1 \oplus \mathbb{Z}/2 \oplus \mathbb{Z} \cong \mathbb{Z}/2 \oplus \mathbb{Z}.$$

Remark: We could have proceeded more directly:

$$\begin{pmatrix} 2 & \\ & 3 \\ 4 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ & 3 \\ & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ & 3 \\ & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ & 1 \\ & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ & 1 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} & 2 \\ 1 & \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 2 \\ 0 & 0 \end{pmatrix}.$$

Example 3.55. Consider $\left(\begin{smallmatrix} 2 \\ & 3 \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. Then

Lect. 8
04.05.23

$$\begin{pmatrix} 2 & \\ & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & \\ 3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & \\ & 6 \end{pmatrix}$$

(the last step is possible since $-1 \in \mathbb{Z}^\times$). This reflects the isomorphism $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$.

Observation 3.56. We can derive the **Jordan normal form** as an application. Let k be a field and V a finite-dimensional k-vector space. Let $f\colon V \to V$ be a k-linear map.

Then V becomes a $k[T]$-module via $p(T)v := p(f)(v)$ for all $p \in k[T]$. Since V is finite-dimensional, V is also finitely-generated as a $k[T]$-module (since there is an embedding $k \hookrightarrow k[T]$, the k-basis is also a $k[T]$-generating set). $k[T]$ is a principal ideal domain, so by the structure theorem 3.52, we obtain

$$V \cong k[T]^r \oplus \bigoplus_{i=1}^{l} k[T]/(h_i(T))$$

with non-zero $h_1 \mid \cdots \mid h_l$ in $k[T]$. Since this is also an isomorphism of k-vector spaces, and since V is finite-dimensional over k, we see that $r = 0$. Using the Chinese remainder theorem 8.5, we can rewrite this as

$$V \cong \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{n} k[T]/(g_j(T)^{n_{ij}}),$$

where $g_1, \ldots, g_n$ are the irreducible factors of $\operatorname{char}(f,T)$ and $\prod_{j=1}^{n} g_j(T)^{n_{ij}} = h_i(T)$ is the prime factorisation of h_i. (By Cayley-Hamilton 8.19, we have $\operatorname{char}(f,f) = 0$. Looking at the decomposition, this is only possible if and only if $h_1, \ldots, h_l \mid \operatorname{char}(f,T)$, so $g_1, \ldots, g_n$ are indeed irreducible factors of $\operatorname{char}(f,T)$.)

If we impose that all $g_i = T - a_i$ are linear for some $a_i \in k$, then

$$k[T]/(g_i(T)^{n_{ij}}) \cong k[T]/(T-a_i)^{n_{ij}} \cong k^{n_{ij}}$$

as n_{ij}-dimensional k-vector spaces with T acting by

$$\begin{pmatrix} a_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & a_i \end{pmatrix} \in M_{n_{ij} \times n_{ij}}(k)$$

on $k^{n_{ij}}$. We can see this if we define the canonical action as multiplication w. r. t. the basis

$$\{(T-a_i)^k + (T-a_i)^{n_{ij}} \mid 0 \le k < n_{ij}\}.$$

Note that the action of T corresponds to the application of (a restriction of) f on $k^{n_{ij}}$.

4 Basics in Homological Algebra

Homological algebra is a relatively recent field of algebra, which originates from algebraic topology and heavily uses categorical concepts in its studies. Here, we want to introduce some basics in order to pursue this topic in more advanced courses. Moreover, these results are widely applicable in many fields of algebra.

4.1 Tensor Products

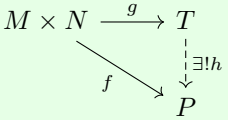
For reference, see [AtMac, ch. 2].

Definition 4.1. Let M, N and P be A-modules. Then a map $f\colon M \times N \to P$ is called **A-bilinear** if for all $x \in M$ and $y \in N$, the maps $f(x,-)\colon N \to P$ and $f(-,y)\colon M \to P$ are A-linear. We define $\operatorname{Bihom}_A(M,N;P)$ as the set of all A-bilinear maps $M \times N \to P$.

Remark 4.2. Similar to vector spaces or abelian groups, we have the bijection

$$\operatorname{Bihom}_A(M,N;P) = \operatorname{Hom}_A(M, \operatorname{Hom}_A(N,P)), \qquad f \mapsto [x \mapsto f(x,-)].$$

Definition 4.3. Let M and N be A-modules. A pair (T,g) with an A-module T and an A-bilinear map $g\colon M \times N \to T$ is the **tensor product** of M and N over A if the following **universal property of tensor products** holds: For all other such pairs (P,f) with an A-module P and an A-bilinear map $f\colon M \times N \to P$, there is a unique A-linear map $h\colon T \to P$ such that the following diagram commutes:



Remark 4.4. By the universal property, tensor products of M and N are unique up to unique isomorphism.

Example 4.5. Before we prove the existence of tensor products in general, we will consider the tensor product for finite free modules first.

Let $M = A^m$ and $N = A^n$. Then for any A-module P, we have the following matrix representation for A-bilinear maps:

$$\mathrm{Bihom}_A(A^m, A^n; P) \cong M_{m\times n}(P), \qquad f \mapsto (f(e_i, f_j))_{\substack{i=1,\dots,m\\ j=1,\dots,n}}.$$

This is possible since f is A-bilinear, and since each element of M or N is a unique linear combination of the e_i or f_j, resp. The matrices have entries in P. Evaluation is realised by multiplying with a column vector in A^m from the right and with a row vector in A^n from the left.

We define the free A-module $T \coloneqq A^{mn}$ with standard basis $\{e_{ij} \mid 1 \le i \le m, 1 \le j \le n\}$. Furthermore, let $g\colon A^m \times A^n \to T$ be the unique A-bilinear map satisfying $g(e_i, f_j) = e_{ij}$, i. e. its matrix representation is precisely $(e_{ij})_{ij} \in M_{m\times n}(T)$.

Then (T, g) is the tensor product of A^m and A^n: Given any A-bilinear map $f\colon A^m \times A^n \to P$, the A-linear map $h\colon T \to P$, $e_{ij} \mapsto f(e_i, f_j)$ is the unique map satisfying $f = h \circ g$ (the uniqueness of h is given by the uniqueness of A-linear combinations over a basis).

We observe that in general, g is not surjective. For example, $e_{11} + e_{22} = g(e_1, f_1) + g(e_2, f_2)$ has no preimage for g is A-bilinear. But $\mathrm{im}(g)$ generates T because $\{e_{ij} \mid i, j\} \subseteq \mathrm{im}(g)$.

Proposition 4.6. *Tensor products of A-modules exist.*

Proof. Let M and N be A-modules.

(i) Consider the (huge) free A-module

$$\tilde{T} \coloneqq \bigoplus_{(x,y)\in M\times N} Ae_{(x,y)},$$

i. e. every pair of elements is a *basis vector*, and a map of sets

$$\tilde{g}\colon M \times N \to \tilde{T}, \qquad (x, y) \mapsto e_{(x,y)}$$

with no further properties.

In general, if $f\colon M \times N \to P$ is any A-bilinear map, then there is a *unique* A-linear map $\tilde{h}\colon \tilde{T} \to P$ such that $f = \tilde{h} \circ \tilde{g}$, namely $\tilde{h}(e_{(x,y)}) = f(x, y)$. Indeed, uniqueness and existence follow from the fact that $\tilde{T}$ is free.

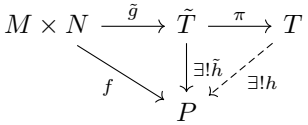
(ii) Let $U \subseteq \tilde{T}$ be the smallest A-submodule (w. r. t. inclusion) such that $g \coloneqq \pi \circ \tilde{g}$ is an A-bilinear map, where $\pi\colon \tilde{T} \twoheadrightarrow \tilde{T}/U$ is the canonical projection. Concretely, U is the submodule generated by

$$\begin{aligned} &e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)}, && e_{(x,ay)} - ae_{(x,y)},\\ &e_{(x_1+x_2,y)} - e_{(x_1,y)} - e_{(x_2,y)}, && e_{(ax,y)} - ae_{(x,y)} \end{aligned}$$

for all $a \in A$, $x, x_1, x_2 \in M$ and $y, y_1, y_2 \in N$. Set $T \coloneqq \tilde{T}/U$. By dividing by U, we effectively set the above generators to 0 in T, i. e. $g\colon M \times N \to T$ is indeed bilinear. E. g. $g(x, y_1 + y_2) = e_{(x,y_1+y_2)} = e_{(x,y_1)} + e_{(x,y_2)} = g(x, y_1) + g(x, y_2)$.

(iii) We will prove that (T, g) satisfies the universal property of tensor products. This establishes (T, g) as a tensor product of M and N over A.

Let $f\colon M \times N \to P$ be any A-bilinear map, and let $\tilde{h}\colon \tilde{T} \to P$, $e_{(x,y)} \mapsto f(x, y)$ be the unique A-linear map such that $f = \tilde{h} \circ \tilde{g}$, see (i). Thus we are left to show that the factorisation $\tilde{h} = h \circ \pi$ exists and is unique.



Let z be one of the generators of U. Then we have $\tilde{h}(z) = 0$ because f is A-bilinear, e. g.

$$\begin{aligned}\tilde{h}(e_{(x,y_1+y_2)} - e_{(x,y_1)} - e_{(x,y_2)}) &= \tilde{h}(e_{(x,y_1+y_2)}) - \tilde{h}(e_{(x,y_1)}) - \tilde{h}(e_{(x,y_2)}) \\ &= f(x, y_1 + y_2) - f(x, y_1) - f(x, y_2) = 0, \\ \tilde{h}(e_{(x,ay)} - ae_{(x,y)}) &= \tilde{h}(e_{(x,ay)}) - a\tilde{h}(e_{(x,y)}) = f(x, ay) - af(x, y) = 0.\end{aligned}$$

Thus $\tilde{h}(u) = 0$ for all $u \in U$, and we conclude the desired factorisation from the universal property of quotient modules (which is induced by the universal property of quotient groups). □

Definition 4.7. Let M and N be A-modules. We denote the tensor product of M and N over A by

$$(M \otimes_A N, (x, y) \mapsto x \otimes y).$$

We call $x \otimes y$ for any $x \in M$ and $y \in N$ **elementary tensors**. They generate $M \otimes_A N$ as an A-module.

So tensor products encapsulate the properties of all bilinear maps in the sense of the universal property. In other words, we can translate each bilinear map to a linear map with the tensor product as the domain.

Example 4.8. $e_1 \otimes e_1 + e_1 \otimes e_2 = e_1 \otimes (e_1 + e_2) \in A^2 \otimes_A A^2$ is elementary, while $e_1 \otimes e_1 + e_2 \otimes e_2$ is not, if $A \neq 0$. More generally, the elementary tensors in $A^2 \otimes_A A^2$ are

$$(ae_1 + be_2) \otimes (ce_1 + de_2) = ace_1 \otimes e_1 + ade_1 \otimes e_2 + bce_2 \otimes e_1 + bde_2 \otimes e_2$$

for any $a, b, c, d \in A$.

4.2 Properties

Observation 4.9. The tensor product is *functorial*: Let $\phi\colon M_1 \to M_2$ and $\psi\colon N_1 \to N_2$ be A-linear maps. We consider

$$\begin{array}{ccc} M_1 \times N_1 & \longrightarrow & M_1 \otimes_A N_1 \\ {\scriptstyle (\phi,\psi)}\downarrow & \searrow & \downarrow{\scriptstyle \phi\otimes\psi} \\ M_2 \times N_2 & \longrightarrow & M_2 \otimes_A N_2 \end{array} \qquad \begin{array}{c} x \otimes y \\ \downarrow \\ \phi(x) \otimes \psi(y) \end{array}$$

As the diagonal composition is A-bilinear, according to the universal property, it factors uniquely through an A-linear map $\phi \otimes \psi\colon M_1 \otimes_A N_1 \to M_2 \otimes_A N_2$. Looking at the commutative diagram ($M_1 \times N_1 \to M_2 \times N_2 \to M_2 \otimes_A N_2$), this map is given on elementary tensors by

$$(\phi \otimes \psi)(x \otimes y) = \phi(x) \otimes \psi(y).$$

Observation 4.10. As a special case, let us consider tensor products with a quotient module:

Let M and N be an A-module and $U \subseteq M$ a submodule. If we let $\phi\colon M \twoheadrightarrow M/U$ and $\psi = \mathrm{id}_N$, then there is a unique A-linear map $M \otimes_A N \twoheadrightarrow M/U \otimes_A N$. This is surjective since it is apparently surjective on elementary tensors ($x \otimes y \mapsto (x + U) \otimes y$) and the elementary tensors generate $M/U \otimes_A N$. If we determine its kernel, then we obtain an alternative description of $M/U \otimes_A N$ by the homomorphism theorem.

We have

$$\begin{aligned}\mathrm{Bihom}_A(M/U, N; P) &= \{f \in \mathrm{Bihom}_A(M, N; P) \mid f|_{U\times N} = 0\} \\ &= \{h \in \mathrm{Hom}_A(M \otimes_A N, P) \mid h \circ (U \otimes_A N \to M \otimes_A N) = 0\} \\ &= \mathrm{Hom}_A(M \otimes_A N / \operatorname{im}(U \otimes_A N \to M \otimes_A N), P).\end{aligned}$$

The first equality uses $f(u+U, y) = f(0, y) = f(0 \cdot 0, y) = 0 f(0, y) = 0$ for all $(u, y) \in U \times N$. The second uses the universal property: Every $f \in \mathrm{Bihom}_A(M, N; P)$ factorises through a unique $h \in \mathrm{Hom}_A(M \otimes_A N, P)$, and each $h \in \mathrm{Hom}_A(M \otimes_A N, P)$ defines exactly one $f \in \mathrm{Bihom}_A(M, N; P)$ through composition. The map $U \otimes_A N \to M \otimes_A N$ is the canonical inclusion $u \otimes n \mapsto u \otimes n$. The last equality reformulates the previous set as a quotient, a kind of converse of the first equality.

By the universal property, we have $\mathrm{Bihom}_A(M/U, N; P) = \mathrm{Hom}_A(M/U \otimes_A N, P)$, where $M/U \otimes_A N$ is unique up to isomorphism. Therefore

$$(M \otimes_A N)/\operatorname{im}(U \otimes_A N \to M \otimes_A N) \cong M/U \otimes_A N, \qquad x \otimes y \mapsto (x+U) \otimes y.$$

Example 4.11. Consider the $\mathbb{Z}$-modules $M = \mathbb{Z}$ and $N = \mathbb{Z}/n$ as well as the submodule $U = n\mathbb{Z} \subseteq M$. We claim $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/n \cong \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n$. For that to be true, it must be $\operatorname{im}(n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n) = 0$, i. e. this map is the zero map. Indeed, $nx \otimes y \mapsto nx \otimes y = x \otimes ny = x \otimes 0 = 0$.

Remark 4.12. One can obtain a similar construction for the tensor product of any A-modules M and N: Pick presentations $M \cong A^{\oplus I}/U$ and $N \cong A^{\oplus J}/V$. Then with Example 4.5,

$$M \otimes_A N \cong A^{\oplus I} \otimes_A A^{\oplus J}/\operatorname{im}(U \otimes_A A^{\oplus J}) + \operatorname{im}(A^{\oplus I} \otimes_A V) \cong A^{\oplus I \times J}/\operatorname{im}(U \otimes_A A^{\oplus J} \oplus A^{\oplus I} \otimes_A V).$$

Example 4.13. Consider the $\mathbb{Z}$-modules $M = \mathbb{Z}/u\mathbb{Z}$ and $N = \mathbb{Z}/v\mathbb{Z}$ for $u, v \in \mathbb{Z}$, and consider the submodules $vM \subseteq M$ and $uN \subseteq N$. Let e and f be the generators of M and N, resp., i. e. $M = \mathbb{Z}e$ and $N = \mathbb{Z}f$.

Observe that $\mathbb{Z}e \otimes_{\mathbb{Z}} \mathbb{Z}f \cong \mathbb{Z}(e \otimes f)$ via $ae \otimes bf \mapsto ab(e \otimes f)$. Furthermore, we have

$$\operatorname{im}((v\mathbb{Z}e) \otimes_{\mathbb{Z}} \mathbb{Z}f \to \mathbb{Z}(e \otimes f), (ve) \otimes f \mapsto v(e \otimes f)) = v\mathbb{Z}(e \otimes f),$$
$$\operatorname{im}(\mathbb{Z}e \otimes_{\mathbb{Z}} (u\mathbb{Z}f) \to \mathbb{Z}(e \otimes f), e \otimes (uf) \mapsto u(e \otimes f)) = u\mathbb{Z}(e \otimes f).$$

Therefore $v\mathbb{Z}(e \otimes f) + u\mathbb{Z}(e \otimes f) = \gcd(u, v)\mathbb{Z}(e \otimes f)$ and

$$\mathbb{Z}e/v\mathbb{Z}e \otimes_{\mathbb{Z}} \mathbb{Z}f/u\mathbb{Z}f \cong \mathbb{Z}(e \otimes f)/(\gcd(u, v)\mathbb{Z}(e \otimes f)) \cong \mathbb{Z}/\gcd(u, v)\mathbb{Z}.$$

We will consider this in more detail in Corollary 4.27.

4.3 Exact Sequences

Lect. 9
08.05.23

Definition 4.14. A sequence of the form

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

of A-linear maps of A-modules is called **exact** if $\ker(f_{i+1}) = \operatorname{im}(f_i)$ for all i.

Example 4.15. In the following, let M, N and P be A-modules, and let f be an A-linear map. Then the following hold:

(i) The sequence

$$0 \longrightarrow M \xrightarrow{f} N$$

is exact if and only if f is injective.

The reason is that f is injective if and only if $\ker(f) = 0 = \operatorname{im}(0 \to M)$.

(ii) The sequence

$$N \xrightarrow{f} P \longrightarrow 0$$

is exact if and only if f surjective.

The reason is that f is surjective if and only if $\operatorname{im}(f) = P = \ker(P \to 0)$.

(iii) The sequence

$$0 \longrightarrow M \longrightarrow N \xrightarrow{f} P$$

is exact if and only if $M \cong \ker(f)$.

If this sequence is exact, then $M \to N$ is injective, and thus $M \cong \operatorname{im}(M \to N)$. By exactness in N, we have $\operatorname{im}(M \to N) = \ker(f)$. Conversely, if $M \cong \ker(f)$, then let $M \cong \ker(f) \hookrightarrow N$ be the inclusion map. This map is injective, and we easily see that $\operatorname{im}(M \hookrightarrow N) = \ker(f)$.

(iv) The sequence

$$M \xrightarrow{f} N \longrightarrow P \longrightarrow 0$$

is exact if and only if $P \cong \operatorname{coker}(f)$.

If the sequence is exact, then $N \to P$ is surjective, and thus $P \cong N/\ker(N \to P)$ by the homomorphism theorem. By exactness in N, we have $\ker(N \to P) = \operatorname{im}(f)$, and hence $N/\ker(N \to P) = N/\operatorname{im}(f) = \operatorname{coker}(f)$. Conversely, if $P \cong \operatorname{coker}(f) = N/\operatorname{im}(f)$, then let $N \twoheadrightarrow N/\operatorname{im}(f) \cong P$ be the projection map. This map is surjective, and we easily $\operatorname{im}(f) = \ker(N \twoheadrightarrow P)$.

Definition 4.16. A **short exact sequence** is an exact sequence of the form

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

Example 4.17. A typical example: Let A be a ring and $\mathfrak{a} \subseteq A$ an ideal. Then

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

is a short exact sequence with the natural inclusion $\mathfrak{a} \hookrightarrow A$ and the natural projection $A \twoheadrightarrow A/\mathfrak{a}$. A concrete example would be

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n \longrightarrow 0$$

Another example: Let M and N be A-modules. Then

$$0 \longrightarrow M \xrightarrow{i_1} M \oplus N \xrightarrow{p_2} N \longrightarrow 0$$

is a short exact sequence with maps $i_1 \colon x \mapsto (x, 0)$ and $p_2 \colon (x, y) \mapsto y$.

Example 4.18. Of course, exact sequences might not end on either side. For example, let $A = k[\varepsilon]/(\varepsilon^2)$. Then the following exact sequence does not end on the left:

$$\cdots \xrightarrow{\cdot\varepsilon} A \xrightarrow{\cdot\varepsilon} A \xrightarrow{\cdot\varepsilon} A \longrightarrow A/(\varepsilon) \longrightarrow 0$$

Indeed, we have $\ker(\cdot\varepsilon) = (\varepsilon) = \operatorname{im}(\cdot\varepsilon)$.

Example 4.19. Any A-linear map $f \colon M \to N$ can be extended to a four-term exact sequence, namely

$$0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} N \longrightarrow \operatorname{coker}(f) \longrightarrow 0$$

Notice that $\ker(f) \to M$ is injective, while $N \to \operatorname{coker}(f)$ is surjective. Furthermore, $\operatorname{im}(\ker(f) \to M) = \ker(f)$ and $\ker(N \to \operatorname{coker}(f)) = \operatorname{im}(f)$.

Proposition 4.20. *Tensor products are right-exact: Assume that*

$$M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

is an exact sequence. If Q is any A-module, then

$$M \otimes_A Q \xrightarrow{f\otimes \mathrm{id}_Q} N \otimes_A Q \xrightarrow{g\otimes \mathrm{id}_Q} P \otimes_A Q \longrightarrow 0$$

is again exact.

Proof.

- The exactness in $P \otimes_A Q$ means $g \otimes \mathrm{id}_Q$ is surjective: By assumption and Example 4.15, $g \colon N \to P$ and hence $(g, \mathrm{id}_Q) \colon N \times Q \to P \times Q$ are surjective. Thus by Observation 4.9, every elementary tensor is of the form $g(n) \otimes q$, and $g \otimes \mathrm{id}_Q$ is surjective on elementary tensors (recall that the generators are given by the universal map $P \times Q \to P \otimes_A Q$, $(p, q) \mapsto p \otimes q$). Now, $P \otimes_A Q$ is generated by these elementary tensors, thus $g \otimes \mathrm{id}_Q$ is surjective.

- The exactness in $N \otimes_A Q$ means $\operatorname{im}(f \otimes \mathrm{id}_Q) = \ker(g \otimes \mathrm{id}_Q)$: Using the surjectivity of $g \otimes \mathrm{id}_Q$, this is equivalent to $P \otimes_A Q \cong \operatorname{coker}(f \otimes \mathrm{id}_Q)$, see Example 4.15. We have the following universal property of cokernels: For any A-linear map $\phi\colon N \otimes_A Q \to X$, a unique factorisation

$$\begin{array}{ccc} N \otimes_A Q & \xrightarrow{g\otimes \mathrm{id}_Q} & P \otimes_A Q \\ {\scriptstyle\phi}\downarrow & \swarrow_{\bar\phi} & \\ X & & \end{array}$$

  through $\bar\phi$ exists if and only if $\phi \circ (g \otimes \mathrm{id}_Q) = 0$.

  By functoriality of the tensor product, the factorisation through $\bar\phi$ exists if and only if for every A-bilinear map $\tilde\phi\colon N \times Q \to X$, there is a unique factorisation

$$\begin{array}{ccc} N \times Q & \xrightarrow{(g,\mathrm{id}_Q)} & P \times Q \\ {\scriptstyle\tilde\phi}\downarrow & \swarrow_{\bar{\tilde\phi}} & \\ X & & \end{array}$$

  through an A-bilinear map $\bar{\tilde\phi}$, where $\tilde\phi(n,q) = \phi(n \otimes q)$. This is possible if and only if $\tilde\phi|_{\ker(g)\times Q} = 0$, since $\bar{\tilde\phi}(g(n), q) = \tilde\phi(n,q)$ is well-defined if and only if $\ker(g) \times Q \subseteq \ker(\tilde\phi)$. Since $\ker(g) = \operatorname{im}(f)$ by assumption, this is equivalent to $\tilde\phi|_{\operatorname{im}(f)\times Q} = 0$, i. e.

$$0 = \tilde\phi(f(m), q) = \phi(f(m) \otimes q) = (\phi \circ (f \otimes \mathrm{id}_Q))(m \otimes q) \qquad \text{for all } m \in M \text{ and } q \in Q.$$

  As the elementary tensors $f(m) \otimes q$ generate $\operatorname{im}(f \otimes \mathrm{id}_Q)$, we equivalently obtain $\phi \circ (f \otimes \mathrm{id}_Q) = 0$. □

This is the beginning of *homological algebra*.

4.4 Presentations and Tensor Products

Definition 4.21. A **presentation** of an A-module M are A-linear maps f and p such that

$$A^{\oplus J} \xrightarrow{f} A^{\oplus I} \xrightarrow{p} M \longrightarrow 0$$

is an exact sequence. Put differently, it is the datum of generators $(m_i)_{i\in I}$ for M and generators $(u_j)_{j\in J}$ for $\ker(A^{\oplus I} \to M, e_i \mapsto m_i)$. We can then write $u_j = \sum_{i\in I} a_{ij} e_i$, where for each $j \in J$, almost all a_{ij} are 0. Then f can be written as a matrix $(a_{ij})_{ij}$, and $M \cong \operatorname{coker}(f)$.

Lemma 4.22. *Every A-module M admits a presentation.*

Proof. Each M has generators $\{m_i \in M \mid i \in I\}$, e. g. $I = M$ and $m_n \coloneqq n$ for all $n \in M$. Thus $p\colon A^{\oplus I} \to M$, $e_i \mapsto m_i$ is surjective. Then again, $\ker(p)$ has generators $\{u_j \in \ker(p) \mid j \in J\}$, e. g. $J = \ker(p)$ and $u_n \coloneqq n$ for all $n \in \ker(p)$. Thus $f\colon A^{\oplus J} \to A^{\oplus I}$, $e_j \mapsto u_j$ is a surjection onto $\ker(p)$, and hence (f, p) gives a presentation. □

Example 4.23. Let $A = k[X, Y]$ and $M = (X, Y) \subseteq A$ as in Example 3.20. There we saw that

$$A \xrightarrow{\binom{-Y}{X}} A^{\oplus 2} \xrightarrow{(X\ Y)} M \longrightarrow 0$$

is a presentation. Here, $\binom{-Y}{X}$ being injective is a bonus feature and is not required by the definition of presentations.

Example 4.24. Let A be a ring and $\mathfrak{a} \subseteq A$ a finitely-generated ideal, say $\mathfrak{a} = (a_1, \ldots, a_n)$. Then

$$A^{\oplus n} \xrightarrow{e_i \mapsto a_i} A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

is a presentation of $A/\mathfrak{a}$.

In order to take the tensor product of presentations, we will have to understand tensor products first.

Proposition 4.25. *Let M, N and P be A-modules. Tensor products have the following properties:*

(i) $A \otimes_A M \cong M$, *given by* $a \otimes m \mapsto am$.

(ii) $M \otimes_A N \cong N \otimes_A M$, *given by* $m \otimes n \mapsto n \otimes m$.

(iii) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$, *given by* $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$.

(iv) $(\bigoplus_{i\in I} M_i) \otimes_A N \cong \bigoplus_{i\in I} M_i \otimes_A N$, *given by* $(\sum_{i\in I} m_i) \otimes n \mapsto \sum_{i\in I} m_i \otimes n$.

Proof. The proof strategy, except for (i), is to use tensor product calculus and the universal property in order to show that certain compositions have to be the identity.

(i) Consider the A-bilinear map $A \times M \to M$, $(a, m) \mapsto am$. By the universal property of tensor products, it factors:

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ \downarrow & \nearrow_{\phi} & \\ A \otimes_A M & & \end{array}$$

where $\phi\colon A \otimes_A M \to M$, $a \otimes m \mapsto am$ is A-linear.

ϕ is evidently surjective. For injectivity, let $x = \sum_{i=1}^n a_i \otimes m_i \in \ker(\phi)$ (we wrote x as a linear combination of elementary tensors). Then $x = \sum_{i=1}^n 1 \otimes (a_i m_i) = 1 \otimes \sum_{i=1}^n a_i m_i$. As $0 = \phi(x) = \sum_{i=1}^n a_i m_i$, we obtain $x = 1 \otimes 0 = 0$.

Alternatively, we know by Remark 4.2 that

$$\mathrm{Bihom}_A(A, M; P) \cong \mathrm{Hom}_A(A, \mathrm{Hom}_A(M, P)) \cong \mathrm{Hom}_A(M, P), \qquad f \mapsto [a \mapsto f(a, -)] \mapsto f(1, -).$$

By the universal property of tensor products, we have $\mathrm{Bihom}_A(A, M; P) \cong \mathrm{Hom}_A(A \otimes_A M, P)$, thus $A \otimes_A M \cong M$.

(ii) Consider the canonical A-bilinear maps

$$M \times N \to N \otimes_A M, (m, n) \mapsto n \otimes m \qquad \text{and} \qquad N \times M \to M \otimes_A N, (n, m) \mapsto m \otimes n.$$

By the universal property of tensor products, they factor through the A-linear maps

$$\Psi\colon N \otimes_A M \to M \otimes_A N, n \otimes m \mapsto m \otimes n \qquad \text{and} \qquad \Phi\colon M \otimes_A N \to N \otimes_A M, m \otimes n \mapsto n \otimes m,$$

resp. As $\Phi \circ \Psi = \mathrm{id}$ and $\Psi \circ \Phi = \mathrm{id}$ are the identity on elementary tensors, it is also the identity on $M \otimes_A N$ and $N \otimes_A M$, resp.

(iii) Similar to the above, by the universal property of tensor products, the A-bilinear maps

$$\begin{aligned} (M \otimes_A N) \times P \to M \otimes_A (N \otimes_A P), &\qquad (m \otimes n, p) \mapsto m \otimes (n \otimes p), \\ M \times (N \otimes_A P) \to (M \otimes_A N) \otimes_A P, &\qquad (m, n \otimes p) \mapsto (m \otimes n) \otimes p \end{aligned}$$

factor through the A-linear maps

$$\begin{aligned} (M \otimes_A N) \otimes_A P \to M \otimes_A (N \otimes_A P), &\qquad (m \otimes n) \otimes p \otimes p \mapsto m \otimes (n \otimes p), \\ M \otimes_A (N \otimes_A P) \to (M \otimes_A N) \otimes_A P, &\qquad m \otimes (n \otimes p) \mapsto (m \otimes n) \otimes p, \end{aligned}$$

which are mutual inverses on elementary tensors and thus on the respective tensor products.

(iv) See Exercise 8.23. □

Remark 4.26. $(\prod_{i\in I} M_i) \otimes_A N \cong \prod_{i\in I} M_i \otimes_A N$ does not hold true for infinite direct products (Exercise 8.26).

Corollary 4.27. *Let N be an A-module.*

(i) *Then* $A^{\oplus I} \otimes_A N \cong N^{\oplus I}$.

(ii) *If* $M \cong \operatorname{coker}((a_{ij})_{ij} \colon A^{\oplus J} \to A^{\oplus I})$ *is a presented module, then* $M \otimes_A N \cong \operatorname{coker}((a_{ij})_{ij} \colon N^{\oplus J} \to N^{\oplus I})$.

Proof.

(i) We have $A^{\oplus I} \otimes_A N \cong (A \otimes_A N)^{\oplus I} \cong N^{\oplus I}$.

(ii) Let $f \coloneqq (a_{ij})_{ij}$, i. e. $M \cong \operatorname{coker}(f)$. From the right-exactness of the tensor product (Proposition 4.20), we know $M \otimes_A N \cong \operatorname{coker}(f \otimes \mathrm{id}_N)$. Now we explicitly express $f \otimes \mathrm{id}_N$ with the help of (i).

We have $A^{\oplus J} \otimes_A N \cong N^{\oplus J}$, given by

$$e_j \otimes n \mapsto (0, \dots, 0, 1 \otimes n, 0, \dots, 0) \mapsto (0, \dots, 0, n, 0, \dots, 0) =: ne_j$$

with non-zero entry at the jth position (ne_j is an abuse of notation). Similarly for $A^{\oplus I} \otimes_A N$. Thus we obtain:

$$\begin{array}{ccc} A^{\oplus J} \otimes_A N & \xrightarrow{f \otimes \mathrm{id}_N} & A^{\oplus I} \otimes_A N \\ \cong \downarrow & & \downarrow \cong \\ N^{\oplus J} & \xrightarrow{???} & N^{\oplus I} \end{array} \qquad \begin{array}{ccc} e_j \otimes n & \longmapsto & (\sum_{i \in I} a_{ij} e_i) \otimes n = \sum_{i \in I} a_{ij}(e_i \otimes n) \\ \uparrow & & \downarrow \\ ne_j & \xmapsto{!!!} & \sum_{i \in I} a_{ij}(ne_i) \end{array}$$

That is, $f \otimes \mathrm{id}_N$ is given by the identification $(a_{ij})_{ij} \colon N^{\oplus J} \to N^{\oplus I}$. □

4.5 Examples

Example 4.28. Let $A = k[X, Y]$ and $\mathfrak{a} = (X, Y) \subseteq A$. Then with Example 4.23 and Corollary 4.27,

$$\mathfrak{a} \otimes_A A/\mathfrak{a} \cong \operatorname{coker}\left(\begin{pmatrix} -Y \\ X \end{pmatrix} \colon A \to A^{\oplus 2}\right) \otimes_A A/\mathfrak{a} \cong \operatorname{coker}\left(\begin{pmatrix} -Y \\ X \end{pmatrix} \colon A/\mathfrak{a} \to (A/\mathfrak{a})^{\oplus 2}\right).$$

But $X, Y \in \mathfrak{a}$, i. e. $X \cdot A/\mathfrak{a} = Y \cdot A/\mathfrak{a} = 0$. Hence

$$\mathfrak{a} \otimes_A A/\mathfrak{a} \cong \operatorname{coker}(0 \colon A/\mathfrak{a} \to (A/\mathfrak{a})^{\oplus 2}) \cong (A/\mathfrak{a})^{\oplus 2} \cong k^2,$$

which is a two-dimensional k-vector space.

Example 4.29. Let A be any ring and $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideals. Then $\mathfrak{a} \times \mathfrak{b} \mapsto \mathfrak{ab}$, $(a, b) \mapsto ab$ is A-bilinear, and factors by the universal property of tensor products:

$$\begin{array}{ccc} \mathfrak{a} \times \mathfrak{b} & \longrightarrow & \mathfrak{ab} \\ \downarrow & \nearrow_{a \otimes b \mapsto ab} & \\ \mathfrak{a} \otimes_A \mathfrak{b} & & \end{array}$$

We observe that $\mathfrak{a} \otimes_A \mathfrak{b} \to \mathfrak{ab} = (ab \mid a \in \mathfrak{a}, b \in \mathfrak{b})$ is always surjective. But when is this injective? This is a subtle question and will depend on A and $\mathfrak{a}$, $\mathfrak{b}$.

(i) Consider $A = k[\varepsilon]/(\varepsilon^2)$ and $\mathfrak{a} = \mathfrak{b} = (\varepsilon)$. Then $\mathfrak{ab} = \mathfrak{a}^2 = 0$. On the other hand,

$$\mathfrak{a} \otimes_A \mathfrak{b} \cong \operatorname{coker}(\cdot\varepsilon \colon A \to A) \otimes_A (\varepsilon) \cong \operatorname{coker}(\cdot\varepsilon \colon (\varepsilon) \to (\varepsilon)) \cong \operatorname{coker}(0 \colon (\varepsilon) \to (\varepsilon)) \cong \mathfrak{a}.$$

In this case, $\mathfrak{a} \otimes_A \mathfrak{b} \to \mathfrak{ab}$ is definitely not injective.

(ii) Now to a very common example. Let A be a principal ideal domain, and let $\mathfrak{a} = (f) \subseteq A$, $\mathfrak{b} = (g) \subseteq A$ with $fg \neq 0$.

It is true that any two non-zero ideals in A are isomorphic as A-modules. Thus $A \cong (f)$, $A \cong (g)$ and $A \cong (f)(g) = (fg)$ as A-modules, given by $1 \mapsto f$, $1 \mapsto g$ and $1 \mapsto fg$, resp. Using Proposition 4.25 (i), we obtain

$$\mathfrak{a} \otimes_A \mathfrak{b} = (f) \otimes_A (g) \cong A \otimes_A A \cong A \cong (fg) = \mathfrak{ab}$$

as A-modules, given by $f \otimes g \mapsto 1 \otimes 1 \mapsto 1 \mapsto fg$. Thus $\mathfrak{a} \otimes_A \mathfrak{b} \to \mathfrak{ab}$ is injective.

(iii) Now the fun begins. Check this out: Consider $A = k[X,Y]$ and $\mathfrak{a} = \mathfrak{b} = (X,Y) \subseteq A$. Then $\mathfrak{a}^2 = (X^2, XY, Y^2)$.

In general, we have $\mathfrak{a}^n \otimes_A A/\mathfrak{a} \cong \mathfrak{a}^n/\mathfrak{a}^{n+1}$. This can be proved as follows: If $\mathfrak{a} = (a_i \mid i \in I)$, then $A^{\oplus I} \to A \to A/\mathfrak{a} \to 0$ is a presentation of $A/\mathfrak{a}$ with the obvious map $A^{\oplus I} \to A$, $e_i \mapsto a_i$. By Corollary 4.27, we have

$$\mathfrak{a}^n \otimes_A A/\mathfrak{a} \cong \mathfrak{a}^n \otimes_A \operatorname{coker}((a_i)_i \colon A^{\oplus I} \to A) \cong \operatorname{coker}((a_i)_i \colon (\mathfrak{a}^n)^{\oplus I} \to \mathfrak{a}^n) \cong \mathfrak{a}^n / \left(\bigoplus_{i \in I} a_i \mathfrak{a}^n \right) = \mathfrak{a}^n/\mathfrak{a}^{n+1}.$$

Thus by Exercise 8.10, we have

$$\mathfrak{a}^2 \otimes_A (A/\mathfrak{a}) \cong \mathfrak{a}^2/\mathfrak{a}^3 = k\bar{X}^2 \oplus k\bar{X} \cdot \bar{Y} \oplus k\bar{Y}^2 \cong k^3.$$

On the other hand, by Proposition 4.25 and Example 4.28, we have

$$(\mathfrak{a} \otimes_A \mathfrak{a}) \otimes_A A/\mathfrak{a} \cong \mathfrak{a} \otimes_A (\mathfrak{a} \otimes_A A/\mathfrak{a}) \cong \mathfrak{a} \otimes_A (A/\mathfrak{a})^{\oplus 2} \cong (\mathfrak{a} \otimes_A A/\mathfrak{a})^{\oplus 2} \cong (A/\mathfrak{a})^{\oplus 4} \cong k^4.$$

In conclusion, $\mathfrak{a} \otimes_A \mathfrak{a} \twoheadrightarrow \mathfrak{a}^2$ is surjective, but not injective, as otherwise we would have $k^3 \cong k^4$. Concretely, $0 \neq z := X \otimes Y - Y \otimes X \in \mathfrak{a} \otimes_A \mathfrak{a}$ is in the kernel of $\mathfrak{a} \otimes_A \mathfrak{a} \to \mathfrak{a}^2$, since $z \mapsto XY - YX = 0$.

But strangely, we have

$$Xz = X^2 \otimes Y - XY \otimes X = X \otimes XY - X \otimes XY = 0$$

in $\mathfrak{a} \otimes_A \mathfrak{a}$, as $X \otimes X \in \mathfrak{a} \otimes_A \mathfrak{a}$. We also have $Yz = 0$ in the same way. Thus z is a torsion element (there exists a regular $a \in A$ such that $az = 0$, the analogue concept of 'zero divisors' in A-modules), although $\mathfrak{a}$ is a torsion-free module over the integral domain A. Moreover, there is the inclusion $k \cong A/\mathfrak{a} \hookrightarrow \mathfrak{a} \otimes_A \mathfrak{a}$, $1 \mapsto z$, i. e. $\mathfrak{a} \otimes_A \mathfrak{a}$ is not torsion-free as an A-module, but torsion-free as an $A/\mathfrak{a}$-module (since this is a k-vector space).

4.6 Algebras

Lect. 10
11.05.23

Definition 4.30. Let A be a ring. An **A-algebra** is a ring B together with a ring homomorphism $\phi \colon A \to B$.
For two A-algebras $\phi \colon A \to B$ and $\psi \colon A \to C$, an **A-algebra map** (or **A-algebra homomorphism**) between B and C is a ring map $f \colon B \to C$ such that $f \circ \phi = \psi$.

Remark 4.31. (From me.) The definition is indeed equivalent to the following definition: An A-algebra B is an A-module with an A-bilinear map $B \times B \to B$. It is unital, associative and commutative, if B together with the bilinear map defines a unital and commutative ring.

Proof: Given a ring map $\phi \colon A \to B$, B is already an abelian group with a B-linear map $B \times B \to B$, $(b_1, b_2) \mapsto b_1 b_2$. This becomes an A-module and an A-bilinear map via $a \bullet b := \phi(a)b$.

Conversely, given a unital associative commutative A-algebra B together with an A-bilinear map $\phi \colon B \times B \to B$, B is already a ring. We obtain a ring map $\psi \colon A \to B$ via $a \mapsto a1_B$ (for multiplicativity, we have $\psi(a_1 a_2) = (a_1 a_2)1_B = \phi((a_1 a_2)1_B, 1_B) = \phi(a_1 1_B, a_2 1_B) = \psi(a_1)\psi(a_2)$).

For (unital) A-algebra maps $f \colon B \to C$, whatever the definition, they have to fulfil $f(b+c) = f(b) + f(c)$, $f(bc) = f(bc)$, $f(a \bullet b) = a \bullet f(b)$ and $f(1) = 1$.

Example 4.32. Why do we care about A-algebras?

(i) Assume that we are given a polynomial $\sum_{i=0}^n a_i T^i$ over a ring A (or a system of polynomial equations). Then we can interpret it in any other ring B which interprets A naturally. That is, for any A-algebra $\phi \colon A \to B$, we have the polynomial $\sum_{i=0}^n \phi(a_i) T^i$ over B.

E. g., $Y^2 - \frac{1}{2}X^3 \in \mathbb{Z}[\frac{1}{2}]$ can be reduced modulo n for odd n, i. e. via $\mathbb{Z}[\frac{1}{2}] \twoheadrightarrow \mathbb{F}_3, \mathbb{F}_5, \mathbb{Z}/27$, etc. We can also embed this polynomial, i. e. via $\mathbb{Z}[\frac{1}{2}] \hookrightarrow \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

(ii) In rings like $\mathbb{C}[T]$ or $\mathbb{C}[X,Y]/(XY)$, we usually want to view the elements of $\mathbb{C}$ as *constants*, i. e. a ring map $\mathbb{C}[T] \to \mathbb{C}[T]$ should map $a \mapsto a$ for all $a \in \mathbb{C}$. This can be formalised by considering these rings as $\mathbb{C}$-algebras via $\mathbb{C} \hookrightarrow \mathbb{C}[T]$.

In this case, we have $\mathrm{Hom}_{\mathbb{C}\text{-Alg}}(\mathbb{C}[T],\mathbb{C}[T]) \cong \mathbb{C}[T]$ via $f \mapsto f(T)$. This is because each $\mathbb{C}$-algebra map $f\colon \mathbb{C}[T] \to \mathbb{C}[T]$ is uniquely determined by $f(T)$ since $f(\sum_{i=0}^n a_i T^i) = \sum_{i=0}^n a_i f(T)^i$. This homomorphism space of $\mathbb{C}$-algebra maps is particularly well-behaved. In comparison, $\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{C},\mathbb{C})$, and thus $\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{C}[T],\mathbb{C}[T])$, have cardinality at least $2^{2^{\aleph_0}}$.

(One can show that $\mathbb{C}/\mathbb{Q}$ has a so called *transcendence basis* T such that T is algebraically independent and $\mathbb{C}/\mathbb{Q}(T)$ is algebraic (see Definition 6.37). Since $\overline{\mathbb{Q}(T)} = \mathbb{C}$, we can lift any field homomorphism $\mathbb{Q}(T) \to \mathbb{C}$ to a field homomorphism $\mathbb{C} \to \mathbb{C}$. Every field homomorphism $\mathbb{Q}(T) \to \mathbb{C}$ is uniquely determined by $T \to \mathbb{C}$. We have $2^{\aleph_0} = |\mathbb{C}| = |\overline{\mathbb{Q}(T)}| = |\mathbb{Q}(T)| = |T|$. Hence there are at least $|T|^{|T|} = 2^{2^{\aleph_0}}$ homomorphisms $\mathbb{Q}(T) \to \mathbb{C}$, and thus at least $2^{2^{\aleph_0}}$ homomorphisms $\mathbb{C} \to \mathbb{C}$.)

Remark 4.33. We have the following general fact: Let $\phi\colon A \to B$ be an A-algebra. The universal property of polynomial and quotient rings then gives the bijection

$$\mathrm{Hom}_{A\text{-Alg}}(A[T_i, i \in I]/(f_j, j \in J), B) \cong \{(b_i)_{i\in I} \in B^I \mid \phi(f_j)(b_i) = 0 \text{ for all } i \in I,\, j \in J\}, \quad f \mapsto (f(T_i))_{i\in I}.$$

Example 4.34. We have

$$\mathrm{Hom}_{\mathbb{C}\text{-Alg}}(\mathbb{C}[X,Y]/(XY),\mathbb{C}) \cong \{(x,y) \in \mathbb{C}^2 \mid xy = 0\}.$$

4.7 Scalar Extension of Modules

Definition 4.35. Let $\phi\colon A \to B$ be an A-algebra and M an A-module. We view B as an A-module via $a \bullet b := \phi(a)b$. Then $B \otimes_A M$ is a B-module via

$$b \bullet (x \otimes m) := (bx) \otimes m.$$

We call it the **extension of scalars** from A to B of M.

Proof. The key point is to show that the map $(b, x \otimes m) \mapsto b \bullet (x \otimes m)$ is well-defined. Multiplication with $b \in B$ defines an A-linear map $[b]\colon B \to B$, $x \mapsto bx$ on B. By functoriality of the tensor product, this gives an A-linear map $[b] \otimes \mathrm{id}_M\colon B \otimes_A M \to B \otimes_A M$, $x \otimes m \mapsto (bx) \otimes m$.

The B-module axioms are immediate (the last one follows by linear extension of the scalar multiplication):

$$\begin{aligned} 1(x \otimes m) &= (1x) \otimes m = x \otimes m, \\ c(b(x \otimes m)) &= (cbx) \otimes m = (cb)(x \otimes m), \\ (b_1 + b_2)(x \otimes m) &= (b_1 x + b_2 x) \otimes m = b_1(x \otimes m) + b_2(x \otimes m), \\ b(x_1 \otimes m_1 + x_2 \otimes m_2) &= b(x_1 \otimes m_1) + b(x_2 \otimes m_2). \end{aligned}$$

□

Remark 4.36. The map $\phi \otimes \mathrm{id}_M$ gives rise to a map of A-modules

$$M \cong A \otimes_A M \to B \otimes_A M, \qquad m \mapsto 1 \otimes m \mapsto 1 \otimes m.$$

Proposition 4.37. *Let $\phi\colon A \to B$ be an A-algebra, and let $M \cong \mathrm{coker}((a_{ij})_{ij}\colon A^{\oplus J} \to A^{\oplus I})$ be a presentation of an A-module. Then $B \otimes_A M \cong \mathrm{coker}((\phi(a_{ij}))_{ij}\colon B^{\oplus J} \to B^{\oplus I})$ as a B-module.*

Proof. By Corollary 4.27, we already have $B \otimes_A M \cong \mathrm{coker}((a_{ij})_{ij}\colon B^{\oplus J} \to B^{\oplus I})$ as A-modules. Since $a \bullet b = \phi(a)b$ by definition, we obtain the stated presentation as B-modules. □

Remark 4.38. Special cases:

(i) $A/\mathfrak{a} \otimes_A M \cong M/\mathfrak{a}M$ (also as $A/\mathfrak{a}$-modules). See Exercise 8.23.

(ii) $A[S^{-1}] \otimes_A M \cong M[S^{-1}]$. We will show this in Proposition 4.52.

(iii) $A[T] \otimes_A M \cong \bigoplus_{i=0}^\infty MT^i =: M[T]$. Since $A[T] = \bigoplus_{i=0}^\infty AT^i \cong \bigoplus_{i=0}^\infty A$, we have $A[T] \otimes_A M \cong \bigoplus_{i=0}^\infty A \otimes_A M \cong \bigoplus_{i=0}^\infty M \cong M[T]$, using Proposition 4.25.

4.8 Tensor Product of A-Algebras

Proposition 4.39. *Let $\phi\colon A \to B$ and $\psi\colon A \to C$ be A-algebras. Then $B \otimes_A C$ becomes a ring via*

$$(b \otimes c)(b' \otimes c') \coloneqq (bb') \otimes (cc').$$

Moreover, the following hold:

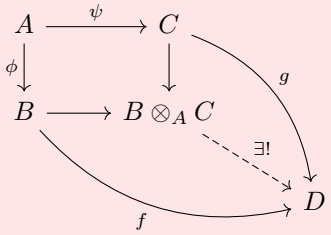
(i) *In fact, $B \otimes_A C$ is an A-algebra via*

$$\phi \otimes \psi\colon A \cong A \otimes_A A \to B \otimes_A C, \qquad a \mapsto \phi(a) \otimes 1 = 1 \otimes \psi(a).$$

In particular, $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ and $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$ are A-algebra maps, and the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\psi} & C \\ {\scriptstyle\phi}\downarrow & & \downarrow \\ B & \longrightarrow & B \otimes_A C \end{array}$$

(ii) ***Universal property for tensor products of algebras**: If $\chi\colon A \to D$ is any A-algebra, and $f\colon B \to D$ and $g\colon C \to D$ are A-algebra maps, then there is a unique factorisation through $B \otimes_A C$:*



Note that by definition of A-algebra maps, we have $f \circ \phi = \chi = g \circ \psi$.

In other words: The category of A-algebras has coproducts, namely the tensor product of A-algebras. This coproduct is a pushout in the category of rings.

To prove this proposition, we need the following statement.

Observation 4.40. Similar to the universal property of tensors product, we can prove a **universal property of multi-tensor products**.

An **A-multilinear map** is a map $f\colon M_1 \times \cdots \times M_r \to P$ with A-modules $M_1, \ldots, M_r, P$, such that f is linear in every variable. Then for each such A-multilinear map f, we obtain the following unique factorisation:

$$\begin{array}{ccc} M_1 \times \cdots \times M_r & \longrightarrow & M_1 \otimes_A \cdots \otimes_A M_r \\ & {\scriptstyle f}\searrow & \downarrow {\scriptstyle \exists!} \\ & & P \end{array}$$

As always with universal properties, the multi-tensor product is unique up to unique isomorphism.

Proof.

(i) We will show that multiplication in $B \otimes_A C$ is well-defined. Consider the A-multilinear map

$$B \times C \times B \times C \to B \otimes_A C, \qquad (b_1, c_1, b_2, c_2) \mapsto (b_1 b_2) \otimes (c_1 c_2).$$

By the universal property of multi-tensor products, it factors uniquely through

$$B \otimes_A C \otimes_A B \otimes_A C \to B \otimes_A C, \qquad b_1 \otimes c_1 \otimes b_2 \otimes c_2 \mapsto b_1 b_2 \otimes c_1 c_2.$$

Precomposing with the universal A-bilinear map

$$(B \otimes_A C) \times (B \otimes_A C) \to B \otimes_A C \otimes_A B \otimes_A C, \qquad (b_1 \otimes c_1, b_2 \otimes c_2) \mapsto b_1 \otimes c_1 \otimes b_2 \otimes c_2,$$

we obtain the existence of such a multiplication

(ii) Checking that $B \otimes_A C$ is a ring is easy. We only need to check the axioms for multiplication. Commutativity and associativity for $B \otimes_A C$ follow directly from B and C. Distributivity holds by definition, and the identity element is $1 \otimes 1$.

Also, $\phi \otimes \psi$ being a ring map is also immediate. $\phi(a) \otimes 1 = a(1 \otimes 1) = 1 \otimes \psi(a)$ follows from the definition of the A-module structure on B and C.

(iii) Now to the universal property: Given two A-algebra maps $f\colon B \to D$ and $g\colon C \to D$, we consider the map $B \times C \to D$, $(b, c) \mapsto f(b)g(c)$. This is A-bilinear, since $f(ab) = f(\phi(a)b) = f(\phi(a))f(b) = \chi(a)f(b) = af(b)$, and similarly for g (f is an A-algebra map by assumption, i. e. $f(\phi(a)) = \chi(a)$). Thus, by the universal property of tensor products, it factors uniquely trough the A-linear map

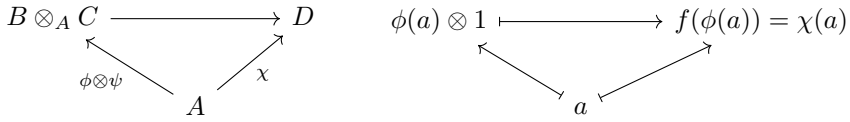
$$B \otimes_A C \to D, \qquad b \otimes c \mapsto f(b)g(c).$$

This is even a ring map, since it is multiplicative:

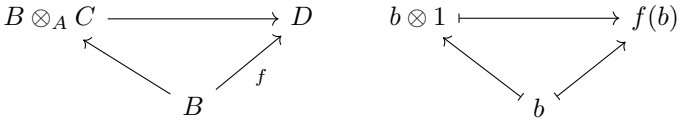
$$\left(\sum_{i=1}^{n} b_i \otimes c_i\right)\left(\sum_{j=1}^{m} b'_j \otimes c'_j\right) = \sum_{i,j} b_i b'_j \otimes c_i c'_j$$

$$\mapsto \sum_{i,j} f(b_i b'_j)g(c_i c'_j) = \left(\sum_{i=0}^{n} f(b_i)g(c_i)\right)\left(\sum_{j=0}^{m} f(b'_j)g(c'_j)\right).$$

This is even an A-algebra map, since the following diagram commutes:



Finally, the following diagram commutes (similarly for C):



□

4.9 Alternative Construction of Coproducts

Definition 4.41. A **presentation** for an A-algebra B is the isomorphism $A[T_i, i \in I]/\mathfrak{a} \cong B$ where $\mathfrak{a} \subseteq A[T_i, i \in I]$ is an ideal.

Lemma 4.42. *Every A-algebra admits a presentation.*

Proof. Let $\phi\colon A \to B$ be an A-algebra. Set $I := B$. By the universal property of polynomial rings, we obtain the ring homomorphism $p\colon A[T_b, b \in B] \twoheadrightarrow B$, $a \mapsto \phi(a)$, $T_b \mapsto b$, which is obviously surjective. Set $\mathfrak{a} := \ker(p)$. By the homomorphism theorem, we obtain $A[T_b, b \in B]/\mathfrak{a} \cong B$. □

Proposition 4.43. *Let $\phi\colon A \to B$ be an A-algebra. Then $B \otimes_A (A[T_i, i \in I]/\mathfrak{a}) \cong B[T_i, i \in I]/(\phi(\mathfrak{a}))$ as A-algebras.*

Proof. We first note that $B[T_i, i \in I]/(\phi(\mathfrak{a}))$ is an A-algebra, for there exists the ring map

$$A \xrightarrow{\phi} B \hookrightarrow B[T_i, i \in I]/(\phi(\mathfrak{a})).$$

Consider the following A-algebra maps:

$$B \xrightarrow{b \mapsto b} B[T_i, i \in I]/(\phi(\mathfrak{a})) \xleftarrow[\phi(a) \leftarrow\!\shortmid a]{T_i \leftarrow\!\shortmid T_i} A[T_i, i \in I]/\mathfrak{a}$$

We want to show that $B[T_i, i \in I]/(\phi(\mathfrak{a}))$ has the universal property of tensor products for algebras. Say $\chi\colon A \to D$ is any A-algebra. Then, since A-algebra maps fix A, we have the bijection

$$\mathrm{Hom}_{A\text{-Alg}}(A[T_i, i \in I]/\mathfrak{a}, D) \cong \{h \in \mathrm{map}(\{T_i \mid i \in I\}, D) \mid \chi(f)(h(T_i)) = 0 \text{ for all } f \in \mathfrak{a},\ i \in I\}.$$

Notice that $f \in \mathfrak{a} \subseteq A[T_i, i \in I]$ are polynomials. $\chi(f)$ denotes the polynomial with coefficients under χ. Thus we obtain

$$\begin{aligned}
&\mathrm{Hom}_{A\text{-Alg}}(B, D) \times \mathrm{Hom}_{A\text{-Alg}}(A[T_i, i \in I]/\mathfrak{a}, D)\\
&\quad\cong \{(g, h) \in \mathrm{Hom}_{A\text{-Alg}}(B, D) \times \mathrm{map}(\{T_i \mid i \in I\}, D) \mid g(\phi(f))(h(d_i)) = 0 \text{ for all } f \in \mathfrak{a},\ i \in I\}\\
&\quad\cong \{\tilde{g} \in \mathrm{Hom}_{A\text{-Alg}}(B[T_i, i \in I], D) \mid \tilde{g}(f) = 0 \text{ for all } f \in (\phi(\mathfrak{a}))\}\\
&\quad\cong \mathrm{Hom}_{A\text{-Alg}}(B[T_i, i \in I]/(\phi(\mathfrak{a})), D).
\end{aligned}$$

By the universal property, we have

$$\mathrm{Hom}_{A\text{-Alg}}(B, D) \times \mathrm{Hom}_{A\text{-Alg}}(A[T_i, i \in I]/\mathfrak{a}, D) \cong \mathrm{Hom}_{A\text{-Alg}}(B \otimes_A A[T_i, i \in I]/\mathfrak{a}, D).$$

Hence $B[T_i, i \in I]/(\phi(\mathfrak{a}))$ fulfils the universal property of tensor products for algebras, and therefore must be isomorphic to $B \otimes_A (A[T_i, i \in I]/\mathfrak{a})$. □

Remark 4.44. Given presentations of two A-algebras $B = A[T_i, i \in I]/\mathfrak{b}$ and $C = A[S_j, j \in J]/\mathfrak{c}$, we obtain an alternative description of the A-algebra $B \otimes_A C$ (with Noether's isomorphism theorem in the second step):

$$B \otimes_A C \cong B[S_j, j \in J]/(\mathfrak{c}) \cong A[T_i, S_j, i \in I, j \in J]/(\mathfrak{b}) + (\mathfrak{c}).$$

Remark 4.45. Special cases.

(i) $A/\mathfrak{a} \otimes_A A/\mathfrak{b} \cong A/\mathfrak{a} + \mathfrak{b}$.

(ii) $B \otimes_A A[S^{-1}] \cong B[\phi(S)^{-1}]$ for any A-algebra $\phi\colon A \to B$.

(iii) $B \otimes_A \kappa(\mathfrak{p}) \cong B/(\phi(\mathfrak{p}))[\phi(A \setminus \mathfrak{p})^{-1}]$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$, where $\kappa(\mathfrak{p}) \coloneqq A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ and $A_\mathfrak{p} \coloneqq A[(A \setminus \mathfrak{p})^{-1}]$ (cf. Observation 2.68).

We can proof these as follows:

(i) Take $B \coloneqq A/\mathfrak{b}$, $I \coloneqq \varnothing$ and $\phi\colon A \to B$ the canonical projection. Then $B \otimes_A A/\mathfrak{a} \cong B/(\phi(\mathfrak{a})) = (A/\mathfrak{b})/(\mathfrak{a} + \mathfrak{b}/\mathfrak{b}) \cong A/\mathfrak{a} + \mathfrak{b}$ via Noether's isomorphism theorem.

(ii) We use the standard construction of localisations: Take $I \coloneqq S$ and $\mathfrak{a} \coloneqq (sT_s - 1 \mid s \in S)$. By definition, $A[S^{-1}] \cong A[T_i, i \in I]/\mathfrak{a}$. This gives $B \otimes_A A[S^{-1}] \cong B[T_i, i \in I]/(\phi(s)T_s - 1 \mid s \in S) \cong B[\phi(S)^{-1}]$.

(iii) We combine the above statements:

$$B \otimes_A \kappa(\mathfrak{p}) \cong B \otimes_A A/\mathfrak{p} \otimes_A A_\mathfrak{p} \cong B/(\phi(\mathfrak{p})) \otimes_A A_\mathfrak{p} \cong B/(\phi(\mathfrak{p}))[\phi(A \setminus \mathfrak{p})^{-1}].$$

4.10 Example: Tensoring Field Extensions

Example 4.46. Let L/K be a finite separate field extension. By the primitive element theorem, we can write $L \cong K[T]/(f(T))$ as a K-algebra, where $f \in K[T]$ is the minimal polynomial of the primitive element and has only simple roots in $\overline{K}$ by separability. Assume that M is a splitting field of f over K, e. g. a normal closure of L in $\overline{K}$ or $\overline{K}$ itself. Then by Remark 4.38 and the Chinese remainder theorem 8.5 (f splits into pairwise different linear factors over M, and $M[T]/(T - \lambda) \cong M$ for any $\lambda \in M$), we obtain an isomorphism

$$M \otimes_K L \cong M \otimes_K K[T]/(f(T)) \cong M[T]/(f(T)) \cong \prod_{i=1}^{[L:K]} M$$

of M-algebras.

For example, if L/K is a Galois extension, i. e. it is finite, separabel and normal, then $L \otimes_K L \cong L^{[L:K]}$. For an example of a non-Galois extension, consider $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$ (L/K is not normal). We obtain with the Chinese remainder theorem 8.5

$$L \otimes_K L \cong L[T]/(T^3 - 2) \cong L \times L[T]/(T^2 + \sqrt[3]{2} + (\sqrt[3]{2})^2).$$

Example 4.47. Let $K = \mathbb{F}_p(x)$ and $L = K(\sqrt[p]{x})$, where p is prime and x is some transcendental element. Notice that L/K is inseparable, as $\operatorname{char}(L) = p$, whence we can write the minimal polynomial of $\sqrt[p]{x}$ as $T^p - x = (T - \sqrt[p]{x})^p$. But L/K is simple, so $L \cong K[T]/(T^p - x)$. We obtain with Remark 4.38

$$L \otimes_K L \cong L \otimes_K K[T]/(T^p - x) \cong L[T]/(T^p - x) \cong L[T]/((T - \sqrt[p]{x})^p) \cong L[\varepsilon]/(\varepsilon^p),$$

where the last isomorphism is given by $T \mapsto \varepsilon + \sqrt[p]{x}$. Clearly, $\bar{\varepsilon} \in L[\varepsilon]/(\varepsilon^p)$ is a zero divisor, hence $L \otimes_K L$ is non-reduced.

Example 4.48. Let K be any field. We consider the transcendental field extensions $L = K(X) = \operatorname{Quot}(K[X])$ and $M = K(Y) = \operatorname{Quot}(K[Y])$ over K. By Proposition 4.43, we obtain

$$L \otimes_K M \cong L[Y][(K[Y] \setminus \{0\})^{-1}] \cong K[X,Y][(K[X] \setminus \{0\})^{-1}, (K[Y] \setminus \{0\})^{-1}].$$

Recall the following:

(i) We know from Proposition 2.55 that for any localisation $A \to A[S^{-1}]$, there exists a bijection $\operatorname{Spec}(A[S^{-1}]) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}$.

(ii) We know from Exercise 8.13 that

$$\operatorname{Spec}(K[X,Y]) = \{(0)\} \sqcup \{(f) \mid f \in K[X,Y] \text{ irreducible}\} \sqcup \operatorname{MaxSpec}(K[X,Y]).$$

Moreover, every $\mathfrak{m} \in \operatorname{MaxSpec}(K[X,Y])$ is of the form $\mathfrak{m} = (\pi, g)$ with prime $\pi \in K[X]$ and irreducible $\bar{g} \in K/\pi[X,Y]$. In particular, all $\mathfrak{m}$ intersect with $K[X]$ non-trivially (or if we understand $K[X,Y] \cong K[Y][X]$, then $\mathfrak{m} \cap K[Y]$ is non-trivial too).

Hence

$$\begin{aligned}\operatorname{Spec}(L \otimes_K M) &= \{\mathfrak{p} \in \operatorname{Spec}(K[X,Y]) \mid \mathfrak{p} \cap (K[X] \cup K[Y]) = \{0\}\} \\ &= \{(0)\} \sqcup \{(f) \mid f \in K[X,Y] \text{ irreducible}, f \notin K[X] \cup K[Y]\}.\end{aligned}$$

For example, the elements $X + aY + c \in K[X,Y]$ with $a, b \in K$ and $a \neq 0$ are irreducible and mutually coprime, hence they generate mutually different prime ideals. Furthermore, elements like $Y^2 - X$, $Y^5X + Y^2 - X$, $Y^5 - X^3 + X$ yield additional prime ideals. In particular, by Exercise 8.11, $L \otimes_K M$ is a principal ideal domain.

4.11 Localisation of Modules

Lect. 11
15.05.23

The definition is very similar to the localisation of rings. For reference, see [AtMac, ch. 3].

Definition 4.49. Let A be a ring, $S \subseteq A$ a multiplicative subset and M an A-module. We define

$$S^{-1}M := \left\{ \frac{m}{s} \;\middle|\; m \in M, s \in S \right\} / \sim$$

with the following equivalence relation: $m_1/s_1 \sim m_2/s_2$ if and only if there exists an $s_3 \in S$ such that $s_3 s_1 m_2 = s_3 s_2 m_1$. We endow $S^{-1}M$ with an A-module structure via

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \qquad \text{and} \qquad a \bullet \frac{m}{s} := \frac{am}{s}.$$

We could check that addition and multiplication defined in this way is well-defined, but this proof is identical to the localisation of rings. We call $S^{-1}M$ the **localisation** of M over S.

Remark 4.50. This construction is functorial.

(i) We have the natural map $M \to S^{-1}M$, $m \mapsto \frac{m}{1}$, which is in general not injective (cf. Corollary 2.47).

(ii) It follows that any A-linear map $f\colon M \to N$ induces a map $S^{-1}f\colon S^{-1}M \to S^{-1}N$, $m/s \mapsto f(m)/s$ (e. g. by the universal property we will prove, or by straightforward calculation).

Now a very important property.

Proposition 4.51. *Localisations are exact: Assume that*

$$M \xrightarrow{f} N \xrightarrow{g} P$$

is an exact sequence of A-modules. Then the sequence

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$$

is exact.

Proof. Since $g \circ f = 0$ by exactness, we have $0 = S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$ by functoriality, that is $\operatorname{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Conversely, let $\frac{n}{s} \in \ker(S^{-1}g)$. This means $g(n)/s = \frac{0}{1}$, i. e. there exists some $t \in S$ such that $0 = tg(n) = g(tn)$. Thus $tn \in \ker(g) = \operatorname{im}(f)$ by exactness, say $tn = f(m)$ with $m \in M$. Then $(S^{-1}f)(\frac{m}{st}) = f(m)/(st) = \frac{tn}{st} = \frac{n}{s}$. Hence we just showed $\ker(S^{-1}g) \subseteq \operatorname{im}(S^{-1}g)$. □

Proposition 4.52. *Let $S \subseteq A$ be a multiplicative subset of a ring A and M an A-module. Then we have the isomorphism*

$$S^{-1}A \otimes_A M \cong S^{-1}M, \qquad \frac{a}{s} \otimes m \mapsto \frac{am}{s}.$$

Proof. We show that $S^{-1}A \times M \to S^{-1}M$, $(\frac{a}{s}, m) \mapsto \frac{am}{s}$ is well-defined and A-bilinear. Suppose that $a_1/s_1 = a_2/s_2$ in $S^{-1}A$, i. e. there exists some $s \in S$ such that $ss_2a_1 = ss_1a_2$. This yields $ss_2a_1m = ss_1a_2m$ for all $m \in M$, whence $a_1m/s_1 = a_2m/s_2$, so this map is well-defined. Additivity in the right variable and multiplicativity of this map is trivial. For additivity in the left variable, we have

$$\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}, m\right) = \left(\frac{a_1s_2 + a_2s_1}{s_1s_2}, m\right) \mapsto \frac{a_1s_2m + a_2s_1m}{s_1s_2} = \frac{a_1m}{s_1} + \frac{a_2m}{s_2}.$$

By the universal property of tensor products, the existence of this A-bilinear map implies the existence of $S^{-1} \otimes_A M \to S^{-1}M$ from the proposition. It is clearly surjective as $\frac{1}{s} \otimes m \mapsto \frac{m}{s}$ for all $\frac{m}{s} \in S^{-1}M$. For injectivity, assume that $\sum_{i=1}^n a_i/s_i \otimes m_i$ lies in the kernel. Put $s \coloneqq \prod_{i=1}^n s_i$ as the common denominator. Then

$$\sum_{i=1}^n \frac{a_i}{s_i} \otimes m_i = \sum_{i=1}^n \frac{a_i \prod_{j\neq i} s_j}{s} \otimes m_i = \sum_{i=1}^n \frac{1}{s} \otimes \left(a_i \prod_{j\neq i} s_j\right) m_i = \frac{1}{s} \otimes m, \quad \text{where } m \coloneqq \sum_{i=1}^n \left(a_i \prod_{j\neq i} s_j\right) m_i.$$

This was possible since $a_i \prod_{j\neq i} s_j \in A$ and $\frac{1}{s} \otimes m_i \in S^{-1}A \otimes_A M$. By assumption, we have $\frac{1}{s} \otimes m \mapsto \frac{m}{s} = 0$. This means there exists some $t \in S$ such that $tm = 0$. We obtain $\frac{1}{s} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$. □

Remark 4.53. In particular, we can interpret $S^{-1}M$ as a scalar extension of M to $S^{-1}A$, so $S^{-1}M$ is an $S^{-1}A$-module via $\frac{a}{s} \bullet \frac{m}{t} = \frac{am}{st}$. Any A-linear map $S^{-1}f\colon S^{-1}M \to S^{-1}N$ is in fact $S^{-1}A$-linear.

Example 4.54. If we apply $\mathbb{Q} \otimes_{\mathbb{Z}} -$ to the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \longrightarrow \mathbb{Z}/n \longrightarrow 0$$

we obtain the following exact sequence:

$$0 \longrightarrow \mathbb{Q} \xrightarrow{\cdot n} \mathbb{Q} \longrightarrow 0 \longrightarrow 0$$

Notice that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0$ since $p \otimes \bar{z} = \frac{p}{n} \otimes n\bar{z} = 0$ for all $p \in \mathbb{Q}$ and $\bar{z} \in \mathbb{Z}/n$.

Corollary 4.55.

(i) *Let $f\colon M \to N$ be an A-linear map. Then*

$$\ker(S^{-1}f) = S^{-1}\ker(f), \qquad \operatorname{coker}(S^{-1}f) = S^{-1}\operatorname{coker}(f), \qquad \operatorname{im}(S^{-1}f) = S^{-1}\operatorname{im}(f).$$

In particular, if $M \subseteq N$ is a submodule, then $S^{-1}(N/M) = S^{-1}N/S^{-1}M$.

(ii) *Let $M_1, M_2 \subseteq N$ be A-submodules. Then*

$$S^{-1}(M_1 \cap M_2) = S^{-1}M_1 \cap S^{-1}M_2 \qquad \text{and} \qquad S^{-1}M_1 + S^{-1}M_2 = S^{-1}(M_1 + M_2).$$

(iii) *Let M be an A-module. Then $S^{-1}(S^{-1}M) \cong S^{-1}M$.*

(iv) *Furthermore, for A-modules M and N, we have*

$$S^{-1}M \otimes_A S^{-1}N \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_A N.$$

All isomorphisms have in common that they map $m \otimes n \mapsto m \otimes n$ for all $m \in M$ and $n \in N$.

(v) ***Universal property of localisations of modules**: Let M be an A-module and N an $S^{-1}A$-module (i. e. an A-module such that multiplication with any $s \in S$ is bijective). Then for all A-linear maps $f\colon M \to N$, there exists a unique factorisation through an $S^{-1}A$-linear map:*

$$\begin{array}{ccc} M & \longrightarrow & S^{-1}M \\ & \searrow^{f} & \downarrow{\scriptstyle \exists!} \\ & & N \end{array}$$

Proof. (From me.)

(i) By exactness of localisations and Example 4.15, applying S^{-1} to the exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow M \xrightarrow{f} N \longrightarrow \operatorname{coker}(f) \longrightarrow 0$$

yields the relations for the kernel and cokernel (we actually obtain equality since $\ker(f)$ is a submodule of M and $\operatorname{coker}(f)$ is a quotient module of N). For the image, we see that by exactness in N and $S^{-1}N$,

$$\operatorname{im}(S^{-1}f) = \ker(S^{-1}N \twoheadrightarrow S^{-1}\operatorname{coker}(f)) = S^{-1}\ker(N \twoheadrightarrow \operatorname{coker}(f)) = S^{-1}\operatorname{im}(f).$$

For $M \subseteq N$, consider $f\colon M \hookrightarrow N$ and $\operatorname{coker}(S^{-1}f)$.

(ii) Clearly, $S^{-1}(M_1 \cap M_2) \subseteq S^{-1}M_1 \cap S^{-1}M_2$. Conversely, let $m_1/s_1 = m_2/s_2$ in $S^{-1}M_1 \cap S^{-1}M_2$ with $m_1 \in M_1$ and $m_2 \in M_2$. Then there is some $s \in S$ such that $ss_2m_1 = ss_1m_2 =: m \in M_1 \cap M_2$. It follows that $ss_1s_2m_1 = s_1m$ and hence $m_1/s_1 = m/(ss_1s_2) \in S^{-1}(M_1 \cap M_2)$.

Again, $S^{-1}(M_1 + M_2) \subseteq S^{-1}M_1 + S^{-1}M_2$ is obvious. The converse follows directly from the definition of addition in $S^{-1}(M_1 + M_2)$.

(iii) This follows from (iv) and Proposition 4.52 via

$$S^{-1}(S^{-1}M) \cong S^{-1}A \otimes_A S^{-1}M \cong S^{-1}(A \otimes_A M) \cong S^{-1}M.$$

(iv) $S^{-1}M \otimes_A S^{-1}N \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N$ is Exercise 8.30 (iii).

By Proposition 4.52 and Exercise 8.30 (ii), we have

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \cong (S^{-1}A \otimes_{S^{-1}A} (S^{-1}A \otimes_A M)) \otimes_A N \\ &\cong S^{-1}A \otimes_A M \otimes_A N. \end{aligned}$$

The last tensor product is isomorphic to $S^{-1}(M \otimes_A N)$ as well as $S^{-1}M \otimes_A N$.

(v) Since multiplication with any $s \in S$ is bijective, for every $n \in N$ and $s \in S$, there is some $n' \in N$ such that $sn' = n$. Hence $\frac{n}{s} = n' \in N$ is well-defined.

Then $\phi\colon S^{-1}M \to N$, $\phi(\frac{m}{s}) = f(m)/s$ is an $S^{-1}A$-linear map. ϕ is well-defined: Suppose that $m_1/s_1 = m_2/s_2$ in $S^{-1}M$, i. e. $ss_2m_1 = ss_1m_2$ for some $s \in S$. Then $\phi(m_1/s_1) = \phi((ss_2m_1)/(ss_1s_2)) = f(ss_1m_2)/(ss_1s_2) = f(m_2)/s_2 = \phi(m_2/s_2)$.

Clearly, ϕ makes the stated diagram commute and is unique such that $\phi(\frac{m}{1}) = f(m)/1 = f(m)$. □

Remark 4.56. Part (v) holds more generally: Let B be an A-algebra, M an A-module and N a B-module. Then

$$\mathrm{Hom}_A(M,N) \cong \mathrm{Hom}_B(B \otimes_A M, N), \qquad \phi \mapsto [b \otimes m \mapsto b\phi(m)].$$

Evidently, $b \otimes m \mapsto b\phi(m)$ is indeed B-linear. The inverse of this map is given by $[m \mapsto \psi(1 \otimes m)] \hookleftarrow \psi$.

Example 4.57. Let $M \cong A^{\oplus I}$ be a free A-module. Then

$$S^{-1}M \cong S^{-1}A \otimes_A M \cong S^{-1}A \otimes_A A^{\oplus I} \cong (S^{-1}A \otimes_A A)^{\oplus I} \cong (S^{-1}A)^{\oplus I}$$

since $S^{-1}A \otimes_A -$ and $(\cdot)^{\oplus I}$ commute. For example, consider $S := \{p^k \mid k \geq 0\} \subseteq \mathbb{Z}$ for some $p \in \mathbb{Z}$. Then $S^{-1}\mathbb{Z}[T] = \mathbb{Z}[T][p^{-1}] \cong \mathbb{Z}[p^{-1}][T]$ considered as $\mathbb{Z}$-modules.

But S^{-1} need not commute with infinite direct products. For example, consider the submodule $S^{-1}\mathbb{Z}[\![T]\!] = \mathbb{Z}[\![T]\!][p^{-1}] \subseteq \mathbb{Z}[p^{-1}][\![T]\!]$. This submodule is, however, proper because $\mathbb{Z}[\![T]\!][p^{-1}]$ consists of those power series whose denominators are bounded. So e. g. $1 + T/p + T^2/p^2 + T^3/p^3 + \cdots \notin S^{-1}\mathbb{Z}[T]$.

4.12 Passing to Local Rings

Notation 4.58. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. Then the $A_\mathfrak{p}$-module $M_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}M$ is the **localisation** of M at $\mathfrak{p}$.

Proposition 4.59. *Let M be an A-module. Then the following are equivalent:*

(i) $M = 0$.

(ii) $M_\mathfrak{p} = 0$ *for all* $\mathfrak{p} \in \mathrm{Spec}(A)$.

(iii) $M_\mathfrak{m} = 0$ *for all* $\mathfrak{m} \in \mathrm{MaxSpec}(A)$.

Proof. We already have (i) $\implies$ (ii) $\implies$ (iii) (recall $\mathrm{MaxSpec}(A) \subseteq \mathrm{Spec}(A)$). For (iii) $\implies$ (i), let $x \in M$. We have to show that $x = 0$.

Consider the **annihilator ideal** $\mathrm{Ann}(x) := \{a \in A \mid ax = 0\}$ of x. Since $M_\mathfrak{m} = 0$ and $1 \in A \setminus \mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, we always have $\frac{x}{1} = 0$. By definition of localisations of modules, there exists some $a \in A \setminus \mathfrak{m}$ such that $ax = 0$. This implies $\mathrm{Ann}(x) \nsubseteq \mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, hence, by Corollary 2.19, $\mathrm{Ann}(x) = A$. In particular, since $1 \in \mathrm{Ann}(x)$, we have $x = 1x = 0$. □

Now we show a converse to Proposition 4.51.

Proposition 4.60. *Assume that*

$$M \xrightarrow{f} N \xrightarrow{g} P \tag{4.61}$$

is a sequence of A-modules such that $g \circ f = 0$, and that for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, the sequence

$$M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{g_\mathfrak{m}} P_\mathfrak{m}$$

is exact. Then (4.61) is exact.

Proof. Since $g \circ f = 0$, we already know $\mathrm{im}(f) \subseteq \ker(g)$, hence $\ker(g)/\mathrm{im}(f)$ exists. Thus with Corollary 4.55, we have $(\ker(g)/\mathrm{im}(f))_\mathfrak{m} = \ker(g)_\mathfrak{m}/\mathrm{im}(f)_\mathfrak{m} = \ker(g_\mathfrak{m})/\mathrm{im}(f_\mathfrak{m}) = 0$ by exactness. Since this holds for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, Proposition 4.59 implies $\ker(g)/\mathrm{im}(f) = 0$, i. e. $\ker(g) = \mathrm{im}(f)$. □

We will now prove the converse of Corollary 3.39 what we promised to do.

Corollary 4.62. *Let $f\colon A^{\oplus J} \to A^n$ be an A-linear map with $|J| \geq n$. Let $I_n(f) := (\det(f_Q) \mid Q \subseteq J, |Q| = n)$ with $f_Q = f \circ i_Q$ and $i_Q\colon A^n \hookrightarrow A^{\oplus J}$, i. e. f_Q are quadratic $n \times n$-minors. If $I_n(f) = A$, then f is surjective.*

Proof. We want to apply Proposition 4.60 to the sequence $A^{\oplus J} \to A^n \to 0$. It is enough to show that $f_\mathfrak{m}\colon A_\mathfrak{m}^{\oplus J} \to A_\mathfrak{m}^n$ is surjective for all $\mathfrak{m} \in \mathrm{MaxSpec}(A)$.

$A_\mathfrak{m}$ is a local ring with the unique maximal ideal $\mathfrak{m}A_\mathfrak{m}$ (Remark 2.62), so $A_\mathfrak{m}^\times = A_\mathfrak{m} \setminus \mathfrak{m}A_\mathfrak{m}$ (Example 2.21). Since $I_n(f) = A$, so depending on $\mathfrak{m} \neq A$, there must be some Q such that $\det(f_Q) \notin \mathfrak{m}$ (otherwise we would

have $I_n(f) \subseteq \mathfrak{m}$), hence $\det(f_{Q,\mathfrak{m}}) \in A_{\mathfrak{m}}^\times$. By Lemma 3.35, $f_{Q,\mathfrak{m}}$ is invertible, so $f_{Q,\mathfrak{m}} = f_{\mathfrak{m},Q} = f_{\mathfrak{m}} \circ i_{Q,\mathfrak{m}}$ is an isomorphism. In particular, $f_{\mathfrak{m}}$ is surjective. □

There are many different implications of this, all known as *Nakayama's lemma*. The following version might be the clearest and argues similarly around $\operatorname{coker}(f)$.

Corollary 4.63 (**Nakayama's lemma**). *Let $(A, \mathfrak{m})$ be a local ring, and let M be a finitely generated A-module. Then $M/\mathfrak{m}M = 0$ implies $M = 0$.*

Proof. We chose any presentation

$$A^{\oplus J} \xrightarrow{f} A^{\oplus n} \longrightarrow M \longrightarrow 0$$

(J might not be finite). Let $\kappa(\mathfrak{m}) \coloneqq A/\mathfrak{m}$ be the residue field of $\mathfrak{m}$. $\kappa(\mathfrak{m}) \otimes_A -$ is right-exact, so applying it yields the following exact sequence:

$$\kappa(\mathfrak{m})^{\oplus J} \xrightarrow{f \bmod \mathfrak{m}} \kappa(\mathfrak{m})^{\oplus n} \longrightarrow M/\mathfrak{m}M = 0 \longrightarrow 0$$

So $f \bmod \mathfrak{m}$ is surjective. As $\kappa(\mathfrak{m})$ is a field, there exists a subset $Q \subseteq J$ with $|Q| = n$ such that $\det(f_Q) \notin \mathfrak{m}$ (we know from linear algebra that we can choose n column vectors of f such that they form a basis of $\operatorname{im}(f)$). Since A is local, we have $\det(f_Q) \in A^\times = A \setminus \mathfrak{m}$, hence $I_n(f) = A$. By Corollary 4.62, f is surjective, and $M \cong \operatorname{coker}(f) = 0$. □

Corollary 4.64 (**Nakayama's lemma**). *Let A be any ring, N a finitely generated A-module, and $f\colon M \to N$ an A-linear map such that $f \bmod \mathfrak{m}\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. Then f is surjective.*

Proof. (From me.) Let $\mathfrak{m} \in \operatorname{MaxSpec}(A)$. Since $f \bmod \mathfrak{m}$ is surjective, by Proposition 4.51, $(f \bmod \mathfrak{m})_{\mathfrak{m}} = f_{\mathfrak{m}} \bmod \mathfrak{m}$ is surjective as well (here, we used Corollary 4.55, namely $(M/\mathfrak{m}M)_{\mathfrak{m}} = M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}}$, and similarly for $N/\mathfrak{m}N$). Now $A_{\mathfrak{m}}$ is local and $N_{\mathfrak{m}}$ is finitely generated, so by the same argument as in Corollary 4.63, $f_{\mathfrak{m}}$ is surjective. As this is true for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$, wee see through Proposition 4.60 that f is surjective. □

Example 4.65. The A-linear map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is not surjective. But for all primes $p \in \mathbb{Z}$ (which precisely generate all maximal ideals), $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}/p\mathbb{Q} = 0$ is surjective. Thus the finite generation assumption of N in Corollary 4.64 is essential.

4.13 Flatness

Definition 4.66. An A-module M is **flat** if $M \otimes_A -$ is an exact operation (functor), i. e. for all exact sequences $N \to P \to Q$ of A-modules, $M \otimes_A N \to M \otimes_A P \to M \otimes_A Q$ is exact.

Example 4.67.

(i) A is a flat A-module (tensoring with A does nothing).

(ii) If $(M_i)_{i \in I}$ is a family of flat A-modules, then $\bigoplus_{i \in I} M_i$ is flat. (Recall that $(\bigoplus_{i \in I} M_i) \otimes_A N \cong \bigoplus_{i \in I} (M_i \otimes_A N)$. Moreover, for a family $(f_i)_{i \in I}$ of A-linear maps, we have $\ker(\bigoplus_{i \in I} f_i) = \bigoplus_{i \in I} \ker(f_i)$ and $\operatorname{im}(\bigoplus_{i \in I} f_i) = \bigoplus_{i \in I} \operatorname{im}(f_i)$.)

In particular, free A-modules $M \cong A^{\oplus I}$ are flat.

(iii) By Propositions 4.51 and 4.52, any localisation $S^{-1}A$ is a flat A-module. More generally, by Corollary 4.55, if M is a flat A-module, then $S^{-1}M$ is a flat A-module as well (we have $S^{-1}M \otimes_A - \cong S^{-1}(M \otimes_A -)$ as functors).

Example 4.68. In general, the quotient of a flat module by a flat module is not flat.

Let $f \in A \setminus A^\times$ be regular, i. e. $\cdot f\colon A \to A$, $a \mapsto fa$ is injective by Remark 4.38. Then $A/(f) \otimes_A (\cdot f\colon A \to A) \cong \cdot 0\colon A/(f) \to A/(f)$ is not injective (notice that $A/(f) \neq 0$). Therefore $A/(f)$ is not a flat A-module (but of course a flat $A/(f)$-module).

Proposition 4.69. *Let M be an A-module. Then the following are equivalent:*

(i) *M is flat as an A-module.*

(ii) *$M_\mathfrak{p}$ is flat as an $A_\mathfrak{p}$-module for all $\mathfrak{p} \in \operatorname{Spec}(A)$.*

(iii) *$M_\mathfrak{m}$ is flat as an $A_\mathfrak{m}$-module for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$.*

Proof.

- (i) $\implies$ (ii): Let $N \to P \to Q$ be an exact sequence of $A_\mathfrak{p}$-modules. Then by Corollary 4.55, we have $(M \otimes_A N)_\mathfrak{p} \cong M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N$, and similarly for P and Q. Since M and $(A \setminus \mathfrak{p})^{-1}A$ are flat (see Example 4.67), $(A \setminus \mathfrak{p})^{-1}A \otimes_A M \cong M_\mathfrak{p}$ is flat.
- (ii) $\implies$ (iii): Trivial since $\operatorname{MaxSpec}(A) \subseteq \operatorname{Spec}(A)$.
- (iii) $\implies$ (i): Let $N \to P \to Q$ be an exact sequence of A-modules. Since localisations are exact, we know that the sequence $N_\mathfrak{m} \to P_\mathfrak{m} \to Q_\mathfrak{m}$ of A-modules or $A_\mathfrak{m}$-modules is exact. By assumption, $M_\mathfrak{m} \otimes_{A_\mathfrak{m}} N_\mathfrak{m} \to M_\mathfrak{m} \otimes_{A_\mathfrak{m}} P_\mathfrak{m} \to M_\mathfrak{m} \otimes_{A_\mathfrak{m}} Q_\mathfrak{m}$ is exact. Because of Corollary 4.55, $M_\mathfrak{m} \otimes_{A_\mathfrak{m}} N_\mathfrak{m} \cong (M \otimes_A N)_\mathfrak{m}$ holds true, and similarly for P and Q. As this holds for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$, with Proposition 4.60, we conclude that $M \otimes_A N \to M \otimes_A P \to M \otimes_A Q$ is exact, i. e. M is flat as an A-module. □

In order to further characterise flatness, we need the following statement multiple times. This is based on the following universal heuristic: If we want to show something for an element x of an algebraic structure A, x can be written as a relation consisting of only finitely many generators. Thus there is a finitely generated substructure with the same properties as A. Lect. 12 22.05.23

Lemma 4.70. *Suppose that $\sum_{i=1}^r m_i \otimes p_i = 0$ in a tensor product $M \otimes_A P$. Then there exist finitely generated A-submodules $M_0 \subseteq M$ and $P_0 \subseteq P$ such that $m_1, \dots, m_r \in M_0$, $p_1, \dots, p_r \in P_0$ and $\sum_{i=1}^r m_i \otimes p_i = 0$ in $M_0 \otimes_A P_0$.*

Proof. Recall the explicit construction of tensors products in Proposition 4.6. We defined $M \otimes_A P$ (up to unique isomorphism) by

$$\left(\bigoplus_{(m,p) \in M \times P} A \cdot m \mathbin{\tilde{\otimes}} p \right) / D_{M \times P} \qquad \text{with} \qquad D_{M \times P} \coloneqq \left\langle \begin{matrix} (m_1 + m_2) \mathbin{\tilde{\otimes}} p - m_1 \mathbin{\tilde{\otimes}} p - m_2 \mathbin{\tilde{\otimes}} p, \\ (am) \mathbin{\tilde{\otimes}} p - a \cdot m \mathbin{\tilde{\otimes}} p, \dots \end{matrix} \right\rangle.$$

Here, $m \mathbin{\tilde{\otimes}} p$ are free generators, i. e. each $(m, p) \in M \times P$ corresponds to a basis vector in $A^{\oplus M \times P}$.

The image of $m \mathbin{\tilde{\otimes}} p$ under the quotient map $A^{\oplus M \times P} \to A^{\oplus M \times P} / D_{M \times P}$ is $m \otimes p \in M \otimes_A P$. Hence $\sum_{i=1}^r m_i \otimes p_i = 0$ means $\sum_{i=1}^r m_i \mathbin{\tilde{\otimes}} p_i \in D_{M \times P}$. Thus it is an A-linear combination of finitely many generators of $D_{M \times P}$, so we can collect all finitely many elements from M (resp. P) appearing in these generators and form a finitely generated submodule $M_0 \subseteq M$ (resp. $P_0 \subseteq P$) such that $\sum_{i=1}^r m_i \mathbin{\tilde{\otimes}} p_i \in D_{M_0 \times P_0}$.

Finally, we can append $m_1, \dots, m_r$ (resp. $p_1, \dots, p_r$) to the list of generators of M_0 (resp. P_0). Thus we have $m_1, \dots, m_r \in M_0$ and $p_1, \dots, p_r \in P_0$ as well as $\sum_{i=1}^r m_i \otimes p_i = 0$ in $M_0 \otimes_A P_0$. □

Proposition 4.71. *Let M be an A-module. Then the following are equivalent:*

(i) *M is flat.*

(ii) *For all injective A-linear maps $f \colon N \hookrightarrow P$, the map $\mathrm{id}_M \otimes f \colon M \otimes_A N \hookrightarrow M \otimes_A P$ is injective as well.*

(iii) *The same as (ii), but for finitely generated N and P.*

Proof.

- (i) $\implies$ (ii): We apply exactness of M to any exact sequence $0 \to N \to P$.
- (ii) $\implies$ (iii): Trivial.

- (ii) $\implies$ (i): Assume that
$$N \xrightarrow{f} P \xrightarrow{g} Q$$
is any exact sequence.
Since $0 \to \ker(g) \to P \to \operatorname{im}(g) \to 0$ is exact, tensoring with M yields that
$$0 \longrightarrow M \otimes_A \ker(g) \longrightarrow M \otimes_A P \longrightarrow M \otimes_A \operatorname{im}(g) \longrightarrow 0 \tag{4.72}$$
is exact: Exactness in $M \otimes_A P$ and $M \otimes_A \operatorname{im}(g)$ follows from the right-exactness of $M \otimes_A -$ (Proposition 4.20), and exactness in $M \otimes_A \ker(g)$ follows from the assumption.
Next by linearity of $\mathrm{id}_M \otimes g$, $\operatorname{im}(\mathrm{id}_M \otimes g)$ is generated by the images of $m \otimes p \in M \otimes_A P$ under $\mathrm{id}_M \otimes g$, i. e. by all elementary tensors $m \otimes g(p)$. Hence the natural map $M \otimes_A \operatorname{im}(g) \twoheadrightarrow \operatorname{im}(\mathrm{id}_M \otimes g)$ is surjective. Furthermore, as the canonical inclusion $\operatorname{im}(g) \hookrightarrow Q$ is injective, $M \otimes_A \operatorname{im}(g) \hookrightarrow M \otimes_A Q$ is injective by assumption. Since $\operatorname{im}(\mathrm{id}_M \otimes g) \subseteq M \otimes_A Q$, we thus obtain $M \otimes_A \operatorname{im}(g) \cong \operatorname{im}(\mathrm{id}_M \otimes g)$.
Then by exactness of (4.72), we have $M \otimes_A \ker(g) \cong \ker(\mathrm{id}_M \otimes g)$. This is actually an equality since $M \otimes_A \ker(g) \subseteq \ker(\mathrm{id}_M \otimes g)$. Moreover, $\mathrm{id}_M \otimes f \colon M \otimes_A N \twoheadrightarrow M \otimes_A \operatorname{im}(f)$ is always surjective. Since $\operatorname{im}(f) = \ker(g)$, we see that
$$\mathrm{id}_M \otimes f \colon M \otimes_A N \twoheadrightarrow M \otimes_A \operatorname{im}(f) = M \otimes_A \ker(g) = \ker(\mathrm{id}_M \otimes g),$$
that is $\operatorname{im}(\mathrm{id}_M \otimes f) = \ker(\mathrm{id}_M \otimes g)$, hence $M \otimes_A N \to M \otimes_A P \to M \otimes_A Q$ is exact.
- (iii) $\implies$ (ii): Let $f \colon N \hookrightarrow P$ be any A-linear injection, and let $\sum_{i=1}^r m_i \otimes n_i \in \ker(\mathrm{id}_M \otimes f)$, i. e. $\sum_{i=1}^r m_i \otimes f(n_i) = 0$. We want to show that $\sum_{i=1}^r m_i \otimes n_i = 0$ already, i. e. $\mathrm{id}_M \otimes f$ is injective.
By Lemma 4.70, there exists a finitely generated submodule $P_0 \subseteq P$ such that $f(n_1), \dots, f(n_r) \in P_0$ and $\sum_{i=1}^r m_i \otimes f(n_i) = 0$ in $M \otimes_A P_0$. Set $N_0 \coloneqq (n_1, \dots, n_r) \subseteq N$. We obtain the restriction $f|_{N_0} \colon N_0 \hookrightarrow P_0$ of finitely generated submodules, which is also injective. By assumption, $\mathrm{id}_M \otimes f|_{N_0}$ is injective, so $\sum_{i=1}^r m_i \otimes n_i \in \ker(\mathrm{id}_M \otimes f|_{N_0}) = 0$. Therefore $\sum_{i=1}^r m_i \otimes n_i = 0$ holds not only in $M \otimes_A N_0$, but certainly also in $M \otimes_A N$. □

Proposition 4.73. *Assume that every finitely generated submodule of an A-module M is flat. Then M is flat.*

Proof. Given $f \colon N \hookrightarrow P$, we want to show that $\mathrm{id}_M \otimes f \colon M \otimes_A N \hookrightarrow M \otimes_A P$ is injective again. This finishes the proof by Proposition 4.71.

Consider $\sum_{i=1}^r m_i \otimes n_i \in \ker(\mathrm{id}_M \otimes f)$, i. e. $\sum_{i=1}^r m_i \otimes f(n_i) = 0$. By Lemma 4.70, there is a finitely generated submodule $M_0 \subseteq M$ such that $m_1, \dots, m_r \in M_0$ and $\sum_{i=1}^r m_i \otimes f(n_i) = 0$ in $M_0 \otimes_A P$. Since M_0 is flat by assumption, $\mathrm{id}_{M_0} \otimes f$ is injective by Proposition 4.71. As $\sum_{i=1}^r m_i \otimes n_i \in \ker(\mathrm{id}_{M_0} \otimes f)$, we have $\sum_{i=1}^r m_i \otimes n_i = 0$ in $M_0 \otimes_A N$, hence also in $M \otimes_A N$. □

4.14 Flatness and Torsion

Torsion is the analogous concept to zero divisors in rings.

Definition 4.74. Let A be an integral domain and M an A-module. We call an element $x \in M$ **torsion** if there exists an $f \in A \setminus \{0\}$ such that $fx = 0$. We denote by $M_f \coloneqq \{x \in M \mid fx = 0\}$ the **f-torsion**. The **torsion submodule** M_{tors} of M is the set of all torsion elements. On the other hand, we call M **torsion-free** if $M_{\mathrm{tors}} = 0$.

Proof. M_f and M_{tors} are indeed submodules of M. For all $a \in A$ and $x \in M_f$ (resp. $x \in M_{\mathrm{tors}}$), we have $fax = afx = 0$ (resp. there is some $f \in A \setminus \{0\}$ such that this holds). □

Exercise 4.75. Show that for any A-module M, M/M_{tors} is torsion-free.

Solution. Suppose that $\bar{x} \in M/M_{\mathrm{tors}}$ is torsion w. r. t. $0 \neq f \in A$, i. e. $f\bar{x} = \overline{fx} = 0$. So $fx \in M_{\mathrm{tors}}$, say w. r. t. $0 \neq e \in A$. Hence $x \in M_{\mathrm{tors}}$ w. r. t. $0 \neq ef \in A$, hence $\bar{x} = 0$ and M/M_{tors} is torsion-free.

Example 4.76. Let A be a principal ideal domain and M a finitely generated A-module. Then M is torsion-free if and only if M is free.

This follows from the structure theorem 3.52. In particular, there are no cyclic direct summands, i. e. summands of the form $A/(a_i)$, i. e. all elementary divisors are 0.

Theorem 4.77. *Let A be a principal ideal domain and M an A-module. Then M is torsion-free if and only if M is flat.*

Proof. If M is torsion-free, then clearly, every finitely generated submodule $M_0 \subseteq M$ is torsion-free. Thus by the structure theorem 3.52, any such M_0 is free, hence flat (A is a flat A-module, and so is $A^{\oplus n}$ for any $n \geq 0$, see Example 4.67). Proposition 4.73 says that M is flat.

Conversely, assume M is flat. A is an integral domain, so for all $0 \neq f \in A$, the multiplication map $f\colon A \to A$ is injective. By Proposition 4.71, the multiplication map $f\colon M \to M$ is again injective (we have $M \otimes_A A \cong M$). We obtain $M_f = \ker(f) = 0$, so $M_{\text{tors}} \subseteq \bigcup_{f \in A \setminus \{0\}} M_f = 0$. □

Example 4.78. We know that $\mathbb{Q}$, $\mathbb{Z}[\frac{1}{n}]$, etc. are flat (and also torsion-free) $\mathbb{Z}$-modules as they are localisations, see Example 4.67. This generally holds for any localisation of $\mathbb{Z}$.

Some new examples for flat $\mathbb{Z}$-modules:

(i) $\prod_{i \in \mathbb{Z}} \mathbb{Z}$ is torsion-free and thus flat (if $(a_i)_{i \in \mathbb{Z}}$ is torsion w. r. t. $0 \neq f \in \mathbb{Z}$, then $fa_i = 0$, i. e. $a_i = 0$ for all $i \in \mathbb{Z}$). It is actually not free, which is quite difficult to prove.

(ii) Let $M \coloneqq \prod_{p \text{ prime}} \mathbb{F}_p$. Then $(1, 1, \dots) \in M$ is non-torsion, as otherwise there is some integer that is divisible by all primes. Hence M/M_{tors} is non-trivial, torsion-free by Exercise 4.75 and thus flat.

(iii) $\langle \frac{1}{p} \mid p \text{ prime} \rangle \subseteq \mathbb{Q}$ is not finitely generated and not free (e. g. $\frac{1}{2} + \frac{1}{3} = 5\frac{1}{6}$). But as a subset of the field $\mathbb{Q}$, it is certainly torsion-free and hence flat.

The following generalises Proposition 4.71, which we will not prove.

Proposition 4.79. *Let M be an A-module. Then the following are equivalent:*

(i) *M is flat.*

(ii) *For all finitely generated ideals $\mathfrak{a} \subseteq A$, the map $\mathfrak{a} \otimes_A M \hookrightarrow M$, $a \otimes m \mapsto am$ is injective.*

Proof.

- (i) $\implies$ (ii): This follows directly from Proposition 4.71, applied to $\mathfrak{a} \hookrightarrow A$.
- (ii) $\implies$ (i): This is actually not difficult, but a bit lengthy. No new techniques are required. See [Sta, 00HD] . □

Remark 4.80.

(i) As $\operatorname{im}(\mathfrak{a} \otimes_A M \hookrightarrow M) = \mathfrak{a}M$, we alternatively have: M is flat if and only if $\mathfrak{a} \otimes_A M \cong \mathfrak{a}M$ for all finitely generated $\mathfrak{a} \subseteq A$.

(ii) Many define torsion more generally for all rings: If A is a ring and M an A-module, then $x \in M$ is *torsion* if there exists a regular $f \in A$ such that $fx = 0$.

Thus if $\mathfrak{a} = (f)$ for a regular $f \in A$, then $\ker((f) \otimes_A M \to fM) = M_f$. Roughly speaking, the above statements should be read as 'flatness is equivalent to $\mathfrak{a}$-torsion-freeness for all finitely generated ideals $\mathfrak{a} \subseteq A$'.

We will not prove the following statement too.

Proposition 4.81. *Let A be a local ring, and let M be a finitely generated A-module. Then M is flat if and only if for all $\mathfrak{p} \in \operatorname{Spec}(A)$, $M_\mathfrak{p}$ is free as an $A_\mathfrak{p}$-module.*

Proof. We know by Proposition 4.69 that M is flat if and only if $M_\mathfrak{p}$ is flat as an $A_\mathfrak{p}$-module for all $\mathfrak{p} \in \operatorname{Spec}(A)$. It remains to show that $M_\mathfrak{p}$ being flat is equivalent to $M_\mathfrak{p}$ being free.

We already know the direction 'freeness implies flatness', see Example 4.67. For the converse, recall that $A_\mathfrak{p}$ is a local ring. We now refer to the renowned [Mat, sec. (3.G), Prop. 3.1]. □

Remark 4.82. The above generalises the following statement: Let A be a principal ideal domain and M a finitely generated A-module. Then M is flat if and only if M is free. (The 'only if' direction follows from the structure theorem 3.52.)

4.15 The Snake Lemma

We now come to a classical tool in homological algebra.

Lemma 4.83 (**snake lemma**). *Assume that we are given the commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

with exact rows. Then there is a natural ***connecting map*** $\delta\colon \ker(f_3) \to \operatorname{coker}(f_1)$ *such that*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f_1) & \longrightarrow & \ker(f_2) & \longrightarrow & \ker(f_3) & \xrightarrow{\delta} & \\ & & & & & & & & \\ & & \operatorname{coker}(f_1) & \longrightarrow & \operatorname{coker}(f_2) & \longrightarrow & \operatorname{coker}(f_3) & \longrightarrow & 0 \end{array}$$

is an exact sequence (this looks like a snake, hence the name).

Proof. The proof is a typical example of a **diagram chase**: We choose an element of one term and iteratively consider images and preimages along a bunch of arrows, 'chasing' the element around the diagram. Most of the time, there is only one obvious way to diagram chase.

(i) We first define δ. We will refer to the following diagram:

$$\begin{array}{ccccc} & & b & \longmapsto & a \\ & & \downarrow & & \downarrow \\ d & \longmapsto & c & \longmapsto & 0 \end{array}$$

Let $a \in \ker(f_3)$. Since $M_2 \to M_3$ is surjective, there exists a preimage $b \in M_2$ of a. Let $c \coloneqq f_2(b) \in N_2$. Since the right square commutes and $b \mapsto a \mapsto 0$, we must have $b \mapsto c \mapsto 0$ as well, i. e. $c \in \ker(N_2 \to N_3)$. By exactness of the bottom row, there exists a preimage $d \in N_1$ of c. Now define $\delta(a) \coloneqq \bar{d}$.

(ii) δ above is well-defined. d as a preimage of c is already unique since by exactness of the bottom row, $N_1 \to N_2$ is injective.

Suppose that $b' \in M_2$ would be another choice for a preimage of a, and let $c' \coloneqq f_2(b') \in N_2$ and $d' \in N_1$ the preimage of c'. We will refer to the following diagram:

$$\begin{array}{ccccc} e & \longmapsto & b - b' & \longmapsto & 0 \\ \downarrow & & \downarrow & & \\ d - d' & \longmapsto & c - c' & & \end{array}$$

Then $b - b' \in \ker(M_2 \to M_3)$ as $b - b' \mapsto a - a = 0$. By the exactness of the top row, we have $b - b' \in \operatorname{im}(M_1 \to M_2)$, so there exists a preimage $e \in M_1$ of $b - b'$. Since the left square commutes and $e \mapsto b - b' \mapsto c - c'$, we must have $e \mapsto f_1(e) \mapsto c - c'$. But by the exactness of the bottom row, $N_1 \to N_2$ is injective, so $f_1(e) = d - d'$. Hence $d - d' \in \operatorname{im}(f_1)$ and $\bar{d} = \bar{d'}$.

(iii) Next we check that $\ker(f_i) \to \ker(f_{i+1})$ and $\operatorname{coker}(f_i) \to \operatorname{coker}(f_{i+1})$ are well-defined.

If $a \in \ker(f_i)$, then $a \mapsto f_i(a) = 0 \mapsto 0$. Since the corresponding square commutes, if $b \in M_{i+1}$ is the image of a, then $a \mapsto b \mapsto 0$, so $b \in \ker(f_{i+1})$.

If $a \in \operatorname{im}(f_i)$, then there is a $b \in M_i$ such that $f_i(b) = a$. Let $c \in M_{i+1}$ be the image of b. Since the corresponding square commutes and $b \mapsto c \mapsto f_{i+1}(c)$, we have $b \mapsto a \mapsto f_{i+1}(c)$, so the image of a under $N_i \to N_{i+1}$ is $f_{i+1}(c) \in \operatorname{im}(f_{i+1})$.

(iv) Now comes the tedious part: Checking exactness in each of the six terms. Only $\ker(f_3)$, being the most difficult to prove, was shown in the lecture.

(a) $\ker(f_1)$: By definition, $\ker(f_1) \to \ker(f_2)$ is the restriction of $M_1 \to M_2$ on $\ker(f_1)$. Since the latter map is injective, so must be the former.

(b) $\ker(f_2)$: Let $a \in \operatorname{im}(\ker(f_1) \to \ker(f_2)) \subseteq \operatorname{im}(M_1 \to M_2)$. By exactness in M_2, we have $a \in \ker(M_2 \to M_3)$, i. e. $a \mapsto 0 \in M_3$. That means $a \in \ker(\ker(f_2) \to \ker(f_3))$.
Conversely, let $a \in \ker(\ker(f_2) \to \ker(f_3)) \subseteq \ker(M_2 \to M_3)$. By exactness in M_2, we also have $a \in \operatorname{im}(M_1 \to M_2)$, so pick any preimage $b \in M_1$ of a. Since the left square commutes and $b \mapsto a \mapsto 0$, we must have $b \mapsto f_1(b) \mapsto 0$ as well. But we know that $N_1 \to N_2$ is injective, hence $f_1(b) = 0$ and $b \in \ker(f_1)$. This shows $a \in \operatorname{im}(\ker(f_1) \to \ker(f_2))$.

(c) $\ker(f_3)$: Let $a \in \operatorname{im}(\ker(f_2) \to \ker(f_3))$. We will construct $\delta(a)$. Pick any preimage $b \in \ker(f_2)$ of a, i. e. $f_2(b) = 0$, so $\delta(a) = 0$. Hence $a \in \ker(\delta)$.
Conversely, let $a \in \ker(\delta)$. We construct b, c, d exactly as in the description of δ. Then $\bar{d} = 0$, i. e. $d \in \operatorname{im}(f_1)$. So pick any $e \in M_1$ such that $f(e) = d$, and let $x \in M_2$ be the image of e. By exactness in M_2, $x \in \ker(M_2 \to M_3)$. So $M_2 \to M_3$ maps $b - x \mapsto a - 0 = a$, and $b' \coloneqq b - x \in M_2$ is a preimage of a. As the left square commutes and $e \mapsto d \mapsto c$, we have $e \mapsto x \mapsto c$, thus $f_2(b') = c - c = 0$, i. e. $b' \in \ker(f_2)$. We obtain $a \in \operatorname{im}(\ker(f_2) \to \ker(f_3))$.

(d) $\operatorname{coker}(f_1)$: Let $\bar{d} \in \operatorname{im}(\delta)$. W. l. o. g., we can choose $d \in N_1$ so that d admits the construction of a, b, c as in the definition of δ. By the definition of δ, we see that $c = f_2(b)$, i. e. $c \in \operatorname{im}(f_2)$. Hence $\bar{d} \mapsto \bar{c} = 0$, and $\bar{d} \in \ker(\operatorname{coker}(f_1) \to \operatorname{coker}(f_2))$.
Conversely, let $\bar{d} \in \ker(\operatorname{coker}(f_1) \to \operatorname{coker}(f_2))$. Let $c \in N_2$ be the image of d, so $\bar{d} \mapsto \bar{c} = 0$, i. e. $c \in \operatorname{im}(f_2)$. Choose any $b \in M_2$ such that $f_2(b) = c$, and let $a \in M_3$ be the image of b. We see from the definition of δ, especially since δ is well-defined, that $\delta(a) = \bar{d}$. This shows $\bar{d} \in \operatorname{im}(\delta)$.

(e) $\operatorname{coker}(f_2)$: Let $\bar{a} \in \operatorname{im}(\operatorname{coker}(f_1) \to \operatorname{coker}(f_2))$, and $\bar{b} \in \operatorname{coker}(f_1)$ be the preimage of $\bar{a}$. Let $x \in N_2$ be the image of b, so $a' \coloneqq a - x \in \operatorname{im}(f_2)$. Chose any $c \in M_2$ such that $f_2(c) = a'$. Furthermore, let $d \in N_3$ be the image of a. By exactness in N_2, we have $x \in \ker(N_2 \to N_3)$, so $a' \mapsto d - 0 = d$. Let $e \in M_3$ be the image of c. Since the right square commutes and $c \mapsto a' \mapsto d$, we must have $c \mapsto e \mapsto d$. This shows $d \in \operatorname{im}(f_3)$, hence $\bar{a} \mapsto \bar{d} = 0$ and $\bar{a} \in \ker(\operatorname{coker}(f_2) \to \operatorname{coker}(f_3))$.
Let $\bar{a} \in \ker(\operatorname{coker}(f_2) \to \operatorname{coker}(f_3))$ and $b \in N_3$ the image of a. Then $\bar{a} \mapsto \bar{b} = 0$, i. e. $b \in \operatorname{im}(f_3)$. So let $c \in M_3$ such that $f_3(c) = b$. As $M_2 \to M_3$ is surjective, we find a preimage $d \in M_2$ of c. Since the right square commutes and $d \mapsto c \mapsto b$, we must have $d \mapsto f_2(d) \mapsto b$. Note that $N_2 \to N_3$ maps $a' \coloneqq a - f_2(d) \mapsto b - b = 0$, hence $a' \in \ker(N_2 \to N_3)$. By exactness in N_2, we have $a' \in \operatorname{im}(N_1 \to N_2)$, so there is a preimage $e \in N_1$ of a'. Further note that $a - a' = f_2(d) \in \operatorname{im}(f_2)$. Thus $\bar{e} \mapsto \bar{a}' = \bar{a}$ and $\bar{a} \in \operatorname{im}(\operatorname{coker}(f_1) \to \operatorname{coker}(f_2))$.

(f) $\operatorname{coker}(f_3)$: By definition, $\operatorname{coker}(f_2) \to \operatorname{coker}(f_3)$ is the quotient map of $N_2 \to N_3$ over $\operatorname{im}(f_2)$. Since the latter map is surjective, so must be the former. □

Remark 4.84. (From me.) In fact, we have not used the injectivity of $M_1 \to M_2$ or the surjectivity of $N_2 \to N_3$. Therefore the exactness in M_1 and N_3 is superfluous.

Example 4.85. Consider multiplication with $n \in \mathbb{Z}$ on the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of $\mathbb{Z}$-modules:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot n} & & \downarrow{\scriptstyle \cdot n} & & \downarrow{\scriptstyle \cdot n} & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathbb{Z}/n & & 0 & & 0 & &
\end{array}$$

The rows are exact, the terms at the very top and bottom are the kernels and cokernels, resp. Note that $\frac{1}{n}\mathbb{Z}$ is not the localisation, but rather the set $\{\frac{a}{n} \mid a \in \mathbb{Z}\}$.

The snake lemma 4.83 then gives that there is a natural isomorphism $\delta\colon \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \mathbb{Z}/n$. This can be constructed explicitly: Let $\frac{a}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Pick any lift of $\frac{a}{n} + \mathbb{Z}$, say $\frac{a}{n} \in \mathbb{Q}$. The image of $\frac{a}{n}$ is $\frac{a}{n} \cdot n = a \in \mathbb{Q}$. Then there is exactly one preimage $a \in \mathbb{Z}$ of a. Hence $\delta(\frac{a}{n} + \mathbb{Z}) = a \bmod (n)$.

Example 4.86. The above example can be generalised. Let A be a ring and $f \in A$ arbitrary. Given an exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ of A-modules, we can consider multiplication with f:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot f} & & \downarrow{\scriptstyle \cdot f} & & \downarrow{\scriptstyle \cdot f} & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

The snake lemma 4.83 states that the following long sequence is exact:

$$0 \longrightarrow M_{1,f} \longrightarrow M_{2,f} \longrightarrow M_{3,f} \xrightarrow{\delta} M_1/fM_1 \longrightarrow M_2/fM_2 \longrightarrow M_3/fM_3 \longrightarrow 0$$

Recall $M_{i,f}$ is the f-torsion of M_i. Note that taking f-torsion, i. e. the functor $M \mapsto M_f$, is left-exact, while the functor $M \mapsto M/fM \cong A/(f) \otimes_A M$, which is taking tensor product, is right-exact. The connecting map δ relates both functors.

(From me.) A proof why taking f-torsion is left-exact.

We first have to check that if $g\colon M_1 \to M_2$ is an A-linear map, then this map induces an A-linear map $M_{1,f} \to M_{2,f}$ (simply by restricting g). If $x \in M_1$ is f-torsion, then $fg(x) = g(fx) = g(0) = 0$, so $g(x) \in M_2$ is f-torsion as well.

Let $0 \to M_1 \to M_2 \to M_3$ be a exact sequence of A-modules. We want to show that $0 \to M_{1,f} \to M_{2,f} \to M_{3,f}$ is exact. Exactness in $M_{1,f}$ is clear since $M_1 \to M_2$ is injective, and so is its restriction $M_{1,f} \to M_{2,f}$.

For exactness in $M_{2,f}$, let $x \in \operatorname{im}(M_{1,f} \to M_{2,f})$. As $\operatorname{im}(M_{1,f} \to M_{2,f}) \subseteq \operatorname{im}(M_1 \to M_2)$, by exactness in M_2, we have $x \mapsto 0 \in M_3$. Hence $x \in \ker(M_{2,f} \to M_{3,f})$.

Conversely, let $x \in \ker(M_{2,f} \to M_{3,f})$. Since $\ker(M_{2,f} \to M_{3,f}) \subseteq \ker(M_2 \to M_3)$, by exactness in M_2, we have $x \in \operatorname{im}(M_1 \to M_2)$. So there is a preimage $y \in M_1$ of x. Then $fy \mapsto fx = 0$. As $M_1 \to M_2$ is injective, we must have $fy = 0$, so $y \in M_{1,f}$, hence $x \in \operatorname{im}(M_{1,f} \to M_{2,f})$.

4.16 Application of the Snake Lemma

Observation 4.87. More generally, assume we are given an A-module M and an exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ of A-modules. We want to understand when $M \otimes_A (0 \to M_1 \to M_2 \to M_3 \to 0)$ is exact, i. e. when M is flat. The snake lemma 4.83 gives an answer.

(i) Pick any presentation of M:

$$A^{\oplus J} \xrightarrow{X} A^{\oplus I} \longrightarrow M \longrightarrow 0$$

(ii) $A^{\oplus J}$ and $A^{\oplus I}$ are flat, so we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1^{\oplus J} & \longrightarrow & M_2^{\oplus J} & \longrightarrow & M_3^{\oplus J} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle X_1} & & \downarrow{\scriptstyle X_2} & & \downarrow{\scriptstyle X_3} & & \\ 0 & \longrightarrow & M_1^{\oplus I} & \longrightarrow & M_2^{\oplus I} & \longrightarrow & M_3^{\oplus I} & \longrightarrow & 0 \end{array}$$

Here, X_i is induced by the natural map $\mathrm{id}_{M_i} \otimes X$.

(iii) By the snake lemma 4.83, the sequence

$$0 \longrightarrow \ker(X_1) \longrightarrow \ker(X_2) \longrightarrow \ker(X_3) \xrightarrow{\delta} M \otimes_A M_1 \longrightarrow M \otimes_A M_2 \longrightarrow M \otimes_A M_3 \longrightarrow 0$$

is exact.

In conclusion, $M \otimes_A (0 \to M_1 \to M_2 \to M_3 \to 0)$ is exact if and only if $\ker(X_2) \to \ker(X_3)$ is surjective.

($M \otimes_A M_1 \to M \otimes_A M_2$ is injective if and only if $\operatorname{im}(\delta) = 0$ by exactness in $M \otimes_A M_1$. This is equivalent to $\ker(\delta) = \ker(X_3)$, which is again equivalent to $\ker(X_2) \to \ker(X_3)$ being surjective by exactness in $\ker(X_3)$.)

Corollary 4.88. *Let A be a ring and $f \in A$. Assume that $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of A-modules, where M_3 is f-torsion-free, i. e. $M_{3,f} = 0$. Then*

$$A/(f) \otimes_A (0 \to M_1 \to M_2 \to M_3 \to 0)$$

is again exact.

Proof. This follows directly from Example 4.86.

Alternatively, consider the presentation

$$A \xrightarrow{\cdot f} A \longrightarrow A/(f) \longrightarrow 0$$

and apply Observation 4.87: The assumption $M_{3,f} = 0$ ensures that $\ker(X_3) = 0$. □

Corollary 4.89. *Let A be a ring and $\mathfrak{a} \coloneqq (f, g) \subseteq A$ an ideal, generated by two elements $f, g \in A$. Assume that*

$$A \xrightarrow{\binom{-g}{f}} A^{\oplus 2} \xrightarrow{(f\ g)} \mathfrak{a} \longrightarrow 0$$

is exact. For example, if B is any ring, then this holds for $(X, Y) \subseteq B[X, Y]$ or $(f, T) \subseteq B[T]$ with regular $f \in B$.

Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of A-modules. If $M_{3,f} \cap M_{3,g} = 0$, then

$$\mathfrak{a} \otimes_A (0 \to M_1 \to M_2 \to M_3 \to 0)$$

is again exact.

Proof. Consider $\binom{-g}{f} \colon M_3 \to M_3^{\oplus 2}$. We have $\ker(\binom{-g}{f}) = M_{3,f} \cap M_{3,-g} = 0$, so the statement follows from Observation 4.87: The assumption $M_{3,f} \cap M_{3,g} = 0$ ensures that $\ker(X_3) = 0$. □

5 Integral Dependence

Lect. 13
25.05.23

The notion of *integral ring extensions* is important for algebraic geometry and algebraic number theory, which we will study later.

We refer to [AtMac, ch. 5].

5.1 Some Terminology on Rings

Definition 5.1. Let $\phi \colon A \to B$ be an A-algebra.

(i) B is of **finite type** or **finitely generated** if $B \cong A[T_1, \dots, T_n]/\mathfrak{a}$ as A-algebras for some $n \geq 0$ and some ideal $\mathfrak{a} \subseteq A[T_1, \dots, T_n]$.

(ii) B is of **finite presentation** or **finitely presented** if $B \cong A[T_1, \dots, T_n]/(f_1, \dots, f_m)$ as A-algebras for some $n, m \geq 0$ and $f_1, \dots, f_m \in A[T_1, \dots, T_n]$.

(iii) B is **finite** over A if B is finitely generated as an A-module (which is the same as saying that B is a finite A-module).

(iv) $x \in B$ is **integral** over A if there exists a monic $f \in A[T]$ such that $f(x) = 0$ (meant as $\phi(f)(x) = 0$).

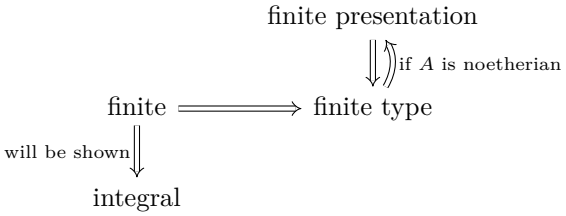
(v) B is **integral** over A if every element in B is integral over A.

Remark 5.2. (From me.) The terms *finite type* and *finite presentation* for A-algebras are very similar to A-modules. One could think that we could describe these terms as exact sequences in the category of rings, but as it turns out, cokernels of ring maps are very difficult to describe. The reason is that the category of rings is, in contrast to the category of A-modules, *not* a so-called *abelian category*.

At least for *finite type*, saying that $B \cong A[T_1, \dots, T_n]/\mathfrak{a}$ is the same as saying that a surjective A-algebra map $\psi \colon A[T_1, \dots, T_n] \twoheadrightarrow B$ exists. If the isomorphism holds, we can recover ψ by the projection

$A[T_1, \dots, T_n] \twoheadrightarrow A[T_1 \dots, T_n]/\mathfrak{a} \cong B$. Conversely, if ψ is given, we obtain the isomorphism by the homomorphism theorem; in this case, we have $\mathfrak{a} = \ker(\psi)$.

Remark 5.3. We have the following picture:



Some comments:

- Finite presentation implies finite type by choosing $\mathfrak{a} = (f_1, \dots, f_m)$.
- If A is noetherian, then by Hilbert's basis theorem 3.30, $A[T_1, \dots, T_n]$ is noetherian as well. So we may write $\mathfrak{a} = (f_1, \dots, f_m)$, and finite type implies finite presentation.
- Suppose that $B = (b_1, \dots, b_n)$ as an A-module. By the universal property of polynomial rings, we can construct an A-algebra map $A[T_1, \dots, T_n] \to B$, $T_i \mapsto b_i$. This map is surjective, as every element in B is the evaluation of a linear polynomial in $A[T_1, \dots, T_n]$. Hence finite implies finite type.

Example 5.4.

(i) Finite field extensions are finite (every finite field extension l/k is of the form $l = k(a_1, \dots, a_n)$).

(ii) Algebraic field extensions are integral by definition.

(iii) Quotients $A \twoheadrightarrow A/\mathfrak{a}$ are finite, as $A/\mathfrak{a}$ is generated by $\bar{1}$.

$A/\mathfrak{a}$ is finitely presented if and only if $\mathfrak{a}$ is finitely generated (exercise).

(iv) If $f \in A[T]$ is monic, then $B \coloneqq A[T]/(f) \cong A^{\oplus \deg(f)}$ as an A-module, namely with basis $\{T^i + (f) \mid 0 \le i < \deg(f)\}$. In particular, B is a finite A-algebra.

This is not necessarily true if f is not monic, e. g. $A[T]/(aT - 1) \cong A[a^{-1}]$ is often not finite. For example, $\mathbb{Z}[\frac{1}{2}]$ is not a finite $\mathbb{Z}$-algebra (2^{-1} cannot be written as a linear combination of numbers 2^{-k} with $k < n$).

(v) For all $n \in \mathbb{Z}$, $\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ for $n \in \mathbb{Z}$ satisfies $(\sqrt{n})^2 - n$, and hence is is integral over $\mathbb{Z}$.

Exercise 5.5. Show that $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$. The same holds for any principal ideal domain A and $B = \mathrm{Quot}(A)$.

Solution. This is a direct consequence of the *rational root theorem* [Sch, Exercise 1.5.2 (i)]. The theorem states: Suppose that $\frac{p}{q} \in B$ is a root of $f = \sum_{i=0}^{n} a_i T^i \in A[T]$. We may assume that $\gcd(p, q) = 1$ after reduction. Then $p \mid a_0$ and $q \mid a_n$.

In our case, if $x = \frac{p}{q} \in B$ with $\gcd(p, q) = 1$ is integral over A, then there exists a monic $f \in A[T]$ such that $f(x) = 0$. This means $q \mid 1$, hence $q \in A^\times$ and $x = p \in A$.

5.2 Finite and Integral Extensions

Ring extensions are useful to reduce problems to easier problems, e. g. solving a system of polynomial equations.

Remark 5.6. Henceforth, we will consider $A \subseteq B$ to be a subring of B, or $B \supseteq A$ a ring extension of A. To apply this in general, given an A-algebra $\phi\colon A \to B$, replace A by the subring $\phi(A) \subseteq B$.

Proposition 5.7. *Let $A \subseteq B$ be rings. For all $x \in B$, the following are equivalent:*

(i) *x is integral over A.*

(ii) *The A-subalgebra $A[x] \subseteq B$ generated by x is finite.*

(iii) *There exists an A-subalgebra $C \subseteq B$ that is finite and contains x.*

Proof.

- (i) $\implies$ (ii): $x \in B$ is integral, say $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. This implies $x^n = -a_{n-1}x^{n-1} - \cdots - a_0$, and by induction, higher powers x^r with $r \geq n$ are in the A-module $(1, x, x^2, \ldots, x^{n-1})$. Thus $A[x]$ is generated by $1, x, x^2, \ldots, x^{n-1}$ as an A-module.
- (ii) $\implies$ (iii): Take $C = A[x]$.
- (iii) $\implies$ (i): Let $c_1, \ldots, c_n \in C$ be the generators of C as an A-module. For each $j = 1, \ldots, n$, we can write $xc_j = \sum_{i=1}^n a_{ij}c_i$ (the a_{ij} might not be uniquely determined). In other words, we have chosen a commutative diagram

$$\begin{array}{ccc} A^{\oplus n} & \xrightarrow{p} & C \\ {\scriptstyle \tilde{x}}\downarrow & & \downarrow{\scriptstyle x} \\ A^{\oplus n} & \xrightarrow{p} & C \end{array}$$

with $p(e_i) = c_i$ and $\tilde{x} = (a_{ij}) \in M_{n\times n}(A)$. Note that we view $x\colon C \to C$ as an A-linear map by left-multiplication. We have $\operatorname{char}_{\tilde{x}}(\tilde{x}) = 0$ by Cayley-Hamilton 8.19. If we set $f(T) \coloneqq \operatorname{char}_{\tilde{x}}(T) \in A[T]$, then f is a monic polynomial such that $f(x) = 0$. (As $f(\tilde{x})$ is the zero map and p is surjective, $f(x)$ must be the zero map as well. In particular, $f(x)\cdot 1 = 0$ in the module C, implying $f(x) = 0$ in the ring B.) □

Corollary 5.8. *Let $A \subseteq B$ be rings.*

(i) *If B is finite over A, then B is integral over A.*

(ii) *If $x_1, \ldots, x_n \in B$ are integral over A, then $A[x_1, \ldots, x_n]$ is finite over A.*

(iii) *Let $\overline{A}^B \subseteq B$ be the set of all integral elements in B over A. Then $\overline{A}^B$ is a subring of B containing A, called the **integral closure** of A in B.*

Proof.

(i) Take $C = B$ in Proposition 5.7, (iii) $\implies$ (i).

(ii) We perform induction on n. The case $n = 1$ is covered by Proposition 5.7.

Assume that $A[x_1, \ldots, x_{n-1}]$ is finite over A. Now x_n is integral over A, hence it is also integral over $A[x_1, \ldots, x_{n-1}]$. By Proposition 5.7, $A[x_1, \ldots, x_n]$ is finite over $A[x_1, \ldots, x_{n-1}]$, hence by assumption, it is finite over A. (The 'composition' of finite algebras is finite: Suppose that $A \subseteq B \subseteq C$ are rings where $B^{\oplus n} \twoheadrightarrow C$ as B-modules and $A^{\oplus m} \twoheadrightarrow B$ as A-modules. Then $A^{\oplus nm} \twoheadrightarrow C$ as A-modules.)

(iii) Apparently $A \subseteq \overline{A}^B$, and in particular $0, 1 \in \overline{A}^B$.

For any $x, y \in \overline{A}^B$, $A[x, y]$ is finite by (ii). By (i), $A[x, y]$ is integral over A. As $x \pm y, xy \in A[x, y]$, we conclude that $x \pm y$ and xy are integral over A, hence $x \pm y, xy \in \overline{A}^B$. □

Corollary 5.9. *Assume that $A \subseteq B \subseteq C$ are rings such that B is integral over A and C is integral over B. Then C is integral over A. In particular, $\overline{\overline{A}^B}^B = \overline{A}^B$.*

Proof. Let $x \in C$. As C is integral over B, we have $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ for certain $b_i \in B$. Then $A[b_0, \ldots, b_{n-1}, x]$ is finite over $A[b_0, \ldots, b_{n-1}]$ by Proposition 5.7. Moreover by Corollary 5.8, $A[b_0, \ldots, b_{n-1}]$ is finite over A since B is integral over A. Similar to the proof of Corollary 5.8 (ii), we conclude that $A[b_0, \ldots, b_{n-1}, x]$ is finite over A. Again by Proposition 5.7, since $x \in A[b_0, \ldots, b_{n-1}, x]$, we know that x is integral over A.

For the statement about integral closures, consider $A \subseteq \overline{A}^B \subseteq \overline{\overline{A}^B}^B$, which are all subrings of B. □

Proposition 5.10. *Let $A \subseteq B$ be an integral ring extension, i. e. B is integral over A. Then the following hold:*

(i) *If $\mathfrak{b} \subseteq B$ is an ideal, then $A/\mathfrak{b} \cap A \subseteq B/\mathfrak{b}$ is integral.*

(ii) *If $S \subseteq A$ is a multiplicative subset, then $S^{-1}A \subseteq S^{-1}B$ is integral.*

(iii) *If $A \to C$ is any A-algebra, then $C \to C \otimes_A B$ is integral (but not necessarily injective).*

Proof.

(i) Let $\bar{x} \in B/\mathfrak{b}$. Since $x \in B$ is integral over A, we can write $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. If we consider this relation modulo $\mathfrak{b}$, we obtain $\bar{x}^n + \bar{a}_{n-1}\bar{x}^{n-1} + \cdots + \bar{a}_0 = 0$ with $\bar{a}_i \in A/\mathfrak{b} \cap A$.

(ii) Let $\frac{b}{s} \in S^{-1}B$. Since $b \in B$ is integral over A, we can write $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. If we divide this relation by s^n, we obtain $(\frac{b}{s})^n + (a_{n-1}/s)(\frac{b}{s})^{n-1} + \cdots + (a_0/s^n) = 0$ with coefficients in $S^{-1}A$.

(iii) Let $c \otimes b \in C \otimes_A B$. Since $b \in B$ is integral over A, we can write $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. This implies

$$(c \otimes b)^n + c \otimes a_{n-1}(c \otimes b)^{n-1} + \cdots + c^n \otimes a_0 = c^n \otimes (b^n + a_{n-1}b^{n-1} + \cdots + a_0) = 0$$

with coefficients in $C \otimes_A A \cong C$. This shows that elementary are integral over C. By Corollary 5.8 on integral closures, integral elements are stable under addition and multiplication. Elementary tensors generate $C \otimes_A B$ as a C-algebra, hence $C \otimes_A B$ is integral over $C \otimes_A A \cong C$. □

5.3 The Going-Up Theorem

Problem 5.11. Let $A \subseteq B$ be an integral ring extension. We want to understand the map

$$\operatorname{Spec}(B) \to \operatorname{Spec}(A), \qquad \mathfrak{q} \mapsto \mathfrak{q} \cap A.$$

Proposition 5.12. *Let $A \subseteq B$ be an integral ring extension of integral domains. Then A is a field if and only if B is a field.*

Proof. Suppose that A is a field, and let $0 \neq y \in B$. By integrality of B, there exists a relation $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$ of y. Since B is an integral domain, we may assume that $a_0 \neq 0$ (otherwise, we may divide our relation by some non-zero power of y such that it is of the desired form). A is a field, so $a_0 \in A^\times$. Rearranging the relation yields $-a_0^{-1}(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1)y = 1$, hence $y \in B^\times$ and B is a field.

Conversely, suppose B is a field, and let $0 \neq x \in A$. Since $x \in B$, we also have $x^{-1} \in B$, which is integral over A. Thus we have a relation $x^{-n} + a_{n-1}x^{-n+1} + \cdots + a_1x^{-1} + a_0 = 0$. Multiplying by x^{n-1} and rearranging yields $x^{-1} = -(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1}) \in A$. Hence $x \in A^\times$ and A is a field. □

Corollary 5.13. *Let $A \subseteq B$ be an integral ring extension and $\mathfrak{q} \subseteq B$ a prime ideal. Then $\mathfrak{q}$ is maximal in B if and only if $\mathfrak{q} \cap A$ is maximal in A.*

Proof. We apply Proposition 5.12 to the integral domains $A/\mathfrak{q} \cap A \subseteq B/\mathfrak{q}$, where this ring extension is integral by Proposition 5.10. □

Corollary 5.14. *Let $A \subseteq B$ be an integral ring extension. Assume that $\mathfrak{q}, \mathfrak{q}' \subseteq B$ are prime ideals with $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ in A. Then $\mathfrak{q} = \mathfrak{q}'$ in B.*

Before we prove this statement, recall the following:

(i) Localisations of A-modules preserve inclusions and finite intersections (the later is Corollary 4.55).

(ii) If $S \subseteq A$ is a multiplicative subset of a ring A, and if $\phi\colon A \to S^{-1}A$ is the universal localisation map, then by Proposition 2.55, there exists a bijection

$$\operatorname{Spec}(S^{-1}A) \cong \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \varnothing\}, \qquad \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}), \qquad \mathfrak{p}S^{-1}A \hookleftarrow \mathfrak{p}.$$

Proof. Henceforth $\mathfrak{p} \coloneqq \mathfrak{q} \cap A \in \operatorname{Spec}(A)$. We localise in $\mathfrak{p}$, i. e. we localise A and B in $S = (A \setminus \mathfrak{p})$. By Proposition 5.10, $A_\mathfrak{p} \subseteq B_\mathfrak{p} \coloneqq S^{-1}B$ is an integral extension. Note that $\mathfrak{q}' \cap S = \varnothing$, so $\mathfrak{q}B_\mathfrak{p} \subseteq \mathfrak{q}'B_\mathfrak{p}$ are two prime ideals in $B_\mathfrak{p}$ according to Proposition 2.55. Since S^{-1} commutes with intersections of A-modules (Corollary 4.55), and since we can interpret $\mathfrak{q}, \mathfrak{q}'$ as A-modules, we obtain

$$\mathfrak{p}A_\mathfrak{p} = S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q} \cap S^{-1}A = \mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p} = \cdots = \mathfrak{q}'B_\mathfrak{p} \cap A_\mathfrak{p}.$$

But we know that $A_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$. Therefore, by Corollary 5.13, $\mathfrak{q}B_\mathfrak{p}$ and $\mathfrak{q}'B_\mathfrak{p}$ are maximal. Both must be equal because of $\mathfrak{q}B_\mathfrak{p} \subseteq \mathfrak{q}'B_\mathfrak{p}$ and maximality of $\mathfrak{q}B_\mathfrak{p}$. If $\phi\colon B \to B_\mathfrak{p}$ is the universal localisation map, then by Lemma 2.52, $\mathfrak{q} = \phi^{-1}(\mathfrak{q}B_\mathfrak{p}) = \phi^{-1}(\mathfrak{q}'B_\mathfrak{p}) = \mathfrak{q}'$. □

Corollary 5.15. *Let $A \subseteq B$ be an integral extension. Then the map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. By Proposition 5.10, $A_\mathfrak{p} \subseteq B_\mathfrak{p}$ is integral. This implies that $B_\mathfrak{p} \neq 0$, and there exists a maximal ideal $\mathfrak{q}B_\mathfrak{p}$ with $\mathfrak{q} \in \operatorname{Spec}(B)$ by Krull's theorem 2.18. According to Corollary 5.13, $\mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p}$ must be maximal in $A_\mathfrak{p}$. But $A_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$, so $\mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. By Lemma 2.52, we pull the prime ideals back in order to obtain $\mathfrak{q} \cap A = \mathfrak{p}$. Thus the map of spectra maps $\mathfrak{q} \mapsto \mathfrak{p}$. □

Theorem 5.16 (going-up theorem). *Let $A \subseteq B$ be an integral extension. Suppose we are given a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ of prime ideals in B and a longer chain $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ of prime ideals in A such that $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ for all $i \leq m$.*

$$\begin{array}{ccccccccccc} \mathfrak{q}_1 & \subseteq & \cdots & \subseteq & \mathfrak{q}_m & & & & & & \\ \cup\mathrel{|} & & & & \cup\mathrel{|} & & & & & & \\ \mathfrak{p}_1 & \subseteq & \cdots & \subseteq & \mathfrak{p}_m & \subseteq & \mathfrak{p}_{m+1} & \subseteq & \cdots & \subseteq & \mathfrak{p}_n \end{array}$$

Then there exists a continuation $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ of prime ideals in B such that $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ for every $i > m$ too.

Proof. We pass to $A/\mathfrak{p}_m \subseteq B/\mathfrak{q}_m$, which is integral due to Proposition 5.10. By Corollary 5.15, there is some prime ideal $\mathfrak{q}_{m+1}/\mathfrak{q}_m \subseteq B/\mathfrak{q}_m$ such that $\mathfrak{q}_{m+1}/\mathfrak{q}_m \cap A/\mathfrak{p}_m = \mathfrak{p}_{m+1}/\mathfrak{p}_m$. Lifting back to B, i. e. taking the preimage under $B \twoheadrightarrow B/\mathfrak{q}_m$, gives $\mathfrak{p}_{m+1} = \mathfrak{q}_{m+1} \cap A$ with prime ideal $\mathfrak{q}_{m+1} \subseteq B$. Now we continue inductively. □

Corollary 5.17. *Let $A \subseteq B$ be an integral extension. Then $\dim(A) = \dim(B)$ for the Krull dimension.*

Proof. For $\dim(A) \geq \dim(B)$, let $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_n$ be any chain of prime ideals in B. Then $\mathfrak{q}_0 \cap A \subseteq \cdots \subseteq \mathfrak{q}_n \cap A$ is a chain of prime ideals in A. By Corollary 5.14, this chain must be proper.

For $\dim(A) \leq \dim(B)$, let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be any chain of prime ideals in A. By Corollary 5.15, we can find some prime ideal $\mathfrak{q}_0 \subseteq B$ such that $\mathfrak{p}_0 = \mathfrak{q}_0 \cap A$. By the going-up theorem 5.16, we can construct a chain $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_n$ of prime ideals in B such that $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. Corollary 5.14 implies that this chain must be proper. □

Example 5.18. Consider the ring extension $\mathbb{C}[x] \subseteq \mathbb{C}[y]$ with $x = y^n$ for some $n \in \mathbb{Z}_{>0}$. Since $\mathbb{C}[y] \cong \mathbb{C}[x][T]/(T^n - x)$ via $y \leftrightarrow T$, $\mathbb{C}[y]$ is certainly finite over $\mathbb{C}[x]$, and hence $\mathbb{C}[x] \subseteq \mathbb{C}[y]$ is integral.

This inclusion induces the spectral map

$$\phi\colon \operatorname{Spec}(\mathbb{C}[y]) \to \operatorname{Spec}(\mathbb{C}[x]), \qquad (0) \mapsto (0), \qquad (y-a) \mapsto (y-a)\mathbb{C}[y] \cap \mathbb{C}[x] = (x - a^n).$$

The equality holds since we know that $(y-a) \cap \mathbb{C}[x]$ must be a principal ideal with irreducible generator, i. e. of the form $(x-t)$ for $t \in \mathbb{C}$. Recall the famous factorisation $(y-a)(y^{n-1} + y^{n-2}a + \cdots + a^{n-1}) = y^n - a^n = x - a^n$, so $t = a^n$.

The spectral map ϕ is the algebraic incarnation of the finite map of Riemann surfaces $\mathbb{C} \to \mathbb{C}$, $a \mapsto a^n$ in the context of complex analysis. Riemann surfaces are used to study *ramification* of certain inverse maps, e. g. the branches of the nth root. E. g. for $n = 2$, we have Figure 5.1. The fact that any non-zero complex number has exactly n different complex nth roots corresponds to the fact that the fibres of non-zero prime ideals under ϕ have exactly n elements.

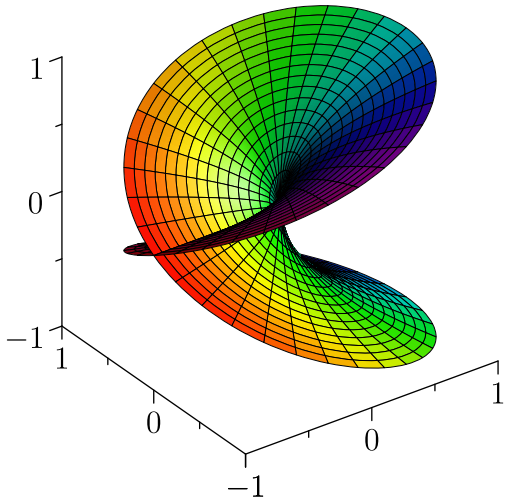


Figure 5.1: Ramification of the square root. Right and left horizontal axes depict $\mathrm{Re}(a)$ and $\mathrm{Im}(a)$, and the vertical axis the real part of $\sqrt{a}$, whereas the colour encodes the imaginary part. Note that only 0 has exactly one point on the surface above it, whereas every other complex number has exactly two points above it. (Proudly done in Asymptote.)

Example 5.19. Consider the ring extension $\mathbb{C}[x_1, x_2] \subseteq \mathbb{C}[y_1, y_2]$ with $x_i = y_i^2$ for $i = 1, 2$. Figure 5.2 shows all possible ways of going up the chain $(0) \subseteq (x_1 - x_2) \subseteq (x_1 - a, x_2 - a) \subseteq \mathbb{C}[x_1, x_2]$ of prime ideals with $0 \neq a \in \mathbb{C}$.

Recall that in Example 2.59, we gave a full description of all prime ideals in two variables over $\mathbb{C}$. We can thus check that these are indeed chains of prime ideals, since $y_1 \pm y_2$ is irreducible and the right-most ideals are indeed of the form $(y_1 - t_1, y_2 - t_2)$ for $t_1, t_2 \in \mathbb{C}$. These are indeed all possible ways since $x_1 - x_2 = (y_1 - y_2)(y_1 + y_2)$ and $x_i - a = (y_i - \sqrt{a})(y_i + \sqrt{a})$.

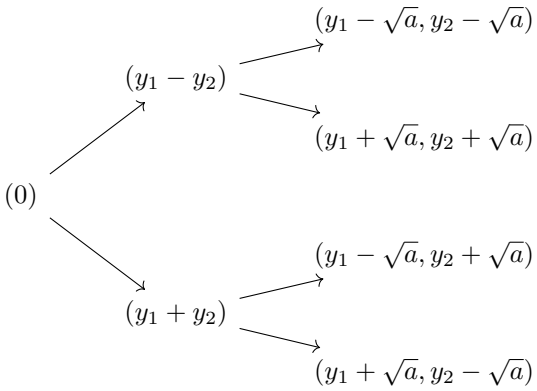


Figure 5.2: Visualisation of Example 5.19.

5.4 Understanding Polynomial Equations and Pythagorean Triples

Lect. 14
05.06.23

After doing this much theory, we will consider a few concrete motivations on why we are even doing it.

Problem 5.20. Let R be a ring (classically $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{C}$) and $f_1, \dots, f_m \in R[T_1, \dots, T_n]$ with $n, m \geq 0$. Let $\phi\colon R \to B$ be an R-algebra. Then we can apply ϕ to all f_i, and we pass to $\phi(f_i) \in B[T_1, \dots, T_n]$.

The **solution set** is

$$X(B) \coloneqq \{(x_1, \dots, x_n) \in B^n \mid \phi(f_1)(x) = \cdots = \phi(f_m)(x) = 0\}$$

(one often writes $f_1(x) = \cdots = f_m(x) = 0$ and drops ϕ), i. e. the set of all points that satisfy the given algebraic relations.

The most basic question is whether $X(B) \neq \varnothing$. If the answer is yes, then what structure does it carry?

As an example, we will characterise *Pythagorean triples*.

Definition 5.21. A **Pythagorean triple** is a triple $(a, b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ such that $a^2 + b^2 = c^2$. We call such a triple **primitive** if $\gcd(a, b, c) = 1$ and $c > 0$.

Remark 5.22. We observe that if (a, b, c) is a Pythagorean triple, then (ka, kb, kc) is a Pythagorean triple as well for all $0 \neq k \in \mathbb{Z}$, since the defining relation is homogeneous. Thus every Pythagorean triple is a multiple of some primitive triple, and it suffices to consider the latter.

Lemma 5.23. *There exists a bijection between primitive Pythagorean triples (a, b, c) and rational points on the unit circle $X(\mathbb{Q}) \coloneqq \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\}$ via $(a, b, c) \mapsto (\frac{a}{c}, \frac{b}{c})$.*

Proof. Indeed, the map $(a, b, c) \mapsto (\frac{a}{c}, \frac{b}{c})$ maps into $X(\mathbb{Q})$.

We can construct the inverse map as follows: Given $(x, y) \in X(\mathbb{Q})$, we can completely reduce the fractions x and y, and then convert them to fractions to a common denominator $c > 0$ being the least common multiple of the fractions. This gives $x = \frac{a}{c}$ and $y = \frac{b}{c}$ with $\gcd(a, b, c) = 1$ and $c > 0$. The inverse map is $(x, y) \mapsto (a, b, c)$, where (a, b, c) is indeed a primitive Pythagorean triple. □

Proposition 5.24. *Let $P \coloneqq (-1, 0) \in X(\mathbb{Q})$. There is a bijection*

$$\mathbb{Q} \to X(\mathbb{Q}) \setminus \{P\}, \qquad q \mapsto \left(\frac{1 - q^2}{1 + q^2}, \frac{2q}{1 + q^2}\right), \qquad \frac{y}{x + 1} \mathrel{\reflectbox{$\mapsto$}} (x, y).$$

Note that $1 + q^2 > 0$ for all $q \in \mathbb{Q}$ and $x + 1 \neq 0$ for all $(x, y) \in X(\mathbb{Q}) \setminus \{P\}$.

Proof. We do the following geometric construction (see Figure 5.3): For each $q \in \mathbb{Q}$, let L_q be the line of slope q through P. Note that L_q is completely determined by the second point $(0, q) \in L_q$. We claim that it intersects $X(\mathbb{Q}) \setminus \{P\}$ in a unique point.

L_q is given by the linear equation $y = qx + q$, so we need to solve the following system of equations:

$$\begin{cases} qx + q = y, \\ x^2 + y^2 = 1. \end{cases}$$

We substitute for y in the second equation and obtain the polynomial relation

$$x^2 + (qx + q)^2 - 1 = (1 + q^2)x^2 + 2q^2x + q^2 - 1 = 0.$$

We already know by construction that $x = -1$ is a *rational* root of the quadratic polynomial since $P \in L_q \cap X(\mathbb{Q})$. Recall that any monic quadratic polynomial having at least one root splits into $(x-\alpha)(x-\beta) = x^2-(\alpha+\beta)x+\alpha\beta$. We see that if α is a *rational* root, then β is automatically a *rational* root as well (this is actually a much deeper fact), so the second root is in $X(\mathbb{Q})$. More concretely, we obtain

$$x = \frac{1 - q^2}{1 + q^2}$$

(this follows from $\alpha = -1$ and $\alpha\beta = (q^2 - 1)/(1 + q^2)$). The y-coordinate is thus

$$y = q\frac{1 - q^2}{1 + q^2} + q = \frac{q - q^3 + q + q^3}{1 + q^2} = \frac{2q}{1 + q^2}.$$

So the claimed map exists.

For the inverse map, the line through a given $(x, y) \in X(\mathbb{Q}) \setminus \{P\}$ and P has slope

$$q = \frac{y}{x + 1}.$$

The two maps are geometrically inverses of each other. Alternatively, one can purely algebraically compute that they are indeed inverses. □

Back to Pythagorean triples.

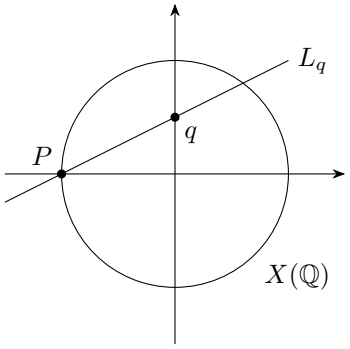


Figure 5.3: Construction in Proposition 5.24.

Theorem 5.25. *All primitive Pythagorean triples are exactly*

$$\begin{cases} (v^2-u^2, 2uv, v^2+u^2), & \text{if } u \text{ or } v \text{ is even,} \\ \left(\dfrac{v^2-u^2}{2}, uv, \dfrac{v^2+u^2}{2}\right), & \text{if } u \text{ and } v \text{ are odd,} \end{cases}$$

with $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{\geq 0}$ *and* $\gcd(u,v) = 1$.

Proof. Due to Lemma 5.23 and Proposition 5.24, we can find a bijection between $\mathbb{Q}$ and primitive Pythagorean triples except the one corresponding to P: Given $q = \frac{u}{v} \in \mathbb{Q}$ with $v > 0$ and $\gcd(u,v) = 1$, we have

$$q \mapsto \left(\frac{1-q^2}{1+q^2}, \frac{2q}{1+q^2}\right) = \left(\frac{v^2-u^2}{v^2+u^2}, \frac{2uv}{v^2+u^2}\right) \mapsto \begin{cases} (v^2-u^2, 2uv, v^2+u^2), & \text{if } u \text{ or } v \text{ is even,} \\ \left(\dfrac{v^2-u^2}{2}, uv, \dfrac{v^2+u^2}{2}\right), & \text{if } u \text{ and } v \text{ are odd.} \end{cases}$$

Notice that they are indeed primitive Pythagorean triples: Suppose that u and v are odd. If $(v^2+u^2)/2$ and $(v^2-u^2)/2$ share a common factor, then their sum v^2 and difference u^2 also shares the same factor, contradicting $\gcd(u,v) = 1$. Hence they are always coprime. The same spiel applies to the case when either u or v is even (remember $\gcd(u,v) = 1$). Then a common factor of v^2-u^2 and v^2+u^2 cannot be 2, and their sum and difference are $2v^2$ and $2u^2$, resp.

Similarly, any divisor of u or v cannot divide $v^2 \pm u^2$, as otherwise we contradict $\gcd(u,v) = 1$, so uv and $v^2 \pm u^2$ are coprime. In the case that either u or v is even, we do not have to consider the factor 2 of $2uv$ as $2 \nmid v^2 \pm u^2$. In the case that u and v are odd, $\gcd(uv, v^2 \pm u^2) = 1$, thus especially $\gcd(uv, (v^2 \pm u^2)/2) = 1$.

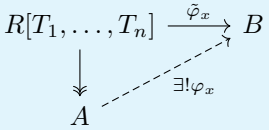
The only missing primitive Pythagorean triple is the one corresponding to $P = (-1, 0)$, namely $(-1, 0, 1)$. This can be brought in the desired form by $(u,v) = (1,0)$, formally the fraction $q = \frac{1}{0}$ at infinity. □

But how does this relate to our problem?

Observation 5.26. Consider polynomials $f_1, \dots, f_m \in R[T_1, \dots, T_n]$ and an R-algebra $R \to B$ again. Set $A \coloneqq R[T_1, \dots, T_n]/(f_1, \dots, f_m)$. Then we have the bijection

$$\operatorname{Hom}_{R\text{-Alg}}(A, B) \cong X(B), \qquad \varphi \mapsto (\varphi(\bar{T}_1), \dots, \varphi(\bar{T}_n)), \qquad [\varphi\colon T_i \mapsto x_i] \mapsfrom (x_1, \dots, x_n). \tag{5.27}$$

Now a proof for this bijection: By the universal property of polynomial rings, any $x = (x_1, \dots, x_n) \in B^n$ gives a unique R-algebra map $\tilde{\varphi}_x\colon R[T_1, \dots, T_n] \to B$, $T_i \mapsto x_i$. Restricting to $x \in X(B)$, we have $\tilde{\varphi}_x(f_j(T_1, \dots, T_n)) = f_j(x_1, \dots, x_n) = 0$ for all $j = 1, \dots, m$ by assumption. Thus $(f_1, \dots, f_m) \subseteq \ker(\tilde{\varphi}_x)$, and by the universal property of quotient rings, we obtain a unique R-algebra map φ_x such that the following diagram commutes:



Conversely, let $\varphi \in \mathrm{Hom}_{R\text{-Alg}}(A,B)$, and set $x_\varphi := (\varphi(\bar{T}_1),\dots,\varphi(\bar{T}_n)) \in B^n$. Observe that x_φ is unique to each φ, as $\bar{T}_1,\dots,\bar{T}_n$ generate A as an R-algebra and thus determine φ uniquely. Now we have $0 = \varphi(f_j(\bar{T}_1,\dots,\bar{T}_n)) = f_j(x_\varphi)$ for all $j = 1,\dots,m$, hence $x_\varphi \in X(B)$.

The proof also shows us an interpretation of the bijection: Every $\varphi \in \mathrm{Hom}_{R\text{-Alg}}(A,B)$ is an evaluation of the polynomials $f_1,\dots,f_m$ that forces $f_j(\varphi(\bar{T}_1),\dots,\varphi(\bar{T}_n)) = 0$ for all $j = 1,\dots,m$, i. e. that evaluation is a solution. Therefore A embodies the system of polynomial equations

$$f_1(x_1,\dots,x_n) = \cdots = f_m(x_1,\dots,x_m) = 0.$$

Specialising to our context of Pythagorean triples again, in Proposition 5.24, we want to compute

$$\mathrm{Hom}_{\mathbb{Q}\text{-Alg}}\left(\mathbb{Q}\left[X,Y,\frac{1}{X+1}\right]/(X^2+Y^2-1),\mathbb{Q}\right).$$

The solutions must satisfy the equation for the unit circle $X^2 - Y^2 - 1 = 0$. The sole reason for $(X+1)^{-1}$ is to exclude the point P from the solution set, as for the image of $X+1$ in $\mathbb{Q}$ to be invertible, we must have $X \neq -1$.

The following improves Proposition 5.24.

Proposition 5.28. *Let $R := \mathbb{Z}[\frac{1}{2}]$. Then there is an isomorphism of R-algebras*

$$R\left[X,Y,\frac{1}{X+1}\right]/(X^2+Y^2-1) \cong R\left[q,\frac{1}{1+q^2}\right], \qquad X \mapsto \frac{1-q^2}{1+q^2}, \quad Y \mapsto \frac{2q}{1+q^2}, \qquad \frac{Y}{X+1} \mapsfrom q.$$

Proof. We are given the diagonal maps in the following diagram:

$$\begin{array}{ccc} R[X,Y] & & R[q] \\ \downarrow & \searrow\swarrow & \downarrow \\ R[X,Y,(X+1)^{-1}]/(X^2+Y^2-1) & \underset{\Phi}{\overset{\Psi}{\rightleftarrows}} & R[q,(1+q^2)^{-1}] \end{array}$$

Our goal is to construct R-algebra maps Φ and Ψ such that the whole diagram commutes.

We check (remember that $2 \in R^\times = \mathbb{Z}[\frac{1}{2}]^\times$)

$$X+1 \mapsto \frac{1-q^2}{1+q^2} + 1 = \frac{1-q^2+1+q^2}{1+q^2} = \frac{2}{1+q^2} \in R\left[q,\frac{1}{1+q^2}\right]^\times,$$

$$X^2+Y^2-1 \mapsto \left(\frac{1-q^2}{1+q^2}\right)^2 + \left(\frac{2q}{1+q^2}\right)^2 - 1 = \frac{1-2q^2+q^4+4q^2-(1+2q^2+q^4)}{(1+q^2)^2} = 0.$$

Hence by the universal property of localisations and by the universal property of quotient rings, we obtain Φ.

We further check, exploiting $X^2+Y^2=1$,

$$1+q^2 \mapsto 1 + \frac{Y^2}{(X+1)^2} = \frac{X^2+2X+1+Y^2}{(X+1)^2} = \frac{2(X+1)}{(X+1)^2} = \frac{2}{X+1} \in R\left[X,Y,\frac{1}{X+1}\right]/(X^2+Y^2-1)^\times.$$

Hence by the universal property of localisations, Ψ exists.

Lastly, one checks that Φ and Ψ are mutually inverses by purely algebraic manipulation, which is an identical calculation to the one in Proposition 5.24. □

Corollary 5.29. *Let B be a $\mathbb{Z}[\frac{1}{2}]$-algebra, i. e. B is a ring with $2 \in B^\times$. Then there is a bijection*

$$\{q \in B \mid 1+q^2 \in B^\times\} \cong \{(x,y) \in B^2 \mid x^2+y^2=1, x+1 \in B^\times\}, \quad q \mapsto \left(\frac{1-q^2}{1+q^2},\frac{2q}{1+q^2}\right), \quad \frac{y}{x+1} \mapsfrom (x,y).$$

Proof. This is literally just a reformulation of the bijection

$$\mathrm{Hom}_{\mathbb{Z}[\frac{1}{2}]\text{-Alg}}\left(\mathbb{Z}\left[\frac{1}{2},q,\frac{1}{1+q^2}\right],B\right) \cong \mathrm{Hom}_{\mathbb{Z}[\frac{1}{2}]\text{-Alg}}\left(\mathbb{Z}\left[\frac{1}{2},X,Y,\frac{1}{X+1}\right]/(X^2+Y^2-1),B\right).$$

Each map on the left hand side is completely determined by its image on q, and likewise each map on the right hand side by its image on X and Y. The bijection is thus a change of basis so to speak. □

We see that finitely presented R-algebras are (roughly speaking) systems of polynomial equations over R, but without an explicit choice of coordinates.

A somewhat related and (for its difficulty) famous problem, which we obviously will not prove:

Theorem 5.30 (**Fermat's last theorem**, Wiles 1994)**.** *For all $n \geq 3$, there are no $(x, y, z) \in \mathbb{Q}^3$ with $xyz \neq 0$ such that $x^n + y^n = z^n$.*

Remark 5.31.

(i) The condition $xyz \neq 0$ excludes the trivial solutions $x^n + 0^n = x^n$, $0^n + y^n = y^n$, $x^n + (-x)^n = 0^n$ for odd n, etc.

(ii) Fermat claimed this to be true in 1637, but without proof. It has motivated generations of mathematicians since then, see Wikipedia.

5.5 The Spectrum, Revisited

Problem 5.32. Let A be a ring. Why do we study $\operatorname{Spec}(A)$? The short answer: $\operatorname{Spec}(A)$ parameterises solutions of polynomial equations in *field extensions*.

Observation 5.33. Again, let R be a ring and $f_1, \dots, f_m \in R[T_1, \dots, T_n]$. Let $R \to B$ be an R-algebra and set $A \coloneqq R[T_1, \dots, T_n]/(f_1, \dots, f_m)$. Let Ω be a field.

Suppose that $R \to \Omega$ is an R-algebra. Given $x = (x_1, \dots, x_n) \in X(\Omega)$, consider the evaluation map $\varphi_x \colon A \to \Omega$. Since Ω is an integral domain, we know that $\ker(\varphi_x) \in \operatorname{Spec}(A)$ (for $\varphi_x(ab) = 0 \in \Omega$ implies $\varphi_x(a) = 0$ or $\varphi_x(b) = 0$). Thus we obtain a canonically induced embedding $\bar{\varphi}_x \colon \operatorname{Quot}(A/\ker(\varphi_x)) \hookrightarrow \Omega$, which is a field extension (notice that after passing to the quotient, $\ker(\bar{\varphi}_x) = 0$ holds).

Conversely, assume that $\mathfrak{p} \in \operatorname{Spec}(A)$ and $\varphi \colon \kappa(\mathfrak{p}) = \operatorname{Quot}(A/\mathfrak{p}) \hookrightarrow \Omega$ is field extension. Then Ω becomes an R-algebra via $R \to A \to \kappa(\mathfrak{p}) \to \Omega$ (the last map is φ), and φ, or, more precisely, the R-algebra map $A \to \kappa(\mathfrak{p}) \to \Omega$, defines a unique solution in $X(\Omega)$.

Example 5.34. Let k be a field. Then we have the following injection of sets:

$$k^n \hookrightarrow \operatorname{Spec}(k[X_1, \dots, X_n]), \qquad x = (x_1, \dots, x_n) \mapsto \mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n).$$

In other words, if $\varphi_x \colon k[X_1, \dots, X_n] \to k$, $X_i \mapsto x_i$ is the evaluation map w. r. t. x, then $\ker(\varphi_x) = \mathfrak{m}_x$. (For an argument for the injection, see the proof of Corollary 6.9. To show $\ker(\varphi_x) = \mathfrak{m}_x$, note that $\mathfrak{m}_x \subseteq \ker(\varphi_x)$ already. Furthermore, $k[X_1, \dots, X_n]/\mathfrak{m}_x \hookrightarrow k$ is a field map and thus injective (in fact, this is an isomorphism). Thus $\mathfrak{m}_x = \ker(\varphi_x)$.)

Remark 5.35. What map does this injection induce on $\operatorname{Spec}(k[X_1, \dots, X_n, f^{-1}])$ for some $f \in k[X_1, \dots, X_n]$? Recall from Proposition 2.55 that

$$\operatorname{Spec}(k[X_1, \dots, X_n, f^{-1}]) = \{\mathfrak{p} \in \operatorname{Spec}(k[X_1, \dots, X_n]) \mid \mathfrak{p} \cap \{f\} = \varnothing\}.$$

Thus we obtain

$$\{x \in k^n \mid f \notin \mathfrak{m}_x\} \hookrightarrow \operatorname{Spec}(k[X_1, \dots, X_n, f^{-1}]).$$

We can rewrite the domain as

$$\{x \in k^n \mid f \notin \mathfrak{m}_x\} = \{x \in k^n \mid \varphi_x(f) \neq 0\} = \{x \in k^n \mid f(x) \neq 0\}.$$

In fact, we will soon prove the following theorem (see Theorem 6.8).

Theorem 5.36 (**Hilbert's Nullstellensatz**)**.** *Assume that k is an algebraically closed field. Then there exists a bijection*

$$k^n \cong \operatorname{MaxSpec}(k[X_1, \dots, X_n]), \qquad x = (x_1, \dots, x_n) \mapsto \mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n).$$

This is compatible with the following statement.

Proposition 5.37. *Consider the $\mathbb{C}$-algebra map $h\colon \mathbb{C}[Y_1,\dots,Y_m] \to \mathbb{C}[X_1,\dots,X_n]$, $Y_j \mapsto f_j(X_1,\dots,X_n)$. Then the following diagram commutes:*

$$\begin{array}{ccc} (x_1,\dots,x_n) & \mathbb{C}^n \xrightarrow[\cong]{\varphi} & \mathrm{MaxSpec}(\mathbb{C}[X_1,\dots,X_n]) \\ \downarrow & \downarrow & \downarrow{\scriptstyle \mathrm{Spec}(h)} \\ (f_1(x),\dots,f_m(x)) & \mathbb{C}^m \xrightarrow[\cong]{\varphi} & \mathrm{MaxSpec}(\mathbb{C}[X_1,\dots,X_m]) \end{array}$$

Proof. Let $x = (x_1,\dots,x_n) \in \mathbb{C}^n$ and $\mathfrak{m}_x \in \mathrm{MaxSpec}(\mathbb{C}[X_1,\dots,X_n])$ by Hilbert's Nullstellensatz 5.36. As noted in Example 5.34, we have $(\mathrm{Spec}(h))(\mathfrak{m}_x) = h^{-1}(\mathfrak{m}_x) = h^{-1}(\ker(\varphi_x))$. Thus this equals the kernel of the composition $h \circ \varphi_x$, $Y_j \mapsto f_j(x)$, which is $(Y_1 - f_1(x),\dots,Y_m - f_m(x))$. If $y := (f_1(x),\dots,f_m(x)) \in \mathbb{C}^m$ is the image of x, then this is indeed $\mathfrak{m}_y \in \mathrm{MaxSpec}(\mathbb{C}[Y_1,\dots,Y_m])$. □

6 Basics in Algebraic Geometry

Lect. 15
12.06.23

In this section, we study the connections between geometry and algebra, and in particular, some notions in *algebraic geometry*. In particular, some geometric problems can be solved very elegantly with algebraic properties.

6.1 Noether Normalisation and Hilbert's Nullstellensatz

We are still in in the context of solving a system of polynomial equations as in Problem 5.20. But from now on, we only consider $R = k$ a field, which includes $k = \mathbb{C}$, the setting of classical geometry.

The following is a motivation for what is about to come.

Proposition 6.1. *Let k be an algebraically closed field and $f \in k[T_1,\dots,T_n]$ be non-constant. Then there exists a solution $x \in k^n$ such that $f(x) = 0$.*

Proof. Since f is non-constant, there exists some T_i such that T_i is in a monomial with non-zero coefficient; otherwise the only monomial would be $T_1^0 \cdots T_n^0$. W. l. o. g. let this variable be T_n. Then we can write $f = f_d T_n^d + f_{d-1} T_n^{d-1} + \cdots + f_0$ with $f_1,\dots,f_d \in k[T_1,\dots,T_{n-1}]$, $f_d \neq 0$ and $d \geq 1$.

If $f_d \neq 0$ is constant, we can choose any $(x_1,\dots,x_{n-1}) \in k^{n-1}$ and have $f_d(x_1,\dots,x_{n-1}) \neq 0$. Otherwise by induction, we may assume that the proposition to be shown is true for $n-1$. Therefore the non-constant polynomial $f_d(T_1,\dots,T_{n-1}) - 1 \in k[T_1,\dots,T_{n-1}]$ has a solution $(x_1,\dots,x_{n-1}) \in k^{n-1}$, and hence $f_d(x_1,\dots,x_{n-1}) = 1 \neq 0$.

In both cases, we obtain that $f(x_1,\dots,x_{n-1},T_n) \in k[T_n]$ is a non-constant polynomial. Since k is algebraically closed, it must have a root $x_n \in k$, and hence $x = (x_1,\dots,x_n) \in k^n$ is a solution of $f(x) = 0$. □

Example 6.2. Consider $T_1 T_2 = 1$. Setting $T_2 = 0$ implies $0T_1 = 1$, which has no solution. The proof above circumvents this by enforcing $T_2 = 1$.

The Noether normalisation theorem states that the method above finds a solution of any system of polynomial equations.

Recall: Let $A \subseteq B$ be rings. We call $x \in B$ *integral* over A if there exists a monic $f \in A[T]$ such that $f(x) = 0$. Furthermore, B is *integral* over A if every $x \in B$ is integral. B is *finite* over A if B is finite as an A-module. Corollary 5.8 states that B being finite implies B being integral.

Definition 6.3. Elements $x_1,\dots,x_m$ of a k-algebra A are called **algebraically independent** over k if $f(x_1,\dots,x_m) = 0$ implies $f = 0$ for all $f \in k[X_1,\dots,X_m]$. Alternatively, $x_1,\dots,x_m \in A$ are algebraically independent if $k[x_1,\dots,x_m] \cong k[X_1,\dots,X_m]$.

This is analogous to linear independence in vector spaces, where linear independent vectors only satisfy the trivial linear relation.

Definition 6.4. Let k be a field. If $f = \sum_{e \in (\mathbb{Z}_{\geq 0})^n} a_e Y^e \in k[Y_1,\dots,Y_n]$ with $a_e \in k$, then we define the **total degree** of f to be $\deg(f) := \max\{e_1 + \cdots + e_n \mid a_e \neq 0\}$.

Theorem 6.5 (**Noether normalisation theorem**). *Let k be a field, and let A a finitely generated k-algebra. Then there are algebraically independent $x_1, \dots, x_m \in A$ such that A is finite over $k[x_1, \dots, x_m]$.*

Proof. Let $y_1, \dots, y_n \in A$ be a finite set of generators of A. Then we can understand A as the ring $k[y_1, \dots, y_n]$. We proceed by induction on n. If $n = 0$, then $A = k$, and we are done by taking $m = 0$.

If $y_1, \dots, y_n$ are algebraically independent, then we are also done by taking $x_i = y_i$. So assume instead that there exists some non-constant $f \in k[Y_1, \dots, Y_n]$ such that $f(y_1, \dots, y_n) = 0$. Let $d \coloneqq \deg(f) \geq 1$ and chose any $\alpha > d$, say $\alpha \coloneqq d + 1 \geq 2$. Put $Z_i \coloneqq Y_i - Y_n^{\alpha^i}$ for all $i = 1, \dots, n-1$. So a change of variables yields the k-algebra isomorphism

$$k[Z_1, \dots, Z_{n-1}, Y_n] \cong k[Y_1, \dots, Y_n], \qquad Z_i \mapsto Y_i - Y_n^{\alpha^i}, \qquad Z_i + Y_n^{\alpha^i} \mapsfrom Y_i.$$

Under this transformation, f becomes

$$f \mapsto g(Z_1, \dots, Z_{n-1}, Y_n) \coloneqq f(Z_1 + Y_n^{\alpha}, Z_2 + Y_n^{\alpha^2}, \dots, Z_{n-1} + Y_n^{\alpha^{n-1}}, Y_n) \in k[Z_1, \dots, Z_{n-1}, Y_n].$$

Furthermore, observe that for monomials of f with $e = (e_1, \dots, e_n) \in (\mathbb{Z}_{\geq 0})^n$,

$$\begin{aligned} a_e Y_1^{e_1} \cdots Y_n^{e_n} &\mapsto a_e (Z_1 + Y_n^{\alpha})^{e_1} \cdots (Z_{n-1} + Y_n^{\alpha^n})^{e_{n-1}} Y_n^{e_n} \\ &= a_e Y_n^{\alpha e_1 + \alpha^2 e_2 + \cdots + \alpha^{n-1} e_{n-1} + e_n} + a_e \varepsilon(Z_1, \dots, Z_{n-1}, Y_n) \end{aligned}$$

where the rest term $\varepsilon(Z_1, \dots, Z_{n-1}, Y_n)$ only involves monomials which are not pure Y_n-powers.

The map

$$\{0, \dots, d\}^n \to \mathbb{Z}_{\geq 0}, \qquad (e_1, \dots, e_n) \mapsto \alpha e_1 + \alpha^2 e_2 + \cdots + \alpha^{n-1} e_{n-1} + e_n$$

is injective. Indeed, by the α-adic expansion of the integers, any positive integer is *uniquely* of the form $\sum_{i=0}^{r} e_i \alpha^i$ with $0 \leq e_i < \alpha$ and $e_r \neq 0$. So the claimed injectivity follows from $d < \alpha$. This implies that the terms $a_e Y^{\alpha e_1 + \alpha^2 e_2 + \cdots + \alpha^{n-1} e_{n-1} + e_n}$ of all monomials of f do not cancel each other. Thus there is some $0 \neq c \in k$ and $N \geq 1$ such that

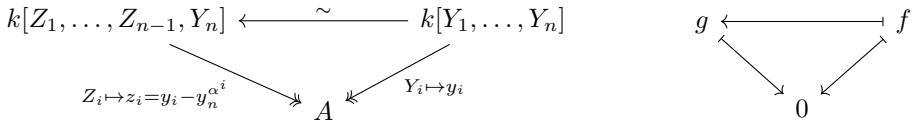
$$g = c Y_n^N + \sum_{k=0}^{N-1} h_k(Z_1, \dots, Z_{n-1}) Y_n^k.$$

(If f is of the form $\sum_{e \in (\mathbb{Z}_{\geq 0})^n} a_e Y^e$, take

$$N \coloneqq \max\{\alpha e_1 + \alpha^2 e_2 + \cdots + \alpha^{n-1} e_{n-1} + e_n \mid e \in (\mathbb{Z}_{\geq 0})^n, a_e \neq 0\}$$

and $c = a_e$.)

So our current situation is the following commutative diagram:



In other words, we get

$$0 = c^{-1} g(z_1, \dots, z_{n-1}, y_n) = y_n^N + c^{-1} \sum_{k=0}^{N-1} h_k(z_1, \dots, z_{n-1}) y_n^k,$$

i. e. y_n and hence A are integral over $B = k[z_1, \dots, z_{n-1}]$.

By our induction hypothesis, we can find algebraically independent $x_1, \dots, x_m \in B$ such that B is finite over $k[x_1, \dots, x_m]$. Hence A is finite over $k[x_1, \dots, x_m]$. □

The idea was to transform all variables except for Y_n, like shearing in vector spaces. Such a transformation will always be an automorphism. The effect is that Y_n will have a large enough power so that it will not vanish.

Example 6.6. Consider $A = k[Y_1, Y_2]/(Y_1Y_2 - 1)$. Set $y_i \coloneqq Y_i \bmod (Y_1Y_2 - 1)$ for $i = 1, 2$.

We claim that A is not integral and thus not finite over $k[y_1]$ or $k[y_2]$. Recall from Corollary 5.15 that if $A \subseteq B$ is integral, then $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective. But the two projection $\operatorname{Spec}(A) \to \operatorname{Spec}(k[y_i])$ on spectra $(i = 1, 2)$ leave out the maximal ideal (y_i) (see Figure 6.1).

The reason is the following: Observe that $A \cong k[Y_i, Y_i^{-1}]$. By Example 2.57, $\operatorname{Spec}(k[Y_i, Y_i^{-1}]) = \{(0)\} \sqcup \{(f) \mid Y_i \neq f \in k[Y_i] \text{ irreducible}\}$. Thus the projection $\operatorname{Spec}(k[Y_i, Y_i^{-1}]) \to \operatorname{Spec}(k[Y_i])$ leaves out (Y_i).

We can circumvent this by applying the transformation we did in the proof of Noether normalisation 6.5. Here, $f = Y_1Y_2 - 1$, so $d = 2$ and $\alpha = 3$. The change of variables is $Z_1 = Y_1 - Y_2^3$, which gives $g = (Z_1 + Y_2^3)Y_2 - 1 = Y_2^4 + Z_1Y_2 - 1$. Then the proof states that y_2 and thus A is integral over $k[z_1] = k[y_1 - y_2^3]$. Indeed, we have $y_2^4 + z_1y_2 - 1 = y_2^4 + y_1y_2 - y_2^4 - 1 = 0$.

But $\operatorname{Spec}(A) \to \operatorname{Spec}(k[y_1 - y_2^3])$ is hard to draw and $k[y_1 - y_2^3] \subseteq A$ is unnecessarily complicated. In fact, $k[z] \subseteq A$ with $z = y_1 - y_2$ is easier (see Figure 6.2). Indeed, $y_1^2 - zy_1 - 1 = y_2^2 + zy_2 - 1 = 0$, so y_1 and y_2 and thus A are integral over $k[z]$.

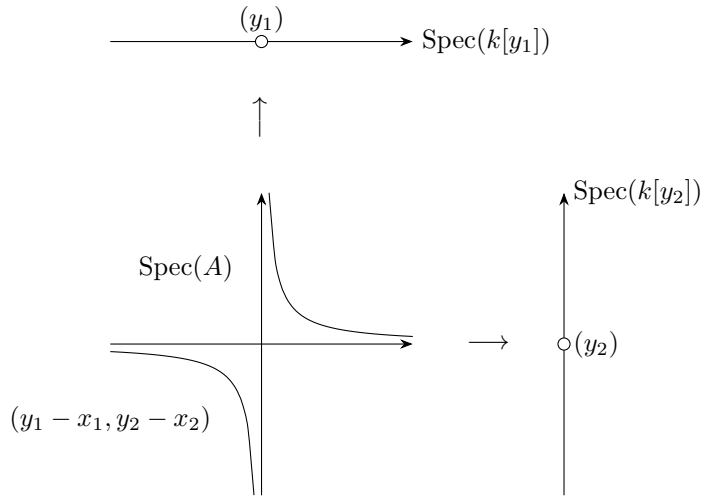


Figure 6.1: Projection $\operatorname{Spec}(A) \to \operatorname{Spec}(k[y_i])$ for algebraically closed k. Note that the generic point (0) is not depicted in any of the spectra.

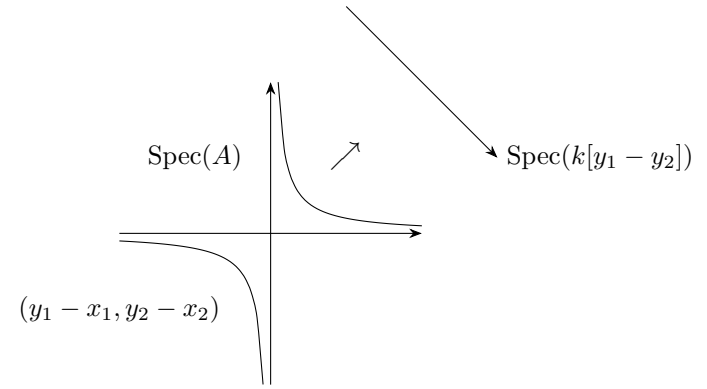


Figure 6.2: Projection $\operatorname{Spec}(A) \to \operatorname{Spec}(k[y_1 - y_2])$ for algebraically closed k. Note that the generic point (0) is not depicted in any of the spectra.

Remark 6.7. (From me.) We obtain $\operatorname{Spec}(A)$ for algebraically closed k in Figure 6.1 as follows: Similar to Example 2.59, the non-zero ideals in $\operatorname{Spec}(k[Y_1, Y_2])$ are (f) with irreducible $f \in k[Y_1, Y_2]$ or maximal $(Y_1 - x_1, Y_2 - x_2)$ with $x_1, x_2 \in k$. By Example 2.57, $\operatorname{Spec}(A)$ consist of ideals in $\operatorname{Spec}(k[Y_1, Y_2])$ containing $Y_1Y_2 - 1$. Since $Y_1Y_2 - 1$ is already irreducible, the only such ideal of the form (f) is $(Y_1Y_2 - 1)$, which corresponds to $(0) \subseteq A$. For ideals $(Y_1 - x_1, Y_2 - x_2) = \mathfrak{m}$, we have $Y_2(Y_1 - x_1) + x_1(Y_2 - x_2) = Y_1Y_2 - x_1x_2 \in \mathfrak{m}$.

So if $Y_1Y_2 - 1 \in \mathfrak{m}$, then necessarily $x_1x_2 = 1$, for otherwise $\mathfrak{m}$ would contain the unit $x_1x_2 - 1$. To summarise,

$$\operatorname{Spec}(A) = \{(0)\} \sqcup \{(y_1 - x_1, y_2 - x_2) \mid x_1, x_2 \in k, x_1x_2 = 1\}.$$

Now an important result in classical algebraic geometry.

Theorem 6.8 (Hilbert's Nullstellensatz). *Let k be a field, let A be a finitely generated k-algebra, and let $\mathfrak{m} \subseteq A$ be a maximal ideal. Then $A/\mathfrak{m}$ is a finite field extension of k.*

Proof. Recall Proposition 5.12: If $A \subseteq B$ is an integral ring extension, and if both A and B are integral domains, then A is a field if and only if B is a field.

By assumption, A is finitely generated, so $A/\mathfrak{m}$ is finitely generated as well. Namely, if $A = k[y_1, \dots, y_n]$, then $A/\mathfrak{m} = k[\bar{y}_1, \dots, \bar{y}_n]$ with $\bar{y}_i \coloneqq y_i + \mathfrak{m}$. By Noether normalisation 6.5, we find algebraically independent $x_1, \dots, x_m \in A/\mathfrak{m}$ such that $A/\mathfrak{m}$ is finite over $k[x_1, \dots, x_m]$. In particular, by Corollary 5.8, $A/\mathfrak{m}$ is integral over $k[x_1, \dots, x_m]$. Both $A/\mathfrak{m}$ and $k[x_1, \dots, x_m] \cong k[X_1, \dots, X_m]$ are integral domains, and $A/\mathfrak{m}$ is a field, so $k[x_1, \dots, x_m]$ is a field. Hence $m = 0$, and therefore $A/\mathfrak{m}$ is finite over k. □

Corollary 6.9. *Let k be an algebraically closed field. Then every maximal ideal of $k[X_1, \dots, X_n]$ is of the form $\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n)$ for a unique tuple $x = (x_1, \dots, x_n) \in k^n$. More precisely, $x \mapsto \mathfrak{m}_x$ is a bijection $k^n \cong \operatorname{MaxSpec}(k[X_1, \dots, X_n])$.*

Proof. First we show uniqueness. If $X_i - x_i, X_i - x_i' \in \mathfrak{m}$, then $x_i - x_i' \in \mathfrak{m}$. Since $\mathfrak{m}$ contains no units by maximality, we must have $x_i - x_i' = 0$.

Now we show the existence of x, given $\mathfrak{m}$. By Hilbert's Nullstellensatz 6.8, $k[X_1, \dots, X_n]/\mathfrak{m}$ is a finite and thus algebraic field extension of k. From [Sch, Thm. 5.41], we know that $k[X_1, \dots, X_n]/\mathfrak{m} \cong k$ since k is already algebraically closed. So $\mathfrak{m}$ is the kernel of the map $\beta^{-1} \circ \alpha$ in the following diagram:

$$\begin{array}{ccc} k[X_1, \dots, X_n] & \xrightarrow{\ \alpha\ } & k[X_1, \dots, X_n]/\mathfrak{m} \\ & \nwarrow \quad \nearrow_{\beta}^{\sim} & \\ & k & \end{array}$$

Let $x_i = (\beta^{-1} \circ \alpha)(X_i)$ for $i = 1, \dots, n$. Then $(\beta^{-1} \circ \alpha)(X_i - x_i) = 0$, hence $\mathfrak{m}_{(x_1, \dots, x_n)}$ is also the kernel. Therefore $\mathfrak{m} = \mathfrak{m}_{(x_1, \dots, x_n)}$.

The bijection follows from the fact that for each $x \in k^n$, the ideal $\mathfrak{m}_x$ is maximal in $k[X_1, \dots, X_n]$ because $k[X_1, \dots, X_n]/\mathfrak{m}_x \cong k$ is a field. □

6.2 Basic Applications

Lect. 16
15.06.23

Now an application to polynomial equations.

Corollary 6.10 (weak Nullstellensatz). *Let k be an algebraically closed field, let $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ be arbitrary, and set $A \coloneqq k[X_1, \dots, X_n]/(f_1, \dots, f_m)$. Then there exists a solution $x \in k^n$ such that $f_1(x) = \cdots = f_m(x) = 0$ if and only if $A \neq 0$, i. e. $1 \notin (f_1, \dots, f_m)$. Moreover, there exist infinitely many solutions if and only if $\dim_k(A) = \infty$ (or equivalently $\dim(A) > 0$ for the Krull dimension).*

Proof. By Corollary 6.9 and Remark 2.3, we have the bijections

$$\{x \in k^n \mid f_1(x) = \cdots = f_m(x) = 0\} \cong \{\mathfrak{m} \in \operatorname{MaxSpec}(k[X_1, \dots, X_n]) \mid (f_1, \dots, f_m) \subseteq \mathfrak{m}\} \cong \operatorname{MaxSpec}(A).$$

(For the first bijection: Recall from Example 5.34 that we can characterise the maximal ideals $\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n)$ as the kernel of the evaluation map $\varphi_x \colon k[X_1, \dots, X_n] \to k$, $f \mapsto f(x)$. Hence for any $x \in k^n$, $f_i(x) = 0$ holds if and only if $f_i \in \ker(\varphi_x) = \mathfrak{m}_x$.) Thus there exists a solution if and only if $A \neq 0$ (Krull's theorem 2.18).

For the second statement, A is finitely generated, so we can apply Noether normalisation 6.5 to find algebraically independent $z_1, \dots, z_d \in A$ such that A is finite over $k[z_1, \dots, z_d]$. Since $k[z_1, \dots, z_d]$ is a k-vector subspace of A, if $\dim_k(A) < \infty$, then $\dim_k(k[z_1, \dots, z_d]) < \infty$. Conversely, if $\dim_k(k[z_1, \dots, z_d]) < \infty$, then this polynomial ring admits a finite k-basis, and since $k[z_1, \dots, z_d] \subseteq A$ is finite, $\dim_k(A) < \infty$ as well. To summarise,

$\dim_k(A) = \infty$ if and only if $\dim_k(k[z_1, \dots, z_d]) = \infty$. But as a polynomial ring, $\dim_k(k[z_1, \dots, z_d]) = \infty$ if and only if $d \geq 1$.

By Corollary 6.9, we have $\mathrm{MaxSpec}(k[z_1, \dots, z_d]) \cong k^d$, which is infinite if and only if $d \geq 1$. Since $k[z_1, \dots, z_d] \subseteq A$ is finite, it is also integral due to Corollary 5.8. By Corollary 5.15 and Exercise 8.43, $\mathrm{Spec}(A) \twoheadrightarrow \mathrm{Spec}(k[z_1, \dots, z_d])$ is surjective with finite fibres. This induces a surjection on maximal spectra, so $\mathrm{MaxSpec}(k[z_1, \dots, z_d])$ is infinite if and only if $\mathrm{MaxSpec}(A)$ is infinite. Recall that $\mathrm{MaxSpec}(A)$ corresponds to the solutions.

(We will later see in Theorem 6.33 that $\dim(k[z_1, \dots, z_d]) = d$ for the Krull dimension, so $d \geq 1$ if and only if $\dim(A) = \dim(k[z_1, \dots, z_d]) = d \geq 1$ by Corollary 5.17.) □

Another classical result, which exemplifies the usage of algebra for geometric problems.

Proposition 6.11 (Bézout's theorem). *Let k be an algebraically closed field, and let $f, g \in k[X, Y]$ be of degrees $\deg(f) = n$ and $\deg(g) = m$. Set $S := \{(x, y) \in k^2 \mid f(x, y) = g(x, y) = 0\}$ as their solution set, and set $A := k[X, Y]/(f, g)$. Then the following hold:*

(i) *S is infinite if and only if f and g have a common non-trivial factor.*

(ii) *If S is finite, then $|S| \leq \dim_k(A) \leq nm$.*

Proof.

(i) f and g have a common non-constant factor $h \in k[X, Y]$ if and only if there exists a height 1 prime ideal $\mathfrak{p} \subseteq k[X, Y]$ such that $f, g \in \mathfrak{p}$ (concretely, $\mathfrak{p} = (h_0)$ for an irreducible factor $h_0 \mid h$). This is equivalent to $\dim(A) \geq 1$ for the Krull dimension.

There exist algebraically independent $z_1, \dots, z_d \in A$ such that $k[z_1, \dots, z_d] \subseteq A$ is finite and thus integral by Noether normalisation 6.5, so Corollary 5.17 says that the above reads as $\dim(k[z_1, \dots, z_d]) = \dim(A) \geq 1$, which is equivalent to $d \geq 1$. By the same arguments as in the proof of Corollary 6.10, $d \geq 1$ if and only if $\mathrm{MaxSpec}(A) \cong S$ is infinite.

(ii) If S is finite, then f and g have no common non-trivial factor by the above. Suppose that $af = bg$ for some $a, b \in k[X, Y]$. As f and g have no common non-trivial factor, it follows that $f \mid b$ and $g \mid a$, i. e. $b = fb'$ and $a = ga'$ for certain $a', b' \in k[X, Y]$. We obtain $fg(a' - b') = 0$, which implies $a' = b'$ (note that $k[X, Y]$ is an integral domain).

In other words, if we write $R := k[X, Y]$, then we have the following short exact sequence of R-modules:

$$0 \longrightarrow R \xrightarrow{\binom{-g}{f}} R^{\oplus 2} \xrightarrow{(f\ g)} (f, g) \longrightarrow 0 \tag{6.12}$$

(Exactness in (f, g) is clear. We just showed $\ker((f\ g)) \subseteq \mathrm{im}(\binom{-g}{f})$. The converse inclusion is obvious.)

Let $R_d := \{h \in R \mid \deg(h) \leq d\}$. By Noether's isomorphism theorem and by the rank-nullity theorem, we have

$$\dim_k((R_d + (f, g))/(f, g)) = \dim_k(R_d/(R_d \cap (f, g))) = \dim_k(R_d) - \dim_k(R_d \cap (f, g)).$$

Observe that since $\dim_k(A) < \infty$ by (i), we can bound $\dim_k(A)$ by the above dimensions for sufficiently large d. Assume that $d \geq n + m$ as well, so that $d - n, d - m \geq 0$. Then

$$\begin{aligned}\dim_k(R_d \cap (f, g)) &\geq \dim_k(\mathrm{im}(\begin{pmatrix} f & g \end{pmatrix} \colon R_{d-n} \times R_{d-m} \to R_d)) \\ &= \dim_k(R_{d-n} \times R_{d-m}) - \dim_k(\ker(\begin{pmatrix} f & g \end{pmatrix}) \cap R_{d-n} \times R_{d-m}).\end{aligned}$$

The inequality follows since the image is a subspace of $R_d \cap (f, g)$. The equality follows from the rank-nullity theorem. By exactness of (6.12), we have

$$\ker(\begin{pmatrix} f & g \end{pmatrix}) \cap R_{d-n} \times R_{d-m} = \mathrm{im}\left(\begin{pmatrix} -g \\ f \end{pmatrix}\right) \cap R_{d-n} \times R_{d-m} \cong R_{d-n-m}.$$

The isomorphism follows since $\binom{-g}{f}$ is injective. (For all $h \in R_{d-n-m}$, we have $\deg(-gh) \leq d-n$ and $\deg(fh) \leq d-m$.) Furthermore, $\dim_k(R_{d-n} \times R_{d-m}) = \dim_k(R_{d-n}) + \dim_k(R_{d-m})$. Now note that a k-basis of R_d is given by all monic monomials and 1, thus

$$\dim_k(R_d) = 1 + 2 + \cdots + (d+1) = \frac{(d+1)(d+2)}{2} =: s(d),$$

whence

$$\dim_k(A) \leq s(d) - s(d-n) - s(d-m) + s(d-n-m) = nm.$$

By Corollary 6.9 and by the proof of Exercise 8.7, we have $|S| = |\mathrm{MaxSpec}(A)| \leq |\mathrm{Spec}(A)| \leq \dim_k(A)$ for finite-dimensional A. □

Remark 6.13. This can be generalised in *algebraic intersection theory*: Let $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$ such that $S := \{x \in k^n \mid f_1(x) = \cdots = f_n(x) = 0\}$ is finite. Then

$$|S| \leq \dim_k(k[X_1, \ldots, X_n]/(f_1, \ldots, f_n)) \leq \deg(f_1) \cdots \deg(f_n).$$

6.3 Algebraic Sets and Ideals

Definition 6.14. Let k be an algebraically closed field. A subset $Z \subseteq k^n$ is **algebraic** if there exists a subset $S \subseteq k[X_1, \ldots, X_n]$ such that $Z = \{x \in k^n \mid f(x) = 0 \text{ for all } f \in S\}$. We call $Z(S) := Z$ the **vanishing set** of S.

Observation 6.15. The algebraic subsets of k^n form the closed sets of a topology on k^n, the so-called **Zariski topology**.

Recall: The axioms of a topological space X are the following: $\varnothing$ and X are closed. For closed sets $Z_i \subseteq X$ with $i \in I$, their intersection $\bigcap_{i \in I} Z_i$ is closed. For closed sets $Z_1, Z_2 \subseteq X$, their union $Z_1 \cup Z_2$ is closed.

(i) $\varnothing$ and k^n are algebraic because $\varnothing = Z(1)$ and $k^n = Z(0)$. Hence they are closed.

(ii) We easily see that $\bigcap_{i \in I} Z(S_i) = Z(\bigcup_{i \in I} S_i)$. Hence $\bigcap_{i \in I} Z(S_i)$ is algebraic, and hence closed.

(iii) We show that $Z(S) \cup Z(T) = Z(\{st \mid s \in S, t \in T\})$. It is clear that $Z(S) \cup Z(T)$ is contained in the right-hand side.

Conversely, suppose there exists some $x \in Z(\{st \mid s \in S, t \in T\})$ with $x \notin Z(S)$, i. e. there is some $s_0 \in S$ such that $s_0(x) \neq 0$. By assumption, $(s_0 t)(x) = 0$ for all $t \in T$. This is only possible if $t(x) = 0$ for all $t \in T$ as k is an integral domain, so $x \in Z(T)$.

Therefore $Z(S) \cup Z(T)$ is algebraic and thus closed.

We observe that $Z(S) = Z((S))$, i. e. the vanishing set depends only on ideals.

Remark 6.16. (From me.) In fact, we also have $Z(\mathfrak{a}) \cup Z(\mathfrak{b}) = Z(\mathfrak{a} \cap \mathfrak{b})$ for ideals $\mathfrak{a}, \mathfrak{b} \subseteq k[X_1, \ldots, X_n]$. Reason being that $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b}$, so $Z(\mathfrak{a}) \cup Z(\mathfrak{b}) \subseteq Z(\mathfrak{a} \cap \mathfrak{b}) \subseteq Z(\mathfrak{ab})$.

Definition 6.17. Let k be an algebraically closed field. Given $Y \subseteq k^n$, we define the **vanishing ideal** as $I(Y) := \{f \in k[X_1, \ldots, X_n] \mid f(y) = 0 \text{ for all } y \in Y\}$.

Remark 6.18. As k is reduced, we have $f^n \in I(Y)$ if and only if $f \in I(Y)$.

Definition 6.19. An ideal $\mathfrak{a}$ of any ring A is **radical** if $f^n \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ for all $f \in A$. This is equivalent to $A/\mathfrak{a}$ being reduced.

For any ideal $\mathfrak{a} \subseteq A$, we define the **radical** of $\mathfrak{a}$ to be $\sqrt{\mathfrak{a}} := \{f \in A \mid f^n \in \mathfrak{a} \text{ for some } n \geq 0\}$.

Remark 6.20. (From me.) The radical $\sqrt{\mathfrak{a}}$ is again an ideal. The proof is very similar to the proof that $\mathrm{nil}(A)$ is an ideal, see Proposition 1.23.

Furthermore, $\sqrt{\mathfrak{a}}$ is radical. If $f^n \in \sqrt{\mathfrak{a}}$, then f^{nm} for some $m \geq 0$, hence $f \in \sqrt{\mathfrak{a}}$.

Remark 6.21. The following hold true:

(i) $Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$ and $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \subseteq I(Z(\mathfrak{a}))$ for all $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$.

Proof: Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, we have $Z(\sqrt{\mathfrak{a}}) \subseteq Z(\mathfrak{a})$. Conversely, let $x \in Z(\mathfrak{a})$. For each $f \in \sqrt{\mathfrak{a}}$, there is some $n \geq 0$ such that $f^n \in \mathfrak{a}$. Thus by assumption, $f(x)^n = 0$, and, as k is reduced, $f(x) = 0$, i. e. $x \in Z(\sqrt{a})$.

For the other statement, observe that in general, $\mathfrak{b} \subseteq I(Z(\mathfrak{b}))$ for all ideals $\mathfrak{b} \subseteq k[X_1, \dots, X_n]$ (for all $x \in Z(\mathfrak{b})$ and $f \in \mathfrak{b}$, we have $f(x) = 0$). Thus $\sqrt{\mathfrak{a}} \subseteq I(Z(\sqrt{\mathfrak{a}})) = I(V(\mathfrak{a}))$.

(ii) $I(Y) = I(\overline{Y})$ and $Y \subseteq \overline{Y} \subseteq Z(I(Y))$ for all subsets $Y \subseteq k^n$, where $\overline{Y}$ is the closure w. r. t. the Zariski topology, i. e. the smallest algebraic set containing Y.

Proof: Since $Y \subseteq \overline{Y}$, we have $I(\overline{Y}) \subseteq I(Y)$. Conversely, let $f \in I(Y)$. By assumption, we have $Y \subseteq Z(f)$, and by minimality of $\overline{Y}$, we have $\overline{Y} \subseteq Z(f)$. Thus $f \in I(\overline{Y})$.

For the other statement, observe that in general, $S \subseteq Z(I(S))$ for all subsets $S \subseteq k^n$ (for all $f \in I(S)$ and $x \in S$, we have $f(x) = 0$). Thus $\overline{Y} \subseteq Z(I(\overline{Y})) = Z(I(Y))$.

Remark 6.22. The Zariski topology on $\mathbb{C}^n$ is coarser then the standard Euclidean topology. We have $\overline{Y}^{\text{Euclidean}} \subseteq \overline{Y}^{\text{Zariski}}$, which is usually strict.

E. g. for $n = 1$, consider $Y = \mathbb{Z} \subset \mathbb{C}$. Then $Y = \overline{Y}^{\text{Euclidean}} \subset \overline{Y}^{\text{Zariski}} = \mathbb{C}$ (there is no polynomial which has infinitely many roots).

The following version for algebraically closed fields in the language of algebraic geometry is also known as *Hilbert's Nullstellensatz*.

Theorem 6.23 (**Hilbert's Nullstellensatz**). *Let k be an algebraically closed field. Then Z and I define mutually inverse bijections between algebraic subsets of k^n and radical ideals in $k[X_1, \dots, X_n]$ via $Z \mapsto I(Z)$ and $Z(\mathfrak{a}) \leftarrow\!\shortmid \mathfrak{a}$. More generally, we have $Z(I(Z)) = Z$ for all algebraic subsets $Z \subseteq k^n$, and $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for all ideals $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$.*

Proof. Abbreviate $R \coloneqq k[X_1, \dots, X_n]$. We claim that $\sqrt{\mathfrak{a}} = I(Z(\mathfrak{a}))$ for all ideals $\mathfrak{a} \subseteq R$. We know $\sqrt{\mathfrak{a}} \subseteq I(Z(\mathfrak{a}))$ from Remark 6.21 already.

For the converse inclusion, let $g \in I(Z(\mathfrak{a}))$. Since R is noetherian (Corollary 3.31), we can write $\mathfrak{a} = (f_1, \dots, f_m)$. Now consider $\mathfrak{b} \coloneqq (f_1, \dots, f_m, Xg - 1) \subseteq R[X]$. Let $x \in Z(\mathfrak{a})$, i. e. $f_1(x) = \cdots = f_m(x) = 0$. By assumption, we have $g(x) = 0$, so $yg(x) - 1 \neq 0$ for all $y \in k$. Therefore $\{f_1, \dots, f_m, Xg - 1\}$ have no common solution in k^{n+1}. Corollary 6.10 implies that $\mathfrak{b} = R[X]$, and hence we can write $1 = a_1 f_1 + \cdots + a_m f_m + a(Xg - 1)$ for suitable $a_i, a \in R[X]$.

Passing to $\operatorname{Quot}(R[X])$, set $Y \coloneqq \frac{1}{X}$ as a variable, i. e. $YX = 1$. Multiplying the above equation by Y^N for large enough N, we obtain $Y^N = c_1 f_1 + \cdots + c_m f_m + c(g - Y)$ with $c_i, c \in R[Y]$. Note that this equation does not contain the variable X anymore. Specialising along $R[Y] \to R$, $Y \mapsto g$ gives $g^n = \bar{c}_1 f_1 + \cdots + \bar{c}_m f_m + 0 \in \mathfrak{a}$, where $\bar{c}_i = c_i(X_1, \dots, X_n, g) \in R$. This shows $g \in \sqrt{\mathfrak{a}}$, finishing the claim.

The claim implies that $\mathfrak{a} \mapsto Z(\mathfrak{a})$ is injective on radical ideals. Surjectivity follows from Remark 6.21, namely $\sqrt{\mathfrak{c}} \leftarrow\!\shortmid Z(\mathfrak{c}) = Z(\sqrt{\mathfrak{c}})$ for any ideal $\mathfrak{c} \subseteq R$. Hence this map is a bijection, and the claim further implies that I is its inverse. □

The implications are immense: We can translate any geometric problem about a system of polynomials into the language of commutative algebra without loosing any information.

Remark 6.24. Recall from Proposition 2.22 that for any ring $A \neq 0$, we have $\sqrt{(0)} = \operatorname{nil}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$. Passing to $A/\mathfrak{a}$, we obtain

$$\sqrt{\mathfrak{a}/\mathfrak{a}} = \operatorname{nil}(A/\mathfrak{a}) = \bigcap_{\bar{\mathfrak{p}} \in \operatorname{Spec}(A/\mathfrak{a})} \bar{\mathfrak{p}}.$$

Lifting to A again gives

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$$

since $\bar{f} \in A/\mathfrak{a}$ is nilpotent if and only if $f \in \sqrt{\mathfrak{a}}$, and the bijection in the proof of Corollary 1.29 commutes with intersections.

Hilbert's Nullstellensatz is closely related to the following.

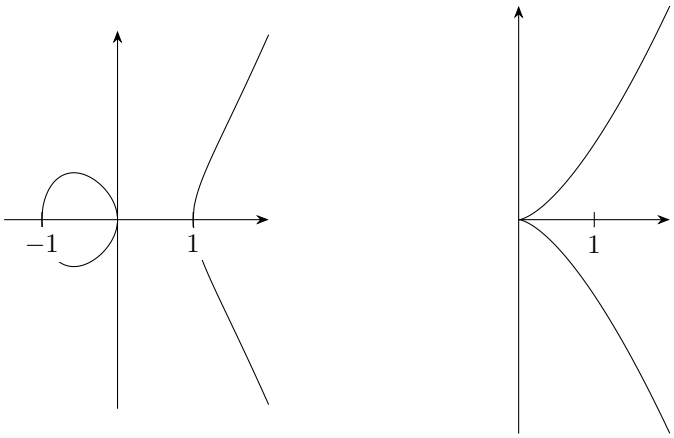


Figure 6.3: Algebraic sets $Z(Y^2 - X^3 - X)$ (left) and $Z(Y^2 - X^3)$ (right). These correspond to the radical ideals $(Y^2 - X^3 - X)$ and $(Y^2 - X^3)$ in $\mathbb{C}[X, Y]$, resp.

Theorem 6.25. *Let k be any field, and let A be a finitely generated k-algebra. Then for all ideals $\mathfrak{a} \subseteq A$, we have*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{m} \in \operatorname{MaxSpec}(A)} \mathfrak{m}. \tag{6.26}$$

*Any ring with the property (6.26) is called a **Jacobson ring**.*

Proof. We will prove this only for $A = k[X_1, \dots, X_n]$ with algebraically closed k. For a general proof, see [Sta, 00G1].

Suppose that $f \in \sqrt{\mathfrak{a}}$. Then $f^n \in \mathfrak{a} \subseteq \mathfrak{m}$ for some $n \geq 0$. Since maximal ideals are prime, we immediately obtain $f \in \mathfrak{m}$. Hence $\sqrt{\mathfrak{a}}$ is contained in the right-hand side.

Conversely, let f be an element of the right-hand side. By Corollary 6.9, every maximal ideal $\mathfrak{m} \subset A$ with $\mathfrak{a} \subseteq \mathfrak{m}$ is of the form $\mathfrak{m} = (X_1 - x_1, \dots, X_n - x_n)$ with $(x_1, \dots, x_n) \in Z(\mathfrak{a})$ (every polynomial in $\mathfrak{a}$ has $(x_1, \dots, x_n)$ as a root). Hence $f \in I(Z(\mathfrak{a}))$. In the proof of the earlier Hilbert's Nullstellensatz 6.23, we have seen that $\sqrt{\mathfrak{a}} = I(Z(\mathfrak{a}))$, so the right-hand side is contained in $\sqrt{\mathfrak{a}}$. □

Remark 6.27. Note that $\mathfrak{p} = \sqrt{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subset A$, so

$$\mathfrak{p} = \bigcap_{\mathfrak{p} \subseteq \mathfrak{m} \in \operatorname{MaxSpec}(A)} \mathfrak{m}.$$

In fact, if A fulfils this property, then A is Jacobson. This follows from the fact that

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \in \operatorname{Spec}(A)} \mathfrak{p}$$

for all ideals $\mathfrak{a} \subset A$.

(From me.) If $f \in \sqrt{\mathfrak{a}}$, then $f^n \in \mathfrak{a}$ for some $n \geq 0$. For all prime ideals $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$, we have $f^n \in \mathfrak{p}$, and by the prime ideal property, $f \in \mathfrak{p}$ for all $\mathfrak{p}$.

Conversely, if $f \notin \mathfrak{a}$, then $f^n \notin \mathfrak{a}$ for all $n \geq 0$. If we consider a consider any prime ideal $\tilde{\mathfrak{p}} \subset A[f^{-1}]$ containing $\mathfrak{a}A[f^{-1}]$ (which exists by Theorem 2.18), then by taking the preimage along $A \to A[f^{-1}]$, this corresponds to a prime ideal $\mathfrak{p} \subset A$ with $f^n \notin \mathfrak{p}$ for all $n \geq 0$ (see Proposition 2.55). In particular, $f \notin \mathfrak{p}$.

Example 6.28. $A = k[\![X_1, \dots, X_n]\!]$ is a local ring with maximal ideal $(X_1, \dots, X_n)$, see Exercise 8.3. But A is not Jacobson, e. g. $0 = \operatorname{nil}(A) \neq \operatorname{jac}(A) = (X_1, \dots, X_n)$.

6.4 Motivation for the Krull Dimension

Lect. 17
19.06.23

Recall: The *(Krull) dimension* $\dim(A)$ of a ring A is the supremum over all $n \geq 0$ such that there exists a chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \subseteq A$.

This notion is interesting for two reasons:

(i) From a technical point of view, we have a natural number over which we can induct.

(ii) The dimension provides intuition for arithmetic in a ring.

Here an example for the second point. The following is a consequence of *Krull's principal ideal theorem*, which we will later prove for finite type algebras over algebraically closed fields.

Theorem 6.29. *Let A be a noetherian integral domain with $\dim(A) = n < \infty$. Let $f_1, \dots, f_m \in A$ be such that $B \coloneqq A/(f_1, \dots, f_m) \neq 0$. Then $\dim(B) \geq n - m$.*

Remark 6.30. (From me.) Krull's theorem actually states the following: Let A be any noetherian ring (not only those with $\dim(A) < \infty$), and let $(f) \subset A$ be a proper principal ideal. Then each minimal prime ideal $\mathfrak{p} \subset A$ containing (f) has height $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Or more general, which can be proved by induction: Let $(f_1, \dots, f_m) \subset A$ be a proper ideal. Then each minimal prime ideal $\mathfrak{p} \subset A$ containing $(f_1, \dots, f_m)$ has height $\operatorname{ht}(\mathfrak{p}) \leq m$. So how does this imply the statement?

Recall that there is a bijection between prime ideals in A containing $(f_1, \dots, f_m)$ and prime ideals in B. Every proper chain of prime ideals in B of maximal length must start with a minimal prime ideal in B, where the latter corresponds to a minimal prime ideal in A above $(f_1, \dots, f_m)$. Thus taking the image in B of a longest proper chain of prime ideals in A cuts of at most m prime ideals at the beginning, and so $\dim(B) \geq n - m$.

The intuition is that given n variables and m equations, if the solution set is non-empty, then its dimension is at least $n - m$.

Example 6.31. Are there $f_1, f_2, f_3 \in \mathbb{C}[X_1, \dots, X_4]$ such that $Z(f_1, f_2, f_3) = \{\mathrm{pt}\} \subseteq \mathbb{C}^4$? The answer is no.

Let us assume that $\dim(\mathbb{C}[X_1, \dots, X_n]) = n$ is true, which we will show in a minute (Theorem 6.33). Put $A \coloneqq \mathbb{C}[X_1, \dots, X_4]/(f_1, f_2, f_3)$. Then by Krull's theorem, $\dim(A) \geq 1$ whenever $A \neq 0$. So Corollary 6.10 says that there are infinitely many solutions, i. e. $Z(f_1, f_2, f_3)$ is infinite, and not only just one point.

Another motivation is the *implicit function theorem*: If $f\colon (f_1, \dots, f_m)\colon \mathbb{R}^n \to \mathbb{R}^m$ is a continuously differentiable multivariate function such that $x \in f^{-1}(0)$ and such that the Jacobian $(\partial f_i/\partial x_j)_{ij}(x)$ has rank m, then a neighbourhood of $x \in f^{-1}(0)$ is homeomorphic to an open subset of $\mathbb{R}^{n-m}$. In particular, $\dim_x(f^{-1}(0)) = n - m$, i. e. $f^{-1}(0)$ is locally at x a $(n-m)$-dimensional submanifold.

Example 6.32. Beware: The picture in $\mathbb{R}$ may be deceiving ($\mathbb{R}$ is not algebraically closed)!

Consider for example $X^2 + Y^2 = 0$. Then $(0, 0) \in \mathbb{R}^2$ is the only solution over $\mathbb{R}$. But over $\mathbb{C}$, we have $X^2 + Y^2 = (X - \mathrm{i}Y)(X + \mathrm{i}Y)$ in $\mathbb{C}[X, Y]$, and thus $Z(X^2 + Y^2) = \{(x, \mathrm{i}x), (x, -\mathrm{i}x) \in \mathbb{C}^2 \mid x \in \mathbb{C}\}$ is a union of two one-dimensional $\mathbb{C}$-vector spaces.

6.5 Dimension of $k[X_1, \dots, X_n]$

Theorem 6.33. *Let k be a field, and let $R_n \coloneqq k[X_1, \dots, X_n]$. Then $\dim(R_n) = n$.*

Proof. Consider the chain of ideals $(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n)$. These are all prime, since $R_n/(X_1, \dots, X_r) \cong k[X_{r+1}, \dots, X_n]$ is an integral domain. Thus we have a proper chain of prime ideals of length n, so $\dim(R_n) \geq n$. It remains to show that $\dim(R_n) \leq n$.

We perform induction over n. The statement is clear for $n = 0, 1$: In these cases, $R_0 = k$ is a field and $R_1 = k[X_1]$ is a principal ideal domain, so $\dim(R_0) = 0$ and $\dim(R_1) = 1$, resp. So assume that $n \geq 2$. Let $(0) \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$ be a chain of m prime ideals in R_n. We want to show $m \leq n$.

Pick any $0 \neq f \in \mathfrak{p}_1$. As R_n is a unique factorisation domain (cf. Gauss's lemma) and $\mathfrak{p}_1$ is prime, there exists a prime factor $p \mid f$ such that $p \in \mathfrak{p}_1$. W. l. o. g. assume that $\mathfrak{p}_1 = (p)$, as otherwise we can simply extend the chain to $(0) \subset (p) \subset \mathfrak{p}_1 \subset \cdots$, and we proceed with the new chain.

Now we use the same technique as during the proof of Noether normalisation 6.5: Let $d \coloneqq \deg(p)$, and let $\alpha \coloneqq d + 1$. Then we have the change of variables $k[Z_1, \dots, Z_{n-1}, X_n] \cong R_n$ via $Z_i \coloneqq X_i - X_n^{\alpha^i}$ for $i = 1, \dots, n-1$. Under this transformation, p becomes

$$p(Z_1 + X_n^{\alpha}, Z_2 + X_n^{\alpha^2}, \dots, Z_{n-1} + X_n^{\alpha^{n-1}}, X_n) = cX_n^N + \sum_{k=0}^{N-1} h_k(Z_1, \dots, Z_{n-1}) X_n^k$$

for appropriate $c \in k^\times$, $N \in \mathbb{Z}_{\geq 0}$ and $h_0, \dots, h_{N-1} \in k[Z_1, \dots, Z_{n-1}]$.

Recall from Example 1.14 that if $f = uT^k + \cdots \in A[T]$ with $u \in A^\times$, then $A[T]/(f) \cong \bigoplus_{i=0}^{k-1} A(T^i + (f))$ as abelian groups, so $A \to A[T]/(f)$ is injective and finite if $k \geq 1$. Thus we see that $k[Z_1, \ldots, Z_{n-1}] \to k[Z_1, \ldots, Z_{n-1}][X_n]/(p) = R_n/(p)$ is injective, finite and, by Corollary 5.8, integral.

From the induction hypothesis, we know that $\dim(k[Z_1, \ldots, Z_{n-1}]) = n-1$. By Corollary 5.17, we have $\dim(R_n/(p)) = \dim(k[Z_1, \ldots, Z_{n-1}]) = n-1$ as well. This gives the chain of prime ideals $(0) = (p)/(p) \subset \mathfrak{p}_2/(p) \subset \cdots \subset \mathfrak{p}_m/(p) \subseteq R_n/(p)$ of length $m-1$. This chain is proper since $R_n \to R_n/(p)$ is surjective. Hence $m \leq n$. □

Corollary 6.34. *Let A be a finitely generated k-algebra. Let $x_1, \ldots, x_d \in A$ be algebraically independent over k such that $k[x_1, \ldots, x_d] \subseteq A$ is finite (this is Noether normalisation 6.5). Then $\dim(A) = d$, implying that d is uniquely determined.*

Proof. Using Corollary 5.17, we have $d = \dim(k[x_1, \ldots, x_d]) = \dim(A)$. □

Example 6.35. Consider $A = k[X_1, X_2, X_3]/X_3(X_1 - X_2, X_1 - X_3)$. Let x_i be the image of X_i in A for $i = 1, 2, 3$. We claim that x_1 and x_2 are algebraically independent, and that $k[x_1, x_2] \subseteq A$ is finite.

The images of x_1 and x_2 along $A \twoheadrightarrow A/(x_3) \cong k[X_1, X_2, X_3]/(X_3) \cong k[X_1, X_2]$ are X_1 and X_2, resp. Since the images of x_1 and x_2 are obviously algebraically independent, x_1 and x_2 must be algebraically independent over k (if x_1 and x_2 satisfy a non-trivial algebraic relation over k, the k-algebra map $A \twoheadrightarrow k[X_1, X_2]$ retains that non-trivial relation). For finiteness, observe that x_3 is integral over $k[x_1, x_2]$ since $x_3^2 - x_1 x_3 = -x_3(x_1 - x_3) = 0$. Thus by Proposition 5.7, $k[x_1, x_2][x_3] \cong A$ is finite over $k[x_1, x_2]$.

Thus $\dim(A) = 2$. Geometrically speaking for $k = \mathbb{C}$ (see Figure 6.4), the $\mathbb{C}$-dimension of each so-called *irreducible component* of $Z(A)$, in this case the plane $Z(X_3)$ and the line $Z(X_1 - X_3, X_2 - X_3)$, cannot exceed $\dim(A)$.

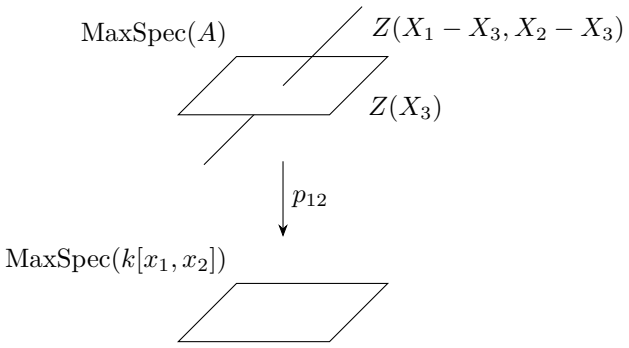


Figure 6.4: Maximal spectra map $p_{12}\colon \operatorname{MaxSpec}(A) \to \operatorname{MaxSpec}(k[x_1, x_2])$, induced by the inclusion $k[x_1, x_2] \hookrightarrow A$. Each maximal spectrum stands in bijection to the solution set of a system of polynomial equations. For A, the equations are $X_3(X_1 - X_2)$ and $X_3(X_1 - X_3)$. For $k[x_1, x_2]$, there are no equations.

The following is a special case of Krull's principal ideal theorem.

Corollary 6.36. *Let k be a field, and let $R_n \coloneqq k[X_1, \ldots, X_n]$. Let $f \in R_n \setminus k$ be a non-constant polynomial. Then $\dim(R_n/(f)) = n - 1$.*

Proof. The change of variables argument from the proof of the theorem can be applied directly to f instead of p. This yields a finite and thus integral ring extension $R_{n-1} \subseteq R_n/(f)$. By Corollary 5.17, we obtain $\dim(R_n/(f)) = \dim(R_{n-1}) = n - 1$. □

6.6 Relation with Transcendence Degree

This subsection is partly based upon [Bos, ch. 7.1].

Definition 6.37. Let L/K be a field extension. A tuple $(x_i)_{i \in I}$ of elements in L is a **transcendence basis** of L if $(x_i)_{i \in I}$ are algebraically independent, and if $L/K(x_i, i \in I)$ is an algebraic field extension.

Recall: $K(x_i, i \in I)$ denotes the smallest intermediate field of L/K containing the x_i, i. e.

$$K(x_i, i \in I) \coloneqq \bigcap_{\substack{K \subseteq M \subseteq L \\ x_i \in M \text{ for all } i}} M.$$

Example 6.38. The elements $X_1, \dots, X_n \in k(X_1, \dots, X_n)$ form a transcendence basis for $k(X_1, \dots, X_n)/k$ because $k(X_1, \dots, X_n)/k(X_1, \dots, X_n)$ is trivially algebraic.

Lemma 6.39. *Let L/K be a field extension. Let $\mathcal{Y} \subseteq L$ be any subset that only consist of over K algebraically independent elements. Let $\mathcal{X} \subseteq L$ be a subset such that $L/K(\mathcal{X})$ is an algebraic field extension. Then there exists a subset $\mathcal{Z} \subseteq \mathcal{X}$ such that $\mathcal{Y} \cup \mathcal{Z}$ is a transcendence basis for L/K.*

Proof. We apply Zorn's lemma to

$$\Sigma \coloneqq \{\mathcal{Z} \subseteq \mathcal{X} \mid \mathcal{Y} \cup \mathcal{Z} \text{ algebraically independent over } K\}$$

w. r. t. the inclusion of sets.

We have $\Sigma \neq \varnothing$ since $\varnothing \in \Sigma$ by assumption. Let $C \subseteq \Sigma$ is a chain, i. e. $\mathcal{Z}_1 \subseteq \mathcal{Z}_2$ or $\mathcal{Z}_2 \subseteq \mathcal{Z}_1$ for all $\mathcal{Z}_1, \mathcal{Z}_2 \in C$. Then $\mathcal{C} \coloneqq \bigcup_{\mathcal{Z} \in C} \mathcal{Z} \in \Sigma$ is an upper bound of C since any algebraic dependence relation (polynomial) over K of elements in $\mathcal{Y} \cup \mathcal{C}$ only involves finitely many elements, and thus occurs already for $\mathcal{Y} \cup \mathcal{Z}$ for some $\mathcal{Z} \in C$.

By Zorn's lemma, a maximal element $\mathcal{Z} \in \Sigma$ exists. $\mathcal{Y} \cup \mathcal{Z}$ is algebraically independent. If L would not be algebraic over $K(\mathcal{Y} \cup \mathcal{Z})$, then $K(\mathcal{Y} \cup \mathcal{X})$ must not be algebraic over $K(\mathcal{Y} \cup \mathcal{Z})$ since $L/K(\mathcal{X})$ and thus $L/K(\mathcal{Y} \cup \mathcal{X})$ are algebraic (cf. [Sch, Cor. 3.9]). So there is some $x \in \mathcal{X} \setminus \mathcal{Z}$ that is transcendental. But then $\mathcal{Y} \cup \mathcal{Z} \cup \{x\}$ is algebraically independent, contradicting the maximality of $\mathcal{Z}$. Thus $\mathcal{Y} \cup \mathcal{Z}$ is a transcendence basis. □

Corollary 6.40.

(i) *Transcendence basis exist.*

(ii) *All transcendence basis have the same cardinality.*

Proof. Let L/K be a field extension.

(i) We apply Lemma 6.39 to $\mathcal{Y} = \varnothing$ and $\mathcal{X} = L$.

(ii) We prove the theorem for finite basis: Let $\mathcal{X} = (x_1, \dots, x_n)$ and $\mathcal{Y}$ be two transcendence basis of L/K. We show that $|\mathcal{Y}| = n$ by induction on n.

If $n = 0$, then L/K as well as $K(\mathcal{Y})/K$ are algebraic. Since $\mathcal{Y}$ is algebraically independent over K, we must have $\mathcal{Y} = \varnothing$.

If $n \geq 1$, then L/K is not algebraic, and $K(\mathcal{Y})/K$ is not algebraic since $L/K(\mathcal{Y})$ is algebraic. So there must exist some $y \in \mathcal{Y}$. Applying Lemma 6.39 to $\{y\}$ and $\mathcal{X}$, we obtain a transcendence basis of the form $(y, x_{i_1}, \dots, x_{i_m})$ with (pairwise different) $x_{i_j} \in \mathcal{X}$. Observe that $m < n$ since y is algebraic over $K(\mathcal{X})$, and otherwise $\{y\} \cup \mathcal{X}$ is not algebraically independent over K.

Now $\mathcal{Y} \setminus \{y\}$ and $(x_{i_1}, \dots, x_{i_m})$ are transcendence bases for $L/K(y)$ (L is obviously algebraic over $K(y)$ adjoin any of the two basis; if there would be a non-trivial algebraic dependence relation of one of the two basis over $K(y)$, then this would be a non-trivial dependence relation of $\mathcal{Y}$ or $(y, x_{i_1}, \dots, x_{i_m})$ over K, a contradiction). By induction, we have $|\mathcal{Y} \setminus \{y\}| = m$, hence $|\mathcal{Y}| \leq |\mathcal{X}|$. In particular, $\mathcal{Y}$ is finite, so we can repeat the same argument with $\mathcal{X}$ and $\mathcal{Y}$ interchanged in order to obtain $|\mathcal{X}| \leq |\mathcal{Y}|$.

(From [Sta, 030F].) For the infinite case, let $\mathcal{X}$ and $\mathcal{Y}$ be two infinite transcendental basis of L/K. Then for each $x \in \mathcal{X}$, there is a finite subset $\mathcal{Y}_x \subseteq \mathcal{Y}$ such that x is algebraic over $K(\mathcal{Y}_x)$ because $L/K(\mathcal{Y})$ is algebraic and any algebraic dependence relation involves only finitely many elements.

Let $\bar{\mathcal{Y}} \coloneqq \bigcup_{x \in \mathcal{X}} \mathcal{Y}_x \subseteq \mathcal{Y}$. By construction, $K(\mathcal{X})$ is algebraic over $K(\bar{\mathcal{Y}})$. Suppose that there exists some $y \in \mathcal{Y} \setminus \bar{\mathcal{Y}}$. Then y is algebraic over $K(\mathcal{X})$ and hence over $K(\mathcal{Y})$, which contradicts the fact that $\mathcal{Y}$ is algebraically independent over K. Therefore $\mathcal{Y} = \bar{\mathcal{Y}}$.

With facts from set-theory (this involves the axiom of choice), we obtain $|\mathcal{Y}| = |\bigcup_{x \in \mathcal{X}} \mathcal{Y}_x| \leq |\mathcal{X}|$ since the $\mathcal{Y}_x$ are finite and $\mathcal{X}$ is infinite. Repeating the same argument with $\mathcal{X}$ and $\mathcal{Y}$ interchanged gives $|\mathcal{X}| \leq |\mathcal{Y}|$. □

Definition 6.41. Let L/K be a field extension. We define the **transcendence degree** $\operatorname{tr.deg}(L/K)$ as the cardinality of any transcendence basis of L/K.

Remark 6.42. Let $M/L/K$ be field extensions. Then

$$\operatorname{tr.deg}(M/L) + \operatorname{tr.deg}(L/K) = \operatorname{tr.deg}(M/K).$$

To proof this, let $\mathcal{X} \subseteq L$ be a transcendence basis of L/K, and let $\mathcal{Y} \subseteq M$ be a transcendence basis of M/L. Since $\mathcal{Y}$ is algebraically independent over L, we must have $\mathcal{Y} \cap L = \varnothing$. Thus $\mathcal{X}$ and $\mathcal{Y}$ are disjoint.

We now check that $\mathcal{X} \sqcup \mathcal{Y}$ is a transcendence basis of M/K, finishing the proof. We know that $M/L(\mathcal{Y})$ and $L/K(\mathcal{X})$ are algebraic, so M is algebraic over $K(\mathcal{X})(\mathcal{Y}) = K(\mathcal{X} \sqcup \mathcal{Y})$. Furthermore, $\mathcal{Y}$ is algebraically independent over L, and $\mathcal{X}$ is algebraically independent over K. If we interpret any algebraic dependence relation of $\mathcal{X} \sqcup \mathcal{Y}$ over K as one of $\mathcal{Y}$ over $K(\mathcal{X}) \subseteq L$, then the coefficients in terms of $\mathcal{Y}$ in this relation are 0. Hence these coefficients are algebraic dependence relations of $\mathcal{X}$ over K, so they must be trivial as well. Thus $\mathcal{X} \sqcup \mathcal{Y}$ is algebraically independent over K.

Corollary 6.43. *Let A be a finitely generated k-algebra that is an integral domain. Then* $\dim(A) = \operatorname{tr.deg}(\operatorname{Quot}(A)/k)$.

Proof. Let $k[x_1, \dots, x_d] \subseteq A$ be finite with algebraically independent $x_1, \dots, x_d$ as in Noether normalisation 6.5. By Corollary 6.34, we have $\dim(A) = d$.

Recall from Proposition 5.10 that if $B \subseteq C$ is integral and $S \subseteq B$ is a multiplicative subset, then $S^{-1}B \subseteq S^{-1}C$ is integral. The same holds for replacing *integral* by *finite* since taking scalar extensions are right-exact (tensor $B^{\oplus m} \twoheadrightarrow C$ with $S^{-1}B$ and use Remark 4.38).

Thus $\operatorname{Quot}(k[x_1, \dots, x_d]) \subseteq (k[x_1, \dots, x_d] \setminus \{0\})^{-1}A$ is finite. As the right-hand side is an integral domain and the left-hand side is a field, then, by Proposition 5.12, the right-hand side must be a field as well. The only field containing A and generated by A is $\operatorname{Quot}(A)$, so the right-hand side is $\operatorname{Quot}(A)$. In conclusion, $\operatorname{Quot}(A)/k(x_1, \dots, x_d)$ is a finite and hence algebraic field extension. So $(x_1, \dots, x_d)$ is a transcendence basis of $\operatorname{Quot}(A)/k$, and thus $\operatorname{tr.deg}(\operatorname{Quot}(A)/k) = d = \dim(A)$. □

6.7 Irreducible Components and Minimal Prime Ideals

Lect. 18
22.06.23

Recall: Let k be algebraically closed, and let $R_n \coloneqq k[X_1, \dots, X_n]$. If $Z \subseteq k^n$ is an algebraic set, then there exists an ideal $\mathfrak{a} \subseteq R_n$ such that $Z = Z(\mathfrak{a})$. Hilbert's Nullstellensatz 6.23 says that there is a bijection between algebraic sets and radical ideals via $Z \mapsto I(Z)$ and $Z(\mathfrak{a}) \mapsto \mathfrak{a}$.

Definition 6.44. Let k be an algebraically closed field. An algebraic set $Z \subseteq k^n$ is **irreducible** if $Z = Z_1 \cup Z_2$ implies $Z = Z_1$ or $Z = Z_2$ for any algebraic $Z_1, Z_2 \subseteq k^n$.

This has a striking similarity to the prime ideal property!

Proposition 6.45. *An algebraic set $Z \subseteq k^n$ is irreducible if and only if $I(Z) \subseteq k[X_1, \dots, X_n]$ is a prime ideal.*

Proof. Exercise 8.48. □

Proposition 6.46. *Suppose that $Z \subseteq k^n$ is an algebraic set. Then there are finitely many irreducible algebraic sets $Z_1, \dots, Z_n \subseteq k^n$ such that $Z = Z_1 \cup \dots \cup Z_r$.*

Proof. We show this by way of contradiction. This strategy is called **noetherian induction** since we use the fact that $k[X_1, \dots, X_n]$ is noetherian (Corollary 3.31).

Assume that Z cannot be written as such a finite union of irreducible algebraic sets. In particular, Z itself is not irreducible, i. e. there exists algebraic $Z_1, Z_2 \subseteq k^n$ such that $Z = Z_1 \cup Z_2$, but $Z \neq Z_1, Z_2$ and $\varnothing \neq Z_1, Z_2$ By assumption, one out of Z_1 or Z_2 cannot be written as a finite union of irreducible algebraic sets.

We can continue recursively to construct a strictly descending chain $Z \supset Z^{(1)} \supset Z^{(2)} \supset \cdots$ By Hilbert's Nullstellensatz 6.23, the chain $I(Z) \subset I(Z^{(1)}) \subset I(Z^{(2)}) \subset \cdots$ is an infinite strictly ascending chain of radical ideals. This contradicts the fact that $k[X_1, \dots, X_n]$ is noetherian. □

Corollary 6.47. *Let k be an algebraically closed field. Every radical ideal $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$ is a finite intersection of prime ideals.*

Proof. By Proposition 6.46, we can write $Z(\mathfrak{a}) = Z_1 \cup \dots \cup Z_r$ as a finite union of irreducible algebraic sets. Observe that $I(Z_1 \cup \dots \cup Z_r) = I(Z_1) \cap \dots \cap I(Z_r)$ (this is dual to Observation 6.15). Then Hilbert's Nullstellensatz 6.23 implies $\mathfrak{a} = I(Z(\mathfrak{a})) = I(Z_1) \cap \dots \cap I(Z_r)$. By Proposition 6.45, the $I(Z_i)$ are prime. □

Example 6.48. Consider the algebraic set (see Figure 6.5)

$$\begin{aligned} &Z(Y - X^3 + X) \cup Z(X - Y^2) \cup Z(Y, X - 3) \\ &\quad = Z((Y - X^3 + X)(X - Y^2)Y, (Y - X^3 + X)(X - Y^2)(X - 3)). \end{aligned}$$

This is a union of irreducible algebraic sets. For example, $Z(X - Y^2)$ cannot be decomposed because any proper algebraic subset of it must be a point.

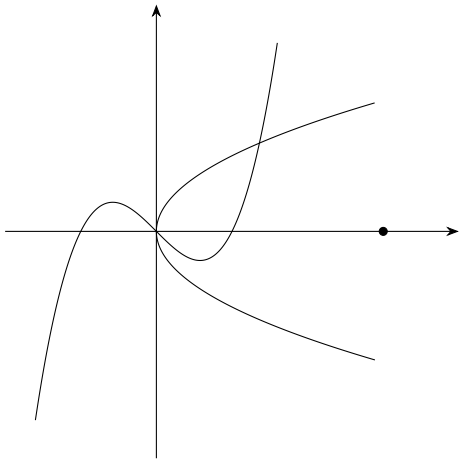


Figure 6.5: Algebraic set $Z(Y - X^3 + X) \cup Z(X - Y^2) \cup Z(Y, X - 3)$.

Definition 6.49. An **irreducible component** of an algebraic set $Z \subseteq k^n$ is an irreducible algebraic subset $Y \subseteq Z$ that is maximal in the following sense: If $Y' \subseteq Z$ is an irreducible algebraic subset with $Y \subseteq Y'$, then $Y = Y'$ already.

Proposition 6.50. *Let $Z \subseteq k^n$ be an algebraic set, and let $\mathcal{C}$ be the set of all irreducible components of Z. Then $\mathcal{C}$ is finite, and $Z = \bigcup_{Y \in \mathcal{C}} Y$.*

Proof. Let $Z = Z_1 \cup \dots \cup Z_r$ be any expression as a finite union of irreducible algebraic sets, see Proposition 6.46. W. l. o. g. we can assume that $Z_i \not\subseteq Z_j$ for all $i \neq j$; otherwise Z_j simply absorbs Z_i. If we show that $\mathcal{C} = \{Z_1, \dots, Z_r\}$, then we are done.

Let $Y \in \mathcal{C}$ be an irreducible component of Z. By De Morgan's laws, we have $Y = Y \cap Z = (Y \cap Z_1) \cup \dots \cup (Y \cap Z_r)$. But Y is irreducible, so $Y = Y \cap Z_i$ for some i, and thus $Y \subseteq Z_i$. Additionally, Y is maximally irreducible, and since Z_i is irreducible, we must have $Y = Z_i$.

Conversely, consider any Z_i. Assume that $Y' \subseteq Z$ is an irreducible algebraic set with $Z_i \subseteq Y'$. By the same argument as before, we have $Y' \subseteq Z_j$ for some j, and hence $Z_i \subseteq Z_j$. Then our assumption on the Z_i implies $i = j$, which gives $Z_i \subseteq Y' \subseteq Z_j = Z_i$, i. e. $Y' = Z_i$. Therefore Z_i is an irreducible component, and $Z_i \in \mathcal{C}$. □

Corollary 6.51. *Let k be an algebraically closed field, and let A be a finitely generated k-algebra. Then A has only finitely many minimal prime ideals.*

Proof. Recall that every prime ideal contains $\operatorname{nil}(A)$ (Proposition 2.22), hence we have an (inclusion preserving) bijection $\operatorname{Spec}(A) \cong \operatorname{Spec}(A/\operatorname{nil}(A))$. So w. l. o. g., assume that A is reduced (according to Proposition 1.23, $A/\operatorname{nil}(A)$ is reduced).

As A is finitely generated, we can chose any presentation $A \cong k[X_1, \dots, X_n]/\mathfrak{a}$. Since A is reduced, $\bar{f}^n = 0$ in $k[X_1, \dots, X_n]/\mathfrak{a}$ implies $\bar{f} = 0$, which is the same as saying that $f^n \in \mathfrak{a}$ implies $f \in \mathfrak{a}$. In other words, $\mathfrak{a} \subseteq k[X_1, \dots, X_n]$ is radical. Hence, by Hilbert's Nullstellensatz 6.23, there is an algebraic set $Z \subseteq k^n$ such that $\mathfrak{a} = I(Z)$.

Combining Example 2.14, Hilbert's Nullstellensatz 6.23 and Proposition 6.45 gives the bijections

$$\begin{aligned}\{\text{minimal prime ideals of } A\} &\leftrightarrow \{\text{minimal prime ideals of } k[X_1, \dots, X_n] \text{ containing } \mathfrak{a}\} \\ &\leftrightarrow \{\text{maximal irreducible algebraic subsets of } Z\} \\ &= \{\text{irreducible components of } Z\}.\end{aligned}$$

(Recall that applying I or Z inverts inclusion relationships.) The set of all irreducible components of Z is finite. □

Remark 6.52. The proof of Hilbert's Nullstellensatz 6.23 used the clever trick of localising a particular ring at a newly introduced variable. The above argument would be quite difficult to perform purely algebraically; Hilbert's Nullstellensatz 'black-boxes' this so that we can manipulate geometric sets on a set-theoretic level. Thus this geometric approach is not only elegant, but very practical.

6.8 Krull's Principal Ideal Theorem

Remark 6.53. (From me.) A note on the dimension that is due for some time. Let $R_n := k[X_1, \dots, X_n]$ with k an algebraically closed field. Let $\mathfrak{a} \subseteq R_n$ be any ideal.

A generalised notion of dimension of vector spaces is the following topological definition: Over all proper chains $Z(\mathfrak{a}_0) \subset Z(\mathfrak{a}_1) \subset \cdots \subset Z(\mathfrak{a}_d) \subseteq Z(\mathfrak{a})$ of irreducible algebraic sets, the *dimension* of $Z(\mathfrak{a})$ is the supremum over d. This intuitively coincides with the notion of k-dimension in vector spaces. If $(b_i)_{i \in I}$ is a basis of a vector space, then the dimension of this vector space is the length of the chain $\{0\} \subset \operatorname{span}_k(b_{i_1}) \subset \operatorname{span}_k(b_{i_1}, b_{i_2}) \subset \cdots \subset \operatorname{span}_k(b_i, i \in I)$.

By Hilbert's Nullstellensatz 6.23 and Proposition 6.45, each maximal length chain of irreducible algebraic sets in $Z(\mathfrak{a})$ corresponds to maximal length chain of prime ideals $\mathfrak{a} \subseteq \mathfrak{p}_d \subset \cdots \subset \mathfrak{p}_0$ in R_n. Or expressed differently, the dimension of $Z(\mathfrak{a})$ is $\dim(R_n/\mathfrak{a})$.

If we consider $k = \mathbb{C}$, then one can show that in many cases, the dimension of $Z(\mathfrak{a})$ in the above sense is its $\mathbb{C}$-dimension as a submanifold in $\mathbb{C}^n$.

Lemma 6.54. *Let A be a finitely generated k-algebra over a field k. Suppose that A has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subset A$. Then*

$$\operatorname{Spec}(A) = \bigcup_{i=1}^{r} \operatorname{Spec}(A/\mathfrak{p}_i) \qquad \text{and} \qquad \dim(A) = \max_{i=1,\dots,r} \dim(A/\mathfrak{p}_i).$$

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(A)$ be arbitrary. Applying the proof of Exercise 8.12 to the set of all prime ideals in $\mathfrak{p}$ shows that $\mathfrak{p}$ contains a minimal prime ideal. Hence $\mathfrak{p}$ is contained in $\operatorname{Spec}(A/\mathfrak{p}_i)$ for some i, which shows the first equality.

For the second equality, observe that by the above fact, every ascending chain of prime ideals of maximal length starts with a minimal prime ideal. Hence this chain is contained in $\operatorname{Spec}(A/\mathfrak{p}_i)$ for some i. □

We can improve Corollary 6.36 by using minimal prime ideals or irreducible components.

Proposition 6.55. *Put $R_n := k[X_1, \dots, X_n]$ with an algebraically closed field k. Let $f \in R_n \setminus k$ be a non-constant polynomial. Then $R_n/(f)$ is **purely of dimension** $n-1$, i. e. for every minimal prime ideal $\mathfrak{p} \subseteq R_n/(f)$, we have $\dim((R_n/(f))/\mathfrak{p}) = n-1$ (or every irreducible component is of dimension $n-1$).*

Proof. R_n is a unique factorisation domain, so let $\prod_{i=1}^{r} p_i^{e_i}$ be the unique prime factorisation of f up to units. Then the minimal prime ideals of $R_n/(f)$ are $(p_1), \dots, (p_r)$. (Let $\mathfrak{q} \in \operatorname{Spec}(R_n)$ with $(f) \subset \mathfrak{q} \subseteq p_i R_n$. Then $p_i \mid g$ for all $g \in \mathfrak{q}$. Since $\mathfrak{q}$ is prime and $f \in \mathfrak{q}$, we have $p_i \in \mathfrak{q}$, i. e. $p_i R_n \subseteq \mathfrak{q}$.) Then $(R_n/(f))/(p_i) \cong R_n/p_i R_n$, which is of Krull dimension $n-1$ according to Corollary 6.36. □

Example 6.56. Consider the algebraic set $Z = Z(X_3) \cup Z(X_1, X_2) \subseteq k^3$ (Figure 6.6). Then we cannot write $Z = Z(f)$ for some $f \in k[X_1, X_2, X_3]$; reason being that the irreducible component $Z(X_1, X_2)$ has dimension 1.

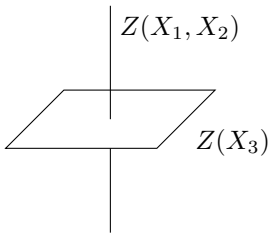


Figure 6.6: Visualisation of Z in Example 6.56.

6.9 First form of Krull's Principal Ideal Theorem

Lect. 19
26.06.23

Theorem 6.57. *Let A be a finitely generated k-algebra that is also an integral domain. Let $0 \neq f \in A \setminus A^\times$. Then $\dim(A/(f)) = \dim(A) - 1$.*

Proof. We have $\dim(A/(f)) \leq \dim(A) - 1$ already: By taking the preimage, any chain of prime ideals $\bar{\mathfrak{p}}_0 \subset \cdots \subset \bar{\mathfrak{p}}_d$ in $A/(f)$ gives a chain of prime ideals $(0) \subset \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d$ in A. (0) is prime since A is an integral domain, and $\mathfrak{p}_0 \neq (0)$ since $f \neq 0$.

So for the rest of the proof, we will show the converse inequality. Let $R_n \coloneqq k[X_1, \ldots, X_n] \subseteq A$ be finite with algebraically independent $X_1, \ldots, X_n \in A$ (these are not variables, but elements of A) as in Noether normalisation 6.5. By Corollary 6.34, we know that $\dim(A) = n$.

Let us regard f as a $\mathrm{Quot}(R_n)$-linear map on the vector space $\mathrm{Quot}(A)$ over $\mathrm{Quot}(R_n) = k(X_1, \ldots, X_n)$ by left-multiplication. Let $h(T) \coloneqq \mathrm{char}(f; T) \in k(X_1, \ldots, X_n)[T]$ be the characteristic polynomial of the map f. The following sentence anticipates statements from the upcoming section on number theory: R_n is a unique factorisation domain, so by Proposition 7.4, it is normal, and Proposition 7.5 implies that $h(T) \in R_n[T]$. Therefore we can write $h(T) = T^e + h_{e-1}T^{e-1} + \cdots + h_0$ with $h_0, \ldots, h_{e-1} \in R_n$.

Firstly, we see how we might finish the proof. Consider any prime ideal $(0) \neq \mathfrak{p} \subset R_n$ of height 1. Since R_n is a unique factorisation domain, we have $\mathfrak{p} = (\pi)$ for some prime element $\pi \in R_n$. We denote

$$\varphi \colon R_n \hookrightarrow A \twoheadrightarrow A/(f).$$

Assume for a moment that $\mathfrak{p} \in \mathrm{im}(\mathrm{Spec}(\varphi))$, say $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}/(f))$ for some $(f) \subseteq \mathfrak{q} \in \mathrm{Spec}(A)$. Observe that in this case, $\mathfrak{p} \subseteq \mathfrak{q}$. Then $R_n/\mathfrak{p} \subseteq A/\mathfrak{q} \cong (A/(f))/(\mathfrak{q}/(f))$ is a finite ring extension, so by Corollary 5.17, we have $\dim(R_n/\mathfrak{p}) = \dim(A/\mathfrak{q})$. Moreover, by Corollary 6.36, $\dim(R_n/(\pi)) = n - 1$. Therefore

$$\dim(A/(f)) \geq \dim((A/(f))/(\mathfrak{q}/(f))) = \dim(A/\mathfrak{q}) = \dim(R_n/(\pi)) = n - 1.$$

Thus the proof is complete if we find a height 1 prime ideal $\mathfrak{p} = (\pi) \in \mathrm{im}(\mathrm{Spec}(\varphi))$.

Next, given $\mathfrak{p} = (\pi) \subset R_n$, we consider the localisations $R_{n,\mathfrak{p}}$ and $A_\mathfrak{p} \coloneqq (R_n \setminus \mathfrak{p})^{-1}A$. Our intermediate goal is to determine $\mathrm{Spec}(R_{n,\mathfrak{p}})$ and $\mathrm{Spec}(A_\mathfrak{p})$. Observe that $R_{n,\mathfrak{p}} \subseteq A_\mathfrak{p}$ is a finite ring extension (tensor $R_n^{\oplus m} \twoheadrightarrow A$ with $R_{n,\mathfrak{p}}$ and use Remark 4.38). Also recall $\mathrm{Spec}(R_{n,\mathfrak{p}}) = \{\mathfrak{q} \in \mathrm{Spec}(R_n) \mid \mathfrak{q} \subseteq \mathfrak{p}\}$. As $\mathfrak{p}$ is a prime ideal of height 1, we have $\mathrm{Spec}(R_{n,\mathfrak{p}}) = \{(0), (\pi)\}$. By Exercise 8.11, $R_{n,\mathfrak{p}}$ is a principal ideal domain. Similarly, $\mathrm{Spec}(A_\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \cap R_n \subseteq \mathfrak{p}\}$. Note that $A_\mathfrak{p}$ is again an integral domain. Thus, according to Exercise 8.43, $\mathrm{Spec}(A_\mathfrak{p}) \to \mathrm{Spec}(R_{n,\mathfrak{p}})$ has finite fibres, so there are only finitely many $\mathfrak{q} \in \mathrm{Spec}(A)$ such that $\mathfrak{q} \cap R_n = \mathfrak{p}$, say $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\} \subset \mathrm{Spec}(A)$. Thus $\mathrm{Spec}(A_\mathfrak{p}) = \{(0), \mathfrak{q}_1 A_\mathfrak{p}, \ldots, \mathfrak{q}_r A_\mathfrak{p}\}$, where the $\mathfrak{q}_i A_\mathfrak{p}$ are maximal by Corollary 5.13.

Now, we show that $\det_{R_{n,\mathfrak{p}}}(f \mid A_\mathfrak{p}) = h_0$. Recall that $R_{n,\mathfrak{p}}$ is a principal ideal domain, and that $A_\mathfrak{p}$ is a finitely generated $R_{n,\mathfrak{p}}$-module. Since $A_\mathfrak{p}$ is an integral domain, it is torsion-free as a module, so by the structure theorem 3.52, $A_\mathfrak{p}$ is a free $R_{n,\mathfrak{p}}$-module. As a consequence,

$$\det_{R_{n,\mathfrak{p}}}(f \mid A_\mathfrak{p}) = \det_{k(X_1,\ldots,X_n)}(f \mid \mathrm{Quot}(A)) = h_0 \tag{6.58}$$

(the determinant of f is the constant term of the characteristic polynomial $h(T)$, see linear algebra; this also holds for modules over integral domains). In more detail: If $A_\mathfrak{p} = \bigoplus_{i=1}^e R_{n,\mathfrak{p}} x_i$ as a free $R_{n,\mathfrak{p}}$-module, then

$$\mathrm{Quot}(A) = A[((A \setminus \mathfrak{p}) \cup (\mathfrak{p} \setminus \{0\}))^{-1}] = A_\mathfrak{p}[\pi^{-1}] = \bigoplus_{i=1}^e R_{n,\mathfrak{p}}[\pi^{-1}]x_i = \bigoplus_{i=1}^e \mathrm{Quot}(R_n)x_i$$

is a $\mathrm{Quot}(R_n) = k(X_1, \dots, X_n)$-vector space. So we can use the same basis for both $A_\mathfrak{p}$ and $\mathrm{Quot}(A)$, hence $f \in M_e(R_{n,\mathfrak{p}})$ is the same in $A_\mathfrak{p}$ and in $\mathrm{Quot}(A)$ via the inclusion $A_\mathfrak{p} \hookrightarrow \mathrm{Quot}(A)$ (see Example 2.49). Thus the determinants of f are also the same, and we obtain (6.58).

After that, we characterise when $\mathfrak{p} = (\pi) \in \mathrm{im}(\mathrm{Spec}(\varphi))$. We have $\mathfrak{p} = (\pi) \in \mathrm{im}(\mathrm{Spec}(\varphi))$ if and only if there is some i such that $\mathfrak{q}_i \in \mathrm{Spec}(A/(f))$ since, in this case, $\varphi^{-1}(\mathfrak{q}_i) = \mathfrak{q}_i \cap R_n = \mathfrak{p}$. Saying that there is some i such that $\mathfrak{q}_i \in \mathrm{Spec}(A/(f))$ is the same as saying that there is some i such that $f \in \mathfrak{q}_i$. This in turn is equivalent to $f \notin A_\mathfrak{p}^\times$ (since $f \in \mathfrak{q}_i A_\mathfrak{p} \neq A_\mathfrak{p}$ for some i, we must have $f \notin A_\mathfrak{p}^\times$; if $f \notin A_\mathfrak{p}^\times$, then there is some maximal $\mathfrak{q}_i A_\mathfrak{p}$ containing f). Combining (6.58) with Lemma 3.35, $f \notin A_\mathfrak{p}^\times$ is equivalent to $h_0 = \det_{R_{n,\mathfrak{p}}}(f \mid A_\mathfrak{p}) \notin R_{n,\mathfrak{p}}^\times = R_{n,\mathfrak{p}} \setminus (\pi R_{n,\mathfrak{p}})$ (recall that $R_{n,\mathfrak{p}}$ is local), i. e. $\pi \mid h_0$.

Now the final step. By assumption, $f \notin A^\times$, so by Lemma 3.35, $h_0 \notin R_n^\times$. Because R_n is a unique factorisation domain, there must exist some prime element $\pi \in R_n$ such that $\pi \mid h_0$, which implies that the height 1 prime ideal $\mathfrak{p} = (\pi)$ lies in $\mathrm{im}(\mathrm{Spec}(\varphi))$, as desired. □

The proof mainly used two tricks: Exhausting the fact that R_n is a unique factorisation domain and passing the determinant of f to the localised vector space.

6.10 Localisation and Dimension

In order to prove the stronger form of Krull's principal ideal theorem, we need to see some properties.

Proposition 6.59. *Let k be an algebraically closed field, and let A be a finitely generated k-algebra as well as an integral domain. Let $0 \neq g \in A$. Then $\dim(A[g^{-1}]) = \dim(A)$.*

Proof. $\dim(A[g^{-1}]) \leq \dim(A)$ is clear since

$$\mathrm{Spec}(A[g^{-1}]) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid g \notin \mathfrak{p}\} \subseteq \mathrm{Spec}(A).$$

We need to show $\dim(A[g^{-1}]) \geq \dim(A)$.

Let $R_n \coloneqq k[X_1, \dots, X_n] \subseteq A$ be finite as in Noether normalisation 6.5 (again, $X_1, \dots, X_n \in A$ are not variables, but elements). Then g is integral over R_n, say $h(g) = 0$ for some $h(T) = T^e + h_{e-1}T^{e-1} + \cdots + h_0 \in R_n[T]$. As A is an integral domain and $g \neq 0$, we may assume that $h_0 \neq 0$; otherwise we divide by a sufficiently high power of T.

If we regard $h_0 \in R_n$ as a polynomial in variables $X_1, \dots, X_n$, then there necessarily exists a point $x = (x_1, \dots, x_n) \in k^n$ such that $h_0(x) \neq 0$, i. e. $h_0(x) \in k^\times$. Let $\mathfrak{m} = (X_1 - x_1, \dots, X_n - x_n) \subset R_n$ be the corresponding maximal ideal by Corollary 6.9 (here, we used that k is algebraically closed). Then $h_0 \bmod \mathfrak{m} \neq 0$ in the field $R_n/\mathfrak{m}$, whence $(g \bmod \mathfrak{m}) \in (A/\mathfrak{m}A)^\times$, namely

$$g^{-1} \bmod \mathfrak{m} = -(h_0 \bmod \mathfrak{m})^{-1}(g^{e-1} + h_{e-1}g^{e-2} + \cdots + h_1 \bmod \mathfrak{m}).$$

By the going-up theorem 5.16, there exists a proper chain $(0) \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ of prime ideals in A that lies above the chain of prime ideals $(0) \subset (X_1 - x_1) \subset (X_1 - x_1, X_2 - x_2) \subset \cdots \subset \mathfrak{m}$ in R_n (start with $(0) \subset A$, which is prime since A is an integral domain, and then extend). Note that $(X_1 - x_1, \dots, X_r - x_r)$ for all $r = 1, \dots, n$ are prime since $R_n/(X_1 - x_1, \dots, X_r - x_r) \cong k[X_{r+1}, \dots, X_n]$ is still an integral domain.

Since $(g \bmod \mathfrak{m}) \in (A/\mathfrak{m}A)^\times$, we have $(g \bmod \mathfrak{m}) \notin \mathfrak{q}/\mathfrak{m}$ for all maximal ideals $\mathfrak{q} \subset A$ above $\mathfrak{m}$, and in particular, $g \notin \mathfrak{q}_n$ (Corollary 2.19). Hence $(0) \subset \mathfrak{q}_1 \cdots \subset \mathfrak{q}_n$ lies in $\mathrm{Spec}(A[g^{-1}])$, i. e. $\dim(A[g^{-1}]) \geq n = \dim(A)$ by Corollary 6.34. □

Remark 6.60. Proposition 6.59 essentially says that a finitely generated k-algebra that is an integral domain has so many maximal ideals that localising at one element does not change the dimension.

On the contrary, consider the k-algebra $A = k[X]_{(X)}$, which is definitely not finitely generated over k. A as a ring is local w. r. t. (X) with $\dim(A) = 1$. But $\dim(A[X^{-1}]) = \dim(k(X)) = 0$ since $k(X) = k[X]_{(X)}[X^{-1}]$ is a field.

6.11 Localisation and Irreducible Components

Lemma 6.61. *Let A be a ring with finitely many distinct minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subset A$. Then there exists some $g \in (\mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r) \setminus \mathfrak{p}_1$. For any such g, we have*

$$\operatorname{Spec}(A[g^{-1}]) \subseteq \operatorname{Spec}(A/\mathfrak{p}_1) \subseteq \operatorname{Spec}(A).$$

This implies

$$\operatorname{Spec}(A[g^{-1}]) = \operatorname{Spec}((A/\mathfrak{p}_1)[g^{-1}]).$$

Proof. Since the $\mathfrak{p}_i$ are minimal and pairwise different, we have $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$. Hence for all $i = 1, \dots, r$, we can pick an $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_1$. Then $g := (x_2 \cdots x_r) \in (\mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r) \setminus \mathfrak{p}_1$ by the prime ideal property.

Furthermore due to Proposition 2.55 and Example 2.14,

$$\begin{aligned}\operatorname{Spec}(A[g^{-1}]) &= \{\mathfrak{p} \in \operatorname{Spec}(A) \mid g \notin \mathfrak{p}\} \subseteq \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p}_2, \dots, \mathfrak{p}_r \not\subseteq \mathfrak{p}\} \\ &\subseteq \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p}_1 \subseteq \mathfrak{p}\} = \operatorname{Spec}(A/\mathfrak{p}_1) \subseteq \operatorname{Spec}(A).\end{aligned}$$

For the first inclusion, we used $g \in \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r$. For the second inclusion, we used that each prime ideal contains some minimal prime, see the proof of Lemma 6.54.

For the second statement, observe that

$$\operatorname{Spec}(A[g^{-1}]) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid g \notin \mathfrak{p}, \mathfrak{p}_1 \subseteq \mathfrak{p}\} = \operatorname{Spec}((A/\mathfrak{p}_1)[g^{-1}]). \qquad \square$$

Example 6.62. Consider $k[X,Y]/(XY)$ and the prime ideals $\mathfrak{p}_1 = (X)$ and $\mathfrak{p}_2 = (Y)$ (we have $(XY) \subseteq (X), (Y)$). Pick for example $g = Yf(Y) \in (Y) \setminus (X)$ with any $0 \neq f(Y) \in k[Y]$. Then

$$k[X,Y,T]/(XY, Yf(Y)T - 1) \cong k[Y, Y^{-1}, f(Y)^{-1}], \qquad X \mapsto 0, \quad Y \mapsto Y, \quad T \mapsto Y^{-1}f(Y)^{-1}.$$

The reason is that

$$X = f(Y)T \cdot XY - X(Yf(Y)T - 1) \in (XY, Yf(Y)T - 1).$$

Now consider $\varphi\colon k[X,Y]/(XY) \to k[Y, Y^{-1}, f(Y)^{-1}]$. Then $\ker(\varphi) = (X) = \mathfrak{p}_1$. Hence $(X) \subseteq \varphi^{-1}(\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Spec}(k[Y, Y^{-1}, f(Y)^{-1}])$. More specifically, the map on spectra is

$$\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(k[Y, Y^{-1}, f(Y)^{-1}]) \to \operatorname{Spec}(k[X,Y]/(XY)), \qquad (Y - y) \mapsto (X, Y - y), \quad (0) \mapsto (X)$$

with $y \neq 0 \neq f(y)$.

6.12 Second Form of Krull's Principal Ideal Theorem

Now the stronger version.

Theorem 6.63 (Krull's principal ideal theorem). *Let k be algebraically closed, and let A be a finitely generated k-algebra as well as an integral domain. Let $0 \neq f \in A \setminus A^\times$. Then $B := A/(f)$ is **purely of dimension** $\dim(A) - 1$, i. e. for all minimal prime ideals $\mathfrak{p} \subseteq B$, we have $\dim(B/\mathfrak{p}) = \dim(A) - 1$.*

Proof. The idea is to localise in order to reduce this theorem to the weaker version.

Given a minimal prime ideal $\mathfrak{p} \subseteq B$, we apply Lemma 6.61 to find

$$g \in \left(\bigcap_{\substack{\text{min. } \mathfrak{q} \in \operatorname{Spec}(B) \\ \mathfrak{q} \neq \mathfrak{p}}} \mathfrak{q} \right) \setminus \mathfrak{p}$$

(by Corollary 6.51, there are only finitely many minimal prime ideals). Furthermore, we have $\operatorname{Spec}(B[g^{-1}]) = \operatorname{Spec}((B/\mathfrak{p})[g^{-1}]) \subseteq \operatorname{Spec}(B/\mathfrak{p})$ by Lemma 6.61, which implies $\dim(B[g^{-1}]) = \dim((B/\mathfrak{p})[g^{-1}])$. Additionally, $\dim((B/\mathfrak{p})[g^{-1}]) = \dim(B/\mathfrak{p})$ by Proposition 6.59 (note that $B/\mathfrak{p}$ is an integral domain and a finitely generated k-algebra). Or aim is to show that $\dim(B/\mathfrak{p}) = \dim(B[g^{-1}]) = \dim(A) - 1$.

Now Lemma 2.54 says that $B[g^{-1}] = (A/(f))[g^{-1}] \cong (A[\tilde{g}^{-1}])/(f)$, where $\tilde{g} \in A$ is a lift of $g \in B$. Since A is an integral domain and a finitely generated k-algebra, $A[\tilde{g}^{-1}]$ is so as well. Also $f \notin A[\tilde{g}^{-1}]^\times$ because $(A[\tilde{g}^{-1}])/(f) \cong B[g^{-1}] \neq 0$ (we have $B \neq 0$ since $f \notin A^\times$, and g is not a zero divisor since $g \notin \mathfrak{p}$ and thus $\tilde{g} \notin (f)$). Thus we can apply Theorem 6.57 to obtain $\dim((A[\tilde{g}^{-1}])/(f)) = \dim(A[\tilde{g}^{-1}]) - 1$. Finally, Proposition 6.59 implies $\dim(A[\tilde{g}^{-1}]) = \dim(A)$, whence $\dim(B[g^{-1}]) = \dim((A[\tilde{g}^{-1}])/(f)) = \dim(A) - 1$. $\square$

Remark 6.64. Some final words: Krull's principal ideal theorem and related results can be actually generalised to any noetherian ring, not just polynomial rings over algebraically closed fields. The reason why we only considered polynomial rings is that we used Hilbert's Nullstellensatz 6.23 to prove these. The general statements use *dimension theory*, which takes some time to develop. See [AtMac, ch. 11].

The generalisations are in particular the following. Let A be any noetherian ring. Then the following hold:

(i) A has only finitely many minimal prime ideals.

(ii) If $f \in A \setminus A^\times$ is not a zero divisor, then $\dim(A/(f)) = \dim(A) - 1$.

(iii) Moreover, by induction, one obtains $\dim(A/(f_1, \dots, f_m)) \geq \dim(A) - m$.

7 Basics in Algebraic Number Theory

Lect. 20
29.06.23

We will generalise our findings about prime factorisations to *Dedekind domains*.

Problem 7.1. We have seen some examples early on in this course, e. g. $\mathbb{Z}[\mathrm{i}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$. We have shown that these are principal ideal domains (Proposition 1.55), in particular unique factorisation domains (Corollary 1.56). As an application, we considered the solutions for $x^2 + y^2 = n$ (Theorem 2.5), $x^2 + 2y^2 = n$ (Remark 2.8, although we just stated the result), and $x^2 + xy + y^2 = n$ (Exercise 8.8) with $(x, y) \in \mathbb{Z}^2$. We have also seen that $\mathbb{Z}[\sqrt{-3}]$ (Exercise 8.10) and $\mathbb{Z}[\sqrt{-5}]$ (Example 2.53) are not principal ideal domains.

This raises the following questions:

(i) The rings $\mathbb{Z}[\mathrm{i}]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$ are clearly related to the field extensions $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\zeta_3)$ over $\mathbb{Q}$. How can we define these ring in general for finite field extensions $K/\mathbb{Q}$?

We will see that these rings are *rings of algebraic integers* $\mathcal{O}_K \subseteq K$ of K.

(ii) In which sense does the principal ideal domain property fail for $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\sqrt{-5}]$?

For $\mathbb{Z}[\sqrt{-3}]$, the reason is that it is not *integrally closed*. For $\mathbb{Z}[\sqrt{-5}]$, the answer is more intricate. The answer is that this ring has non-trivial *class groups*.

(iii) What about prime factorisation in $\mathcal{O}_K$?

We will see that prime factorisations exist, but only in terms of prime ideals.

7.1 Integral Closure

Recall: Let $A \to B$ be an A-algebra. Then the *integral closure* $\overline{A}^B$ of A in B is the set of all integral $b \in B$ over A. We know that $\overline{\overline{A}^B}^B = \overline{A}^B$.

Definition 7.2. Let $A \subseteq B$ be a ring extension. We call A **integrally closed** in B if $A = \overline{A}^B$.

Definition 7.3. Let A be an integral domain, and let L/K be a finite field extension with $K := \mathrm{Quot}(A)$. We define:

(i) A is **normal** if $A = \overline{A}^K$, i. e. A is integrally closed in $K = \mathrm{Quot}(A)$.

(ii) The integral closure $\overline{A}^L$ of A in L is the set of all integral $x \in L$ over A via $A \subseteq L$.

Proposition 7.4. *Every unique factorisation domain is normal.*

Proof. Let A be a unique factorisation domain. Suppose $\frac{a}{s} \in \mathrm{Quot}(A)$ is integral over A, i. e. we have an integral dependence relation $(\frac{a}{s})^n + b_{n+1}(\frac{a}{s})^{n-1} + \dots + b_0 = 0$ with $b_i \in A$. Multiplying with s^n yields $a^n + sb_{n-1}a^{n-1} + \dots + s^n b_0 = 0$. Since A is a unique factorisation domain, we may demand that $\gcd(a, s) = 1$; otherwise we factor out $\gcd(a, s)^n \neq 0$, and the remaining relation must be 0. Then the relation shows that if a prime element $\pi \in A$ divides s, then $\pi \mid a$. By the assumption $\gcd(a, s) = 1$, no such π can exists, so necessarily $s \in A^\times$, and thus $\frac{a}{s} \in A$. □

Proposition 7.5. *Let A be a normal integral domain, and let L/K be a finite field extension with $K \coloneqq \mathrm{Quot}(A)$. Then $x \in L$ lies in $\overline{A}^L$ if and only if $\mathrm{char}_{L/K}(x,T) \in A[T]$ if and only if $\min_{L/K}(x,T) \in A[T]$.*

Here $\mathrm{char}_{L/K}(x,T)$ and $\min_{L/K}(x,T)$ are the characteristic and minimal polynomial of x over K, where we view x as the K-linear map $x\colon L \to L$, $a \mapsto ax$ on the K-vector space L by left-multiplication.

Remark 7.6. (From me.) Actually a fact that we have not shown in the introduction to algebra: Let L/K be a finite field extension, and let $x \in L$. It is true that $\mathrm{char}_{L/K}(x,T) = \min_{L/K}(x,T)^{[L:K(x)]}$.

Proof: We know that $\{1, x, \dots, x^{[K(x):K]-1}\}$ is a K-basis of $K(x)/K$, and let $B_1 \coloneqq \{y_1, \dots, y_{[L:K(x)]}\}$ be a $K(x)$-basis of $L/K(x)$. Then for the tower of fields $K \subseteq K(x) \subseteq L$, we have $[L:K] = [L:K(x)] \cdot [K(x):K]$, and $B_2 \coloneqq \{x^i y_j \text{ for all } i,j\}$ is a K-basis of L/K. Observe that $L = \bigoplus_{j=1}^{[L:K(x)]} y_j K(x)$ as K-vector spaces.

Next we consider the K-linear map $x\colon L \to L$. Note that we can restrict x onto $K(x)/K$. In this case, $\mathrm{char}_{K(x)/K}(x,T) = \min_{K(x)/K}(x,T)$ since $\min(x,T) \mid \mathrm{char}(x,T)$ and $\deg(\mathrm{char}(x|_{K(x)},T)) = [K(x):K] = \deg(\min(x|_{K(x)},T))$.

Now we observe that the matrix presentation of $x \in M_{[L:K]}(K)$ over B_2 is actually a block matrix of $[L:K(x)]$ many identical blocks, which are the matrix presentation of $x|_{K(x)} \in M_{[K(x):K]}(K)$ over B_1. The reason is the decomposition of L into a direct sum of isomorphic K-vector subspaces (recall that similar (i. e. conjugate) matrices have the same determinant and thus minimal polynomial). Hence the characteristic polynomial of $x \in M_{[L:K]}(x,T)$ is $\mathrm{char}_{L/K}(x,T) = \min_{K(x)/K}(x,T)^{[L:K(x)]}$. Thus we have $\min_{K(x)/K}(x,T) = \min_{L/K}(x,T)$.

Proof. By Remark 7.6, $\min_{L/K}(x,T) \in A[T]$ implies $\mathrm{char}_{L/K}(x,T) = \min_{L/K}(x,T)^{[L:K(x)]} \in A[T]$. By Cayley-Hamilton 8.19, we have $\mathrm{char}_{L/K}(x,x) = 0$, so if $\mathrm{char}_{L/K}(x,T) \in A[T]$, then x is integral over A, i. e. $x \in \overline{A}^L$. So there is only one last implication to show.

Let $x \in \overline{A}^L$. Pick any algebraic closure $L \subseteq \overline{K}$, where $r \leq [L:K]$. Let $x_1 = \mathrm{id}(x)$, $x_2 = \varphi_2(x)$, …, $x_r = \varphi_r(x)$ be the conjugates of x under $\mathrm{Aut}(\overline{K}/K)$. (The *conjugates* of x are all roots of $\min_{L/K}(x,T)$ in $\overline{K}$. We know from the introduction to algebra that for each root x_i, there is a field homomorphism $\varphi_i'\colon K(x) \to \overline{K}$ fixing K with $\varphi_i'(x) = x_i$, see [Sch, Thm. 6.4]. After that, we can extend this to a field automorphism $\varphi_i\colon \overline{K} \to \overline{K}$.) Observe that if $f(x) = 0$ for some $f \in A[T]$, then $f(x_i) = f(\varphi_i(x)) = \varphi_i(f(x)) = 0$ (φ_i also fixes $A \subseteq K$), so all $x_1, \dots, x_r$ are integral over A. By Corollary 5.8, $A \subseteq A[x_1, \dots, x_n]$ is integral.

We have $\min_{L/K}(x,T) = (\prod_{i=1}^r (T - x_i))^e$ in $\overline{K}[T]$, where $e = 1$ if $K(x)/K$ is separable, and $e = p^k$ else, where $p = \mathrm{char}(K)$ is the characteristic of K (in the latter case, there is a separable $f \in K[T]$ such that $\min_{L/K}(x,T) = f(T^{p^k})$, see [Sch, Thm. 6.21]; now use the Frobenius endomorphism for $T^{p^k} - x_i^{p^k} = (T - x_i)^{p^k}$, see [Sch, Lem. 6.18]). Thus all coefficients of $\min_{L/K}(x,T)$ are sums of products of the x_i, and thus the coefficients are integral over A. By assumption, A is normal, so $\min_{L/K}(x,T) \in \overline{A}^K[T] = A[T]$. □

Example 7.7. The ring $\mathbb{Z}[\sqrt{-3}]$ is not normal since $\frac{1}{2}(1+\sqrt{-3}) \notin \mathbb{Z}[\sqrt{-3}]$ is integral over $\mathbb{Z}[\sqrt{-3}]$, namely via $T^3 + 1$. Therefore, by Proposition 7.4, $\mathbb{Z}[\sqrt{-3}]$ is not a unique factorisation domain and thus not a principal ideal domain.

Definition 7.8. Let $K/\mathbb{Q}$ be a finite field extension, which we call an **(algebraic) number field**. We define

$$\mathcal{O}_K \coloneqq \overline{\mathbb{Z}}^K = \{x \in K \mid \mathrm{char}_{K/\mathbb{Q}}(x,T) \in \mathbb{Z}[T]\}.$$

to be the **ring of (algebraic) integers** in K.

Definition 7.9. Let L/K be a finite field extension. Then we define the **norm**, **trace** and **characteristic polynomial** to be

$$\begin{aligned} N_{L/K}\colon L^\times \to K^\times, &\qquad a \mapsto \det_K(a\colon L \to L), \\ \mathrm{tr}_{L/K}\colon L \to K, &\qquad a \mapsto \mathrm{tr}_K(a\colon L \to L), \\ \mathrm{char}_{L/K}(a,T) \coloneqq \mathrm{char}_K(a\colon L \to L, T) &\in K[T], \end{aligned}$$

where a acts K-linearly on L by left-multiplication.

Proposition 7.10. *Let $D \in \mathbb{Z}$ be square-free, i. e. D is not divisible by any square number, and let $K \coloneqq \mathbb{Q}(\sqrt{D})$. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \equiv 2,3 \mod (4), \\ \mathbb{Z}\left[\dfrac{1+\sqrt{D}}{2}\right], & \text{if } D \equiv 1 \mod (4). \end{cases}$$

Proof. Suppose $a + b\sqrt{D} \in \mathcal{O}_K$ with $a, b \in \mathbb{Q}$. Then

$$a + b\sqrt{D} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} \in M_2(\mathbb{Q})$$

w. r. t. the $\mathbb{Q}$-basis $(1, \sqrt{D})$ of $K/\mathbb{Q}$. Recall from linear algebra that the constant coefficient of $\operatorname{char}_{K/\mathbb{Q}}(x, T)$ is $\det_K(x)$, and the coefficient of second highest degree (the coefficient next to the leading coefficient 1) is $\operatorname{tr}_K(x)$. Observe that $\det_K(x)$ and $\operatorname{tr}_K(x)$ determine $\operatorname{char}_{K/\mathbb{Q}}(x, T)$ completely since the characteristic polynomial is of degree 2. Thus $\operatorname{char}_{K/\mathbb{Q}}(x, T) \in \mathbb{Z}[T]$ if and only if $\operatorname{tr}(a + b\sqrt{D}) = 2a \in \mathbb{Z}$ and $N(a + b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Z}$.

There are two cases for a according to the trace equation. If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$ by the norm equation since D is square-free (D cannot cancel the denominator of b^2 completely, hence the denominator of b^2 is 1). Otherwise, a is a completely reduced proper fraction of the form $a = \frac{2k+1}{2}$ for some $k \in \mathbb{Z}$. Then by the norm equation, $b = \frac{2l+1}{2}$ for some $l \in \mathbb{Z}$ since D is square-free (same argument as before, which becomes the most clear if we consider $(2a)^2 - (2b)^2 D \in \mathbb{Z}$). This yields

$$N(a + b\sqrt{D}) = \frac{4k^2 + 4k + 1 - (4l^2 + 4l + 1)D}{4} \in \mathbb{Z} + \frac{1 - D}{4}\mathbb{Z},$$

which lies in $\mathbb{Z}$ if and only if $D \equiv 1 \mod (4)$. In this case,

$$a + b\sqrt{D} = (k - l) + (2l + 1)\frac{1 + \sqrt{D}}{2} \in \mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right]. \qquad \square$$

Example 7.11. Some important examples in number theory.

(i) If $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ (we will not prove this).

(ii) For cyclotomic fields, if $K = \mathbb{Q}(\zeta_n)$, where $\zeta_n \in \mathbb{C}$ is an nth root of unity, then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

Example 7.12. A geometric example. Let $A = k[x, y]/(y^2 - x^3)$, and let $K \coloneqq \operatorname{Quot}(A)$.

We show that $x \nmid y$ in A. If $x \mid y$ in A, we have $y = fx + g(y^2 - x^3)$ in $k[x, y]$ for some $f, g \in k[x, y]$. Rearranging yields $y(1 - gy) = x(f - gx^2)$. But $x \nmid y$ in $k[x, y]$, so we would get $x \mid (1 - gy)$. This is impossible because the constant coefficient of $1 - gy$ is non-trivial.

Now set $t \coloneqq y/x \in K \setminus A$. Then t is integral over A since $t^2 = y^2/x^2 = x^3/x^2 = x \in A$. Hence A is not normal. Since $t^3 = y^3/x^3 = yx^3/x^3 = y \in A$, we have $A \subseteq k[t] \subseteq \overline{A}^K$. But $k[t]$ is a principal ideal domain, so it is normal by Proposition 7.4, and we already have $k[t] = \overline{A}^K$.

If we consider the map on spectra $\operatorname{Spec}(k[t]) \to \operatorname{Spec}(A)$ (Figure 7.1), by taking the integral closure of A, we removed the cusp at the point $(0, 0)$, i. e. at the prime ideal (x, y) (also cf. Exercise 8.51). So normality is an algebraic notion for what it means to for a space to be non-singular, e. g. to be a $\mathbb{C}$-manifold.

Proposition 7.13. *Let A be a normal noetherian integral domain, and let L/K be a finite separable field extension with $K \coloneqq \operatorname{Quot}(A)$. Then $A \subseteq \overline{A}^L$ is a finite ring extension.*

Proof. For any finite field extension L/K, we can define the **trace pairing**

$$Q \colon L \times L \to K, \qquad Q(x, y) \coloneqq \operatorname{tr}_{L/K}(xy).$$

By the properties of the trace, the trace pairing is a K-bilinear form (i. e. it maps to the scalar field K).

The following fact holds true: L/K is separable if and only Q is non-degenerate (i. e. $Q(x, y) = 0$ for all $y \in L$ if and only if $x = 0$) if and only if there exists some $x \in L$ such that $\operatorname{tr}_{L/K}(x) \neq 0$.

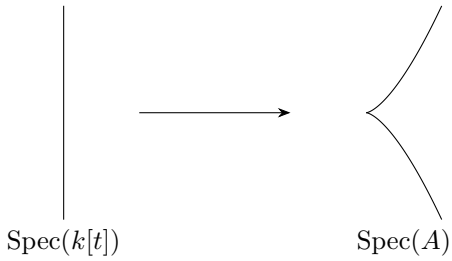


Figure 7.1: The map $\operatorname{Spec}(k[t]) \to \operatorname{Spec}(A)$ for algebraically closed k. The generic point (0) is missing in the picture.

If Q is non-degenerate, pick any $0 \neq x \in L$. Then there exists some $y \in L$ such that $Q(x,y) = \operatorname{tr}_{L/K}(xy) \neq 0$. Conversely, if $\operatorname{tr}_{L/K}(x) \neq 0$ for some $x \in L$, then $Q(xy^{-1}, y) = \operatorname{tr}_{L/K}(x) \neq 0$ for all $y \in L^\times$. For the other equivalence, see e. g. [Sta, 0BIL].

Now to the actual proof. By the primitive element theorem, there exists an $\alpha \in L$ such that $L = K(\alpha)$. We can assume that α is integral over A: Let $m(T) \coloneqq \min_{L/K}(\alpha, T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in K[T]$. Pick $s \in A \setminus \{0\}$ such that $sa_i \in A$ for all i, for example the product of all denominators. Then $\min_{L/K}(s\alpha, T) = T^n + sa_{n-1}T^{n-1} + \cdots + s^n a_0 \in A[T]$ since $\min_{L/K}(s\alpha, s\alpha) = s^n m(\alpha) = 0$ and $K(s\alpha) \cong K(\alpha)$ as K-vector spaces ($\{1, s\alpha, \dots, (s\alpha)^{n-1}\}$ is a K-basis), i. e. the minimal polynomial must have degree $[K(\alpha) : K] = n$. So from now on, we assume that α is integral over A; otherwise we consider $s\alpha$.

Then $B \coloneqq A[\alpha] \subseteq L$ is a finite ring extension by Proposition 5.7, and even free as an A-module of rank n since $B \cong A[T]/(m(T))$, i. e. $B = \bigoplus_{i=0}^{n-1} A\alpha^i$. (The kernel of the evaluation $A[T] \twoheadrightarrow B$, $T \mapsto \alpha$ is $(m(T))$: Every polynomial $g(T) \in A[T]$ with $g(\alpha) = 0$ is divisible by $m(T)$ in $K[T]$, which is a unique factorisation domain. Thus there is some $h(T) \in K[T]$ such that $m(T)h(T) = g(T)$. Multiplying with the product of all denominators of the coefficients in h, we see that $g(T) \in (m(T))$. By the homomorphism theorem, we have $B \cong A[T]/\ker(A[T] \twoheadrightarrow B)$.)

Now consider $M \coloneqq \{x \in L \mid Q(x,b) \in A \text{ for all } b \in B\}$, which is an A-submodule of B by linearity of Q in the first variable. If $x \in \overline{A}^L$, then $bx \in \overline{A}^L$ for all $b \in B$ since $B \subseteq \overline{A}^L$. Since A is normal, we have $\operatorname{char}(xb, T) \in A[T]$ by Proposition 7.5. This implies $\operatorname{tr}_{L/K}(xb) \in A$ for all $b \in B$ as $\operatorname{tr}_{L/K}(xb)$ is the coefficient of the term of second highest degree of $\operatorname{char}(xb, T)$. Thus $x \in M$, so $\overline{A}^L \subseteq M$.

We claim that M is finite (and even free) as an A-module. Then, since A is noetherian by assumption, $\overline{A}^L \subseteq M$ is a finite A-submodule by Corollary 3.25 as desired.

We know that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an A-basis of the finite free module B and a K-basis of the vector space L. Let $Z \in \mathrm{GL}_n(K)$ be the matrix such that

$$Q(x,y) = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} Z \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

w. r. t. that basis. Z must be invertible since Q is non-degenerate (see linear algebra).

Then we have $x \in M$ if and only if $Q(x,b) = b^t Z x \in A$ for all $b \in B$ if and only if $Q(x, \alpha^{i-1}) = (e_i)^t Z x \in A$ for all $i = 1, \dots, n$. Note that $(e_i)^t Z x$ describes the ith entry of Zx, so this is equivalent to $Zx \in A^{\oplus n}$, i. e. $x \in Z^{-1}A^{\oplus n} \cong Z^{-1}B$. Summarising, $Z \colon L \to L$ is a K-vector space as well as an A-linear automorphism such that $M \cong S^{-1}B$. In particular, M is free of rank n since B is. □

Corollary 7.14. *Let A be a normal noetherian integral domain, and let $L/\operatorname{Quot}(A)$ be a finite separable field extension. Then $\overline{A}^L$ is again a normal noetherian integral domain.*

Proof. By Corollary 5.9, we have $\overline{\overline{A}^L}^L = \overline{A}^L$, so $\overline{A}^L$ is normal. Proposition 7.13 and Corollary 3.25 imply that $\overline{A}^L$ is noetherian. $\overline{A}^L$ as a subset of the field L must be an integral domain. □

Corollary 7.15. *If $K/\mathbb{Q}$ is a finite field extension, then $\mathcal{O}_K$ is a one-dimensional normal noetherian integral domain, and $\mathcal{O}_K \cong \mathbb{Z}^{\oplus[K:\mathbb{Q}]}$ as a finite free $\mathbb{Z}$-module.*

Proof. With Proposition 7.4, $A = \mathbb{Z}$ is a normal noetherian integral domain. Since $\operatorname{char}(\mathbb{Q}) = 0$, by [Sch, Thm. 6.21], every field extension of $\mathbb{Q}$, and in particular $K/\mathbb{Q}$, is separable. Hence $K/\operatorname{Quot}(\mathbb{Z})$ is a finite separable field extension. Thus $\overline{\mathbb{Z}}^K = \mathcal{O}_K$ is a normal noetherian integral domain by Corollary 7.14. Because of Proposition 7.13, $\mathbb{Z} \subseteq \mathcal{O}_K$ is a finite ring extension, so $\dim(\mathcal{O}_K) = \dim(\mathbb{Z}) = 1$ by Corollary 5.17.

Since $\mathcal{O}_K \subseteq K$, $\mathcal{O}_K$ is a torsion-free $\mathbb{Z}$-module. Hence $\mathcal{O}_K \cong \mathbb{Z}^{\oplus r}$ by the structure theorem 3.52. Observe that since $\alpha \in \mathcal{O}_K$ and $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, we have $(\mathbb{Z} \setminus \{0\})^{-1}\mathcal{O}_K = K$. Localising with $\mathbb{Z} \setminus \{0\}$ yields $K \cong (\mathbb{Z} \setminus \{0\})^{-1}\mathbb{Z}^{\oplus r} \cong \mathbb{Q}^{\oplus r}$ as $\mathbb{Q}$-vector spaces. Thus $r = [K : \mathbb{Q}]$. □

Remark 7.16. Many integral closures one encounters as a working mathematician are actually finite, and there are many similar statements implying finiteness of integral closures. For example, consider the following statement:

Proposition: Let A be an integral domain which is finitely generated over a field or over $\mathbb{Z}$. Let L/K with $K := \operatorname{Quot}(A)$ be a finite field extension. Then $A \subseteq \overline{A}^L$ is finite.

Further information can be found under the keywords *excellent rings* ([Mat, ch. 13], [Sta, 07QS]) and *Japanese rings* ([Mat, ch. 12], [Sta, 0BI1]).

7.2 Relation with Localisation

Proposition 7.17. *Let A be an integral domain.*

(i) *If $S \subseteq A$ is a multiplicative subset, and if A is normal, then $S^{-1}A$ is normal.*

(ii) *Conversely, if $A_\mathfrak{m}$ is normal for all maximal ideals $\mathfrak{m} \subset A$, then A is normal.*

Thus normality is a local property (local in the sense of localisations).

Proof. Set $K := \operatorname{Quot}(A)$.

(i) Let $\frac{x}{y} \in K$ be integral over $S^{-1}A$, i. e.

$$\left(\frac{x}{y}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{x}{y}\right)^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

with $a_i/s_i \in S^{-1}A$ is an integral dependence relation. We want to see that $\frac{x}{y} \in S^{-1}A$.

Put $s = ys_{n-1}\cdots s_0$. Then multiplying with s^n yields

$$\left(s\frac{x}{y}\right)^n + s\frac{a_{n-1}}{s_{n-1}}\left(s\frac{x}{y}\right)^{n-1} + \cdots + s^n\frac{a_0}{s_0} = 0.$$

This is an integral dependence relation of $s\frac{x}{y} \in K$ over A. Hence $s\frac{x}{y} \in A$ since A is normal, whence $\frac{x}{y} = s^{-1}(s\frac{x}{y}) \in S^{-1}A$.

(ii) Let $x \in K$ be integral over A. We want to show that $x \in A$. The proof will be similar to Proposition 4.59.

Let us consider the ideal $\mathfrak{a} := \{a \in A \mid ax \in A\} \subseteq A$. Let $\mathfrak{m} \subset A$ be a maximal ideal. By the normality of $A_\mathfrak{m}$, we have $x \in A_\mathfrak{m}$, so we can write $x = \frac{a}{m}$ for some $a \in A$ and $m \notin \mathfrak{m}$. Thus we have $m \in \mathfrak{a}$, so $\mathfrak{a} \nsubseteq \mathfrak{m}$. Since this holds for all maximal $\mathfrak{m}$, by Corollary 2.19, $\mathfrak{a} = A$ holds. In particular, $1 \in \mathfrak{a}$, i. e. $x = 1x \in A$.

Alternative: We can also reformulate the above proof. Define $\mathfrak{a}$ as before. Let $\mathfrak{m} \subset A$ be maximal. If we pass $\mathfrak{a}$ to $A_\mathfrak{m}$, we obtain $\mathfrak{a}A_\mathfrak{m} = \{a \in A_\mathfrak{m} \mid ax \in A_\mathfrak{m}\}$. By the normality of $A_\mathfrak{m}$, we have $x \in A_\mathfrak{m}$, hence $\mathfrak{a}A_\mathfrak{m}$ contains a unit of $A_\mathfrak{m}$, i. e. $\mathfrak{a}A_\mathfrak{m} = A_\mathfrak{m}$. Observe that $\mathfrak{a} \nsubseteq \mathfrak{m}$ as otherwise, $\mathfrak{a}A_\mathfrak{m} \subseteq \mathfrak{m}A_\mathfrak{m} \neq A_\mathfrak{m}$ because $A_\mathfrak{m}$ is local. Since this holds for all maximal $\mathfrak{m}$, we obtain $\mathfrak{a} = A$. □

Corollary 7.18. *Let A be an integral domain. Then the following are equivalent:*

(i) *A is normal.*

(ii) *$A_\mathfrak{p}$ is normal for all $\mathfrak{p} \in \operatorname{Spec}(A)$.*

(iii) *$A_\mathfrak{m}$ is normal for all $\mathfrak{m} \in \operatorname{MaxSpec}(A)$.*

Lect. 21
03.07.23

7.3 Discrete Valuation Rings

We will study one-dimensional normal noetherian local integral domains.

Lemma 7.19. *Let $(A, \mathfrak{m})$ be a one-dimensional local integral domain. Assume that $\mathfrak{m}$ is finitely generated. Let $(0) \neq \mathfrak{a} \subseteq \mathfrak{m}$ be any ideal. Then there exists an $n \geq 0$ such that $\mathfrak{m}^n \subseteq \mathfrak{a}$.*

Proof. As A is one-dimensional, there are only two prime ideals, namely (0) and $\mathfrak{m}$. Then $A/\mathfrak{a}$ is of dimension 0 since $\mathfrak{a} \neq (0)$ (we 'cut' of the prime ideal (0), leaving $\mathfrak{m}$) with unique prime ideal $\bar{\mathfrak{m}} \coloneqq \mathfrak{m}/\mathfrak{a}$. Thus $\operatorname{nil}(A/\mathfrak{a}) = \bar{\mathfrak{m}}$ by Proposition 2.22. By assumption, $\bar{\mathfrak{m}} = (x_1, \dots, x_r)$ is finitely generated, so there is some $k \geq 0$ such that $x_1^k = \cdots = x_r^k = 0$. Now set $n \coloneqq rk$. Since $\bar{\mathfrak{m}}^n = (x_1^{e_1} \cdots x_r^{e_r} \mid e_1 + \cdots + e_r = n, e_i \geq 0)$, we see that each generator contains a power $x_i^{e_i}$ with $e_i \geq k$, i. e. every generator is 0. We obtain $\bar{\mathfrak{m}}^n = 0$, which means $\mathfrak{m}^n \subseteq \mathfrak{a}$. □

Proposition 7.20. *Let $(A, \mathfrak{m})$ be a one-dimensional local integral domain. Assume that $\mathfrak{m}$ is finitely generated. Then*

$$\bigcap_{n \geq 0} \mathfrak{m}^n = (0).$$

Proof. Assume that $0 \neq x \in \bigcap_{n \geq 0} \mathfrak{m}^n$. In particular, $(0) \neq (x) \subseteq \mathfrak{m}$, so by Lemma 7.19, there is some $n \geq 0$ such that $\mathfrak{m}^n \subseteq (x)$. We also have $(x) \subseteq \mathfrak{m}^n$, hence $(x) = \mathfrak{m}^n$. It follows that $x \in \mathfrak{m}^{2n} \subseteq (x^2)$, which means that $x = ax^2$ for some $a \in A$. Since A is an integral domain and $x \neq 0$, we can divide by x to obtain $1 = ax$, i. e. $x \in A^\times$ But this contradicts $x \in \mathfrak{m}$. □

Remark 7.21. Under these assumptions, one can show that A is noetherian.

In fact, if A is any noetherian ring, then $\bigcap_{n \geq 0} \mathfrak{a}^n = (0)$ for all ideals $\mathfrak{a} \subset A$. This result is known as **Krull's intersection theorem**, see [AtMac, ch. 10]

Proposition 7.22. *Let $(A, \mathfrak{m})$ be a local integral domain such that*

(i) *$\mathfrak{m} = (\pi)$ for some $\pi \neq 0$ and*

(ii) *$\bigcap_{n \geq 0} \mathfrak{m}^n = (0)$.*

Then A is a principal ideal domain. More precisely, every ideal $(0) \neq \mathfrak{a} \subseteq A$ is of the form (π^n) for a unique $n \geq 0$.

Proof. Let $0 \neq a \in A$ be arbitrary. Observe that we have an infinite chain of ideals $\cdots \subset \mathfrak{m}^2 \subset \mathfrak{m} \subset A$. (This chain is proper as otherwise $\pi^n = a\pi^{n+1}$ for some $a \in A$, i. e. $\pi \in A^\times$, contradicting $\mathfrak{m} = (\pi)$.) Hence by (ii), there exists a unique number $v(a) \geq 0$ such that $a \in \mathfrak{m}^{v(a)} \setminus \mathfrak{m}^{v(a)+1}$ ($v(a)$ will be the *valuation*). Using (i), this means that $a = u\pi^{v(a)}$ with $u \notin A \setminus \mathfrak{m} = A^\times$ as A is local.

This implies for all ideals $(0) \neq \mathfrak{a} \subseteq A$ that $\mathfrak{a} = (\pi^{v(\mathfrak{a})})$ where $v(\mathfrak{a}) \coloneqq \min\{v(a) \mid a \in \mathfrak{a}\}$. □

Theorem 7.23. *Let $(A, \mathfrak{m})$ be a one-dimensional normal noetherian local integral domain. Then A is a principal ideal domain.*

Proof. We first show that $\mathfrak{m} = (\pi)$ is principal. Let $z = \frac{y}{x} \in \operatorname{Quot}(A) \setminus A$ with $x, y \in A$. Then necessarily $0 \neq x \in A \setminus A^\times = \mathfrak{m}$ (A is local). By Lemma 7.19, there is some $n \geq 1$ such that $\mathfrak{m}^n \subseteq (x)$, and hence $\mathfrak{m}^n z \subseteq (x)\frac{y}{x} = (y) \subseteq A$. Choose n minimally with the property $\mathfrak{m}^n z \subseteq A$, i. e. $\mathfrak{m}^{n-1} z \nsubseteq A$, and let $s \in \mathfrak{m}^{n-1}$ be such that $w \coloneqq sz \notin A$. Then $\mathfrak{m}w = (\mathfrak{m}s)z \subseteq \mathfrak{m}^n z \subseteq A$ is some ideal.

We will show that $\mathfrak{m}w \subseteq \mathfrak{m}$ is impossible by way of contradiction. So assume that $\mathfrak{m}w \subseteq \mathfrak{m}$. We view $A^{\oplus r} \twoheadrightarrow \mathfrak{m}$ as a finitely generated A-module, which is justified by the assumption that A is noetherian. We now repeat an argument from Proposition 5.7: Cayley-Hamilton 8.19 implies that there exists some monic polynomial $f \in A[T]$ such that $f(w) = 0$ in A.

In more detail, interpret $w \in \operatorname{End}_A(\mathfrak{m})$ as an A-linear map by left-multiplication (this is possible since $\mathfrak{m}w \subseteq \mathfrak{m}$). Pick a lift $\tilde{w} \in M_r(A)$ such that the following diagram commutes:

$$\begin{array}{ccc} A^{\oplus r} & \twoheadrightarrow & \mathfrak{m} \\ \downarrow{\scriptstyle \tilde{w}} & & \downarrow{\scriptstyle w} \\ A^{\oplus r} & \twoheadrightarrow & \mathfrak{m} \end{array}$$

Now we apply Cayley-Hamilton 8.19 to $\tilde{w}$, i. e. if $f(T) \coloneqq \operatorname{char}_{\tilde{w}}(T) \in A[T]$, then $f(\tilde{w}) = 0$ in $M_r(A)$, but by surjectivity of $A^{\oplus r} \twoheadrightarrow \mathfrak{m}$, also $f(w) = 0$ in $\operatorname{End}_A(\mathfrak{m})$. Since we are in an integral domain, $\mathfrak{m}$ is torsion-free as an A-module. Hence the map $A \to \operatorname{End}_A(\mathfrak{m})$ is injective, meaning that multiplication with $a \in A$ is the zero map in $\operatorname{End}_A(\mathfrak{m})$ if and only if $a = 0$. We deduced that $f(w) = 0$ in A.

Therefore w is integral over A. By assumption, A is normal, implying that $w \in A$, a contradiction.

Thus not $\mathfrak{m}w \subseteq \mathfrak{m}$, but $\mathfrak{m}w = A$. In other words, there is some $\pi \in \mathfrak{m}$ such that $\pi w = 1$. Then we can write each $m \in \mathfrak{m}$ as $m = \pi m w$ with $mw \in \mathfrak{m}w \subseteq A$. Thus $\mathfrak{m} \subseteq (\pi) \subset A$, and by maximality of $\mathfrak{m}$, finally $\mathfrak{m} = (\pi)$. Propositions 7.20 and 7.22 finish the proof. □

Example 7.24. We do not automatically obtain $f(w) = 0$ in A from $f(w) = 0$ in $\mathfrak{m}$ (cf. Proposition 5.7). Some extra argument is necessary; in this case, $\mathfrak{m}$ was a torsion-free A-module.

To see how this otherwise breaks, consider $w = \frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z}$, $f = T + 1 \in \mathbb{Z}[T]$ and $M = \mathbb{Z}/3$, which is a finitely generated $\mathbb{Z}$-module and *not* torsion-free. If we view $w \in \operatorname{End}_{\mathbb{Z}}(M)$, then $\frac{1}{2} \equiv -1 \mod (3)$, so we obtain $f(w) = 0$ in $\operatorname{End}_{\mathbb{Z}}(M)$, but $f(w) \neq 0$ in $\mathbb{Q}$.

Definition 7.25.

(i) A **discrete valuation ring** (DVR) is a one-dimensional normal noetherian local integral domain. Equivalently, a discrete valuation ring is a local principal ideal domain that is not a field.

(ii) Let $(A, \mathfrak{m})$ be a discrete valuation ring. A **uniformiser** of A is a prime element $\pi \in A$ such that $\mathfrak{m} = (\pi)$. Once π is fixed, we can write any $0 \neq a \in A$ as $a = u\pi^{v(a)}$ with unique $v(a) \in \mathbb{Z}_{\geq 0}$ and $u \in A^\times$.

(iii) Let $(A, \mathfrak{m})$ be a discrete valuation ring. The **valuation** of A is the function

$$v \colon A \to \mathbb{Z}_{\geq 0} \cup \{\infty\}, \qquad a \mapsto \begin{cases} v(a), & \text{if } a \neq 0, \\ \infty, & \text{otherwise.} \end{cases}$$

We can uniquely extend v to $\operatorname{Quot}(A)$ by

$$v \colon \operatorname{Quot}(A) \to \mathbb{Z} \cup \{\infty\}, \qquad v\left(\frac{a}{b}\right) \coloneqq v(a) - v(b).$$

Proof. (From me.)

(i) We show that the two definitions are indeed equivalent. Let $(A, \mathfrak{m})$ be a discrete valuation ring.

We know from Theorem 7.23 that A in the first sense implies that A is a principal ideal domain. Furthermore, A cannot be a field since $\dim(A) = 1 \neq 0$.

Conversely, with Proposition 7.4, every principal ideal domain is a normal noetherian integral domain. Furthermore, let $(0) \neq \mathfrak{m} = (\pi)$ with prime element $\pi \in A$ (A is not a field). For any prime ideal $(\pi') \subset A$, we thus have $(\pi') \subseteq (\pi)$, i. e. $\pi \mid \pi'$. Since π' is prime, it follows that $\pi = \pi'$. In other words, $(\pi) = \mathfrak{m}$ is the only non-zero prime ideal, and hence $\dim(A) = 1$.

(ii) Existence and uniqueness follows by applying Proposition 7.22 to $\mathfrak{a} = (a) \neq (0)$.

(iii) The extension to $\operatorname{Quot}(A)$ is well-defined: If $0 \neq \frac{a}{b} \in \operatorname{Quot}(A)$ is not fully reduced, $v(a)$ and $v(b)$ differ by the same amount, and this difference vanishes in $v(\frac{a}{b})$. If $\frac{a}{b} = 0$ with $a = 0$ and $b \neq 0$, then $v(b) < \infty$ and $v(\frac{a}{b}) = \infty - v(b) = \infty$. □

Example 7.26. Here some examples for discrete valuation rings.

(i) Let $A = k[\![t]\!]$, and let $K = (\!(t)\!)$. We know that A is local principal ideal domain w. r. t. (t) (Proposition 1.50). Then uniformisers are e. g. t or $(1 + t)t$ (recall from Example 1.48 that $(1 + t) \in A^\times$). The valuation is $v(a_n t^n + a_{n+1} t^{n+1} + \cdots) = n$ if $a_n \neq 0$ since $a_n + a_{n+1} t + \cdots \in A^\times$ if $a_n \in k^\times$ (Proposition 1.47).

(ii) Let $A \subset \mathbb{C}[\![t - a]\!]$ be the ring of all power series $f(t) = \sum_{k=0}^{\infty} a_k (t - a)^k$ that converge absolutely on an open neighbourhood of $a \in \mathbb{C}$, i. e. the ring of all *analytic* functions in a. Complex analysis says that a function is analytic if and only if it is holomorphic, i. e. differentiable on the complex plane.

Then A is called the *ring of germs of holomorphic functions in a*, where addition and multiplication is defined pointwise. Here, a *germ* is the equivalence class of all functions in A that agree on some open neighbourhood of a. One can show that A is a discrete valuation ring with uniformiser e. g. $(t-a)$ and valuation $v(f) = \operatorname{ord}_{t=a}(f)$, which is the order of vanishing in a (the multiplicity of the root a). (For instance, A is local since the set of all germs that vanish at a are precisely all non-unit germs, which form the ideal $(t-a)$.)

$K = \operatorname{Quot}(A)$ then consists of convergent *Laurent series* $f(t) = \sum_{k=-\infty}^{\infty} a_k (t-a)^k$. One calls K the *field of germs of meromorphic functions in a*, i. e. holomorphic functions which have singularities, and $\operatorname{ord}_{t=a}(f) < 0$ if and only if f has a pole in a.

(iii) Let $A = \mathbb{Z}_{(p)}$. Then (A, pA) is a one-dimensional ($\operatorname{ht}((p)) = 1$ in $\mathbb{Z}$) normal (Propositions 7.4 and 7.17) noetherian (Proposition 3.28) local integral domain. Thus A is a discrete valuation ring with uniformiser p and *p-adic valuation* $v_p \colon \mathbb{Q}^\times \to \mathbb{Z}$, $v_p(p^n \frac{a}{b}) \coloneqq n$ if $p \nmid ab$.

(iv) Let A be a normal noetherian integral domain, and let $\mathfrak{p} \subset A$ be a prime ideal of height 1. Then $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$ is a discrete valuation ring by the same argument as in part (iii).

We can pull back the valuation $v_\mathfrak{p} \colon A_\mathfrak{p} \to \mathbb{Z}_{\geq 0}$ to A via the localisation map, i. e. define $v_\mathfrak{p} \colon A \to A_\mathfrak{p} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$. If A is a finite type algebra over a field k of Krull dimension m, then $v_\mathfrak{p}(f)$ for $f \in A$ can be thought of as the vanishing order of f along $Z(\mathfrak{p}) \subseteq \overline{k}^m$.

Proposition 7.27 (properties of valuation)**.** *Let A be a discrete valuation ring with valuation v, and let $K \coloneqq \operatorname{Quot}(A)$. Then the following hold:*

(i) *$v(xy) = v(x) + v(y)$ for all $x, y \in A$.*

(ii) *$v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in A$ (**strong triangle inequality**).*

(iii) *We have the following short exact sequence:*

$$1 \longrightarrow A^\times \longrightarrow K^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

Remark 7.28. The strong triangle inequality in the above form might look unreasonable; especially since the relation sign is reversed. In analysis, an *ultrametric* d on some space X is a metric that satisfies the *strong triangle inequality* $d(x+y) \leq \max\{d(x), d(y)\}$ for all $x, y \in X$.

Note that (i) is the logarithmic functional equation. So we can equivalently bring the valuation in multiplicative form, which is usually done for p-adic valuation of $\mathbb{Z}_{(p)}$. We define $|x|_p \coloneqq p^{-v_p(x)}$ for all $x \in \mathbb{Q}$. Then we obtain $|xy| = |x| \cdot |y|$ and $|x+y| \leq \max\{|x|, |y|\}$ as well as $|x| = 0$ if and only if $x = 0$ (hence the minus sign). In particular, $|\cdot|_p$ is an ultrametric. We recover v_p via $v_p(x) = -\log_p |x|$.

Proof. (This follows from the definitions.) Let $\pi \in A$ be a uniformiser.

(i) Write $x = u\pi^{v(x)}$ and $y = w\pi^{v(y)}$ with $u, w \in A^\times$. Then $xy = uw\pi^{v(x)+v(y)}$ with $uw \in A^\times$, hence $v(xy) = v(x) + v(y)$.

(ii) Write $x = u\pi^{v(x)}$ and $y = w\pi^{v(y)}$ with $u, w \in A^\times$. If $m \coloneqq \min\{v(x), v(y)\}$, then $x+y = \pi^m(u\pi^{v(x)-m} + w\pi^{v(y)-m})$, hence $v(x+y) \geq m$.

(iii) Exactness in $A^\times$ is clear (this is the inclusion $A^\times \hookrightarrow K^\times$, $a \to \frac{a}{1}$). For exactness in $K^\times$, observe that $x \in \ker(v)$ if and only if $x = u\pi^0$ for some $u \in A^\times$. Exactness in $\mathbb{Z}$ follows from $\pi \neq 0$ and $v(\pi^n) = n$ for all $n \in \mathbb{Z}$. □

7.4 Dedekind Rings

Definition 7.29. A **Dedekind ring** is a one-dimensional normal noetherian integral domain. Equivalently, a Dedekind ring is a noetherian integral domain A that is not a field, and such that $A_\mathfrak{p}$ is a discrete valuation ring for all prime ideals $(0) \neq \mathfrak{p} \subset A$.

Proof. (From me.) We proof the equivalence of both definitions.

Let A be of the first form. Then $\operatorname{ht}(\mathfrak{p}) = 1$ for all prime ideals $(0) \neq \mathfrak{p} \subset A$, so A is not a field. Furthermore, $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$ is a one-dimensional normal (Corollary 7.18) noetherian (Proposition 3.28) local integral domain. Thus $A_\mathfrak{p}$ is a discrete valuation ring.

Conversely, let A be of the second form. Since $\dim(A_\mathfrak{p}) = 1$ for all prime ideals $(0) \neq \mathfrak{p} \subset A$, we have $\dim(A) = 1$ too. Normality of A follows from Corollary 7.18. □

Compared to the definition of discrete valuation rings, we drop the local property.

Example 7.30. Let $K/\mathbb{Q}$ be a finite field extension. Recall that $\mathcal{O}_K \coloneqq \overline{\mathbb{Z}}^K = \{x \in K \mid \operatorname{char}_{K/\mathbb{Q}}(x) \in \mathbb{Z}[T]\}$, which is a Dedekind ring by Corollary 7.15. Every prime ideal $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ defines a discrete valuation ring $\mathcal{O}_{K,\mathfrak{p}}$ with its so-called **$\mathfrak{p}$-adic valuation** $v_\mathfrak{p} \colon K^\times \to \mathbb{Z}$.

Example 7.31. Let $D \in \mathbb{Z}$ be square-free, and let $K \coloneqq \mathbb{Q}(\sqrt{D})$. Proposition 7.10 gives the complete description

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \equiv 2,3 \mod (4), \\ \mathbb{Z}\left[\dfrac{1+\sqrt{D}}{2}\right], & \text{if } D \equiv 1 \mod (4). \end{cases}$$

Assume that there is an odd prime p dividing D. Then

$$\mathcal{O}_K/p\mathcal{O}_K \cong \begin{cases} \mathbb{F}_p[t]/(t^2 - D) \cong \mathbb{F}_p[t]/(t^2), & \text{if } D \equiv 2,3 \mod (4), \\ \mathbb{F}_p[t]/\left(t^2 - t + \dfrac{1-D}{4}\right) \cong \mathbb{F}_p[t]/\left(t - \dfrac{1}{2}\right)^2, & \text{if } D \equiv 1 \mod (4), \end{cases} \tag{7.32}$$

via $t \mapsto t$ in both cases since $D = 0$ in $\mathbb{F}_p$. In greater detail, by the homomorphism theorem,

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[f]/p\mathbb{Z}[f] \cong \mathbb{Z}/p[f] = \mathbb{F}_p[f] \cong \mathbb{F}_p[t]/(\min_{\mathbb{F}_p}(f,t))$$

where

$$\min_{\mathbb{F}_p}(f,t) = \begin{cases} t^2 - D, & \text{if } f = \sqrt{D}, \\ t^2 - t + \dfrac{1-D}{4}, & \text{if } f = \dfrac{1+\sqrt{D}}{2}, \end{cases}$$

(it is important that $p \neq 2$, as otherwise $\min_{\mathbb{F}_2}(\sqrt{D}, t) = t - 1$).

We see that $\mathbb{F}_p[t]/(t^2)$ (resp. $\mathbb{F}_p[t]/(t - \frac{1}{2})^2$) has a unique prime ideal containing t^2 (resp. $(t - \frac{1}{2})^2$), namely (t) (resp. $(t - \frac{1}{2})$). Due to the isomorphisms in (7.32), this corresponds to a unique prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$ (cf. Observation 2.4). Passing $\mathfrak{p}$ to the localisation $\mathcal{O}_{K,\mathfrak{p}}$, we know that $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = (\pi)$ must be principal. The above computation shows that π corresponds to t (resp. $t - \frac{1}{2}$), so

$$\pi = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2,3 \mod (4), \\ \dfrac{1+\sqrt{D}}{2} - \dfrac{1}{2} = \dfrac{\sqrt{D}}{2}, & \text{if } D \equiv 1 \mod (4), \end{cases} \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \setminus \mathfrak{p}^2\mathcal{O}_{K,\mathfrak{p}}$$

(note that $p \neq 2$, so $2 \in \mathcal{O}_{K,\mathfrak{p}}^\times$ and thus $\frac{1}{2}\sqrt{D} \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$). Thus we may choose $\pi = \sqrt{D}$ as the uniformiser in both cases. It holds that $v_\mathfrak{p}(p) = 2$ because $\pi^2 = D = p\frac{D}{p}$ and $\frac{D}{p} \in \mathcal{O}_{K,\mathfrak{p}} \setminus \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}^\times$ since $p \nmid \frac{D}{p}$ by the square-freeness assumption on D ($\frac{D}{p}$ is an integer!).

7.5 Factorisation in Dedekind Domains

Lect. 22
06.07.23

Recall: A *Dedekind ring* is a one-dimensional normal noetherian integral domain.

Definition 7.33. Let A be a Dedekind ring, and let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal. Then $A_\mathfrak{p}$ is a discrete valuation ring. We define the **$\mathfrak{p}$-adic valuation** to be

$$v_\mathfrak{p} \colon A \to A_\mathfrak{p} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}, \qquad u\pi_\mathfrak{p}^n \mapsto n,$$

where $\pi_\mathfrak{p} \in A_\mathfrak{p}$ is a uniformiser and $u \in A_\mathfrak{p}^\times$.

We can extend this definition to ideals $(0) \neq \mathfrak{a} \subseteq A$ via

$$v_\mathfrak{p}(\mathfrak{a}) \coloneqq \min\{v_\mathfrak{p}(a) \mid a \in \mathfrak{a}\} \in \mathbb{Z}_{\geq 0},$$

which is the unique integer such that $\mathfrak{a}A_\mathfrak{p} = (\pi_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})}$ (we have $\pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \mid a$ in $A_\mathfrak{p}$ for all $a \in \mathfrak{a}$ and $u\pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \in \mathfrak{a}A_\mathfrak{p}$ for some $u \in A_\mathfrak{p}^\times$ since $v_\mathfrak{p}(\mathfrak{a}) < \infty$).

The main theorem about Dedekind rings states that ideals can be uniquely factored into prime ideals, mirroring the prime factorisation in principal ideal domains (Theorem 1.38). Before we proof this theorem, we need the following auxiliary statement.

Lemma 7.34. *Let A be any ring, let M be an A-module, and let $N_1, N_2 \subseteq M$ be two A-submodules. If $N_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}$ as $A_\mathfrak{p}$-submodules of $M_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, then $N_1 \subseteq N_2$.*

Proof. Recall from Proposition 4.60 that for $(M \to N \to P) = 0$, the sequence $M \to N \to P$ is exact if and only if the sequence $M_\mathfrak{p} \to N_\mathfrak{p} \to P_\mathfrak{p}$ is exact for all $\mathfrak{p} \in \operatorname{Spec}(A)$.

We apply this as follows in order to obtain a sequence of equivalent statements:

- $N_1 \subseteq N_2$.
- $f\colon N_1 \hookrightarrow M \twoheadrightarrow M/N_2$ is the zero map.
- The sequence
$$N_1 \xrightarrow{\text{id}} N_1 \xrightarrow{f} M/N_2 \xrightarrow{\text{id}} M/N_2$$
is exact.
- The sequence
$$N_{1,\mathfrak{p}} \xrightarrow{\text{id}} N_{1,\mathfrak{p}} \xrightarrow{f_\mathfrak{p}} (M/N_2)_\mathfrak{p} = M_\mathfrak{p}/N_{2,\mathfrak{p}} \xrightarrow{\text{id}} (M/N_2)_\mathfrak{p}$$
is exact for all $\mathfrak{p} \in \operatorname{Spec}(A)$ ($(M/N_2)_\mathfrak{p} = M_\mathfrak{p}/N_{2,\mathfrak{p}}$ follows from Corollary 4.55).
- $f_\mathfrak{p} = 0$ for all $\mathfrak{p}$.
- $N_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}$ for all $\mathfrak{p}$.

Alternative: This proof is in the same vein as Propositions 4.59 and 7.17. Let $\mathfrak{a} \coloneqq \{a \in A \mid aN_1 \subseteq N_2\} \subseteq A$, which is an ideal. Passing to the localisation $A_\mathfrak{p}$, we obtain $\mathfrak{a}A_\mathfrak{p} = \{a \in A_\mathfrak{p} \mid aN_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}\}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$. By assumption, we have $N_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}$, hence $\mathfrak{a}A_\mathfrak{p}$ contains a unit, i. e. $\mathfrak{a}A_\mathfrak{p} = A_\mathfrak{p}$. This implies $\mathfrak{a} \nsubseteq \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$; otherwise we would have $\mathfrak{a}A_\mathfrak{p} \subseteq \mathfrak{p}A_\mathfrak{p} \neq A_\mathfrak{p}$ since $A_\mathfrak{p}$ is local. This also holds for all $\mathfrak{p} = \mathfrak{m} \in \operatorname{MaxSpec}(A)$, and by Corollary 2.19, $\mathfrak{a} = A$. In particular, $1 \in \mathfrak{a}$, whence $N_1 = 1N_1 \subseteq N_2$. □

Corollary 7.35. *(From me, also cf. Proposition 4.60.) Let $\phi\colon M \to N$ be an A-linear map of A-modules. Then the following are equivalent:*

(i) *$\phi\colon M \to N$ is injective.*

(ii) *$\phi_\mathfrak{p}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for all $\mathfrak{p} \in \operatorname{Spec}(A)$.*

(iii) *$\phi_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for all $\mathfrak{m} \in \operatorname{Spec}(A)$.*

Now the main theorem.

Theorem 7.36. *Let A be a Dedekind ring, and let $(0) \neq \mathfrak{a} \subseteq A$ be an ideal. Then $v_\mathfrak{p}(\mathfrak{a}) \geq 1$ only for finitely many prime ideals $(0) \neq \mathfrak{p} \subset A$, and*

$$\mathfrak{a} = \prod_{\substack{(0) \neq \mathfrak{p} \subset A \\ v_\mathfrak{p}(\mathfrak{a}) \geq 1}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}.$$

Proof.

(i) We first show that $v_\mathfrak{p}(\mathfrak{a}) \geq 1$ for only finitely many $\mathfrak{p}$. We may assume that $\operatorname{Spec}(A)$ is infinite, as otherwise the claim is obvious.

First note that $v_\mathfrak{p}(\mathfrak{a}) \geq 1$ if and only if $\mathfrak{a}A_\mathfrak{p}$ does not contain a unit of $A_\mathfrak{p}$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$. Next, we apply Zorn's lemma to find a maximal element $\mathfrak{b}$ of the set

$$\{\text{ideals } \mathfrak{b} \subseteq A \mid \mathfrak{b} \subseteq \mathfrak{p} \text{ for infinitely many prime ideals } \mathfrak{p} \subset A\}$$

We claim that $\mathfrak{b}$ is prime. Assume that $ab \in \mathfrak{b}$. By construction, $ab \in \mathfrak{p}$ for infinitely many $\mathfrak{p}$ that contain $\mathfrak{b}$. Hence a or b lies in infinitely many $\mathfrak{p}$ that contain $\mathfrak{b}$; w. l. o. g. let a be the element with this property. Then $\mathfrak{b} + (a)$ is contained in infinitely many $\mathfrak{p}$. But $\mathfrak{b}$ is already maximal, so $\mathfrak{b} + (a) = \mathfrak{b}$, i. e. $a \in \mathfrak{b}$. This shows the claim.

Since A is a one-dimensional integral domain, (0) is the only prime ideal contained in infinitely many $\mathfrak{p}$. So we must have $\mathfrak{b} = (0)$. Furthermore, by maximality of $\mathfrak{b}$, $\mathfrak{b} = (0)$ is the only ideal contained in infinitely many $\mathfrak{p}$. In particular, $\mathfrak{a} \neq (0)$ is contained in only finitely many $\mathfrak{p}$, thus $v_\mathfrak{p}(\mathfrak{a}) \geq 1$ for only those $\mathfrak{p}$.

(ii) Put $\mathfrak{b} \coloneqq \prod_{v_\mathfrak{q}(\mathfrak{a}) \geq 1} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{a})}$, where all $(0) \neq \mathfrak{q} \subset A$ are prime. We next show that $\mathfrak{b}A_\mathfrak{p} = \mathfrak{a}A_\mathfrak{p}$ for all $\mathfrak{p}$. We have

$$\mathfrak{b}A_\mathfrak{p} = \left(\prod_{v_\mathfrak{q}(\mathfrak{a}) \geq 1} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{a})} \right) A_\mathfrak{p} = \prod_{v_\mathfrak{q}(\mathfrak{a}) \geq 1} (\mathfrak{q}A_\mathfrak{p})^{v_\mathfrak{q}(\mathfrak{a})} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})} = \mathfrak{a}A_\mathfrak{p}.$$

The second equality is always true. Namely, taking the extension of ideals commutes with products: Let $f\colon A \to B$ be any ring map. Then for ideals $\mathfrak{a}, \mathfrak{b} \subseteq A$, we have $f(\mathfrak{a}\mathfrak{b})B = \{f(a)f(b) \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}B = (f(\mathfrak{a})B)(f(\mathfrak{b})B)$. On the third equality: For all $(0) \neq \mathfrak{q} \neq \mathfrak{p}$, we have $\mathfrak{q} \not\subseteq \mathfrak{p}$ since $\dim(A) = 1$. Hence there exists some $s \in \mathfrak{q} \setminus \mathfrak{p}$, whence $\mathfrak{q}A_\mathfrak{p} = A_\mathfrak{p}$ because $s \in A_\mathfrak{p}^\times$. The last equality is the definition of $v_\mathfrak{p}$.

(iii) Applying Lemma 7.34 to $\mathfrak{b}A_\mathfrak{p} \subseteq \mathfrak{a}A_\mathfrak{p} \subseteq \mathfrak{b}A_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$ yields $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$, and we win. □

7.6 Fractional Ideals

The ideals in a Dedekind ring form an abelian monoid under multiplication. We want to turn them into an abelian group.

Definition 7.37. Let A be a Dedekind ring, and put $K \coloneqq \operatorname{Quot}(A)$. A **fractional ideal** of A is a finitely generated A-submodule $(0) \neq \mathfrak{a} \subseteq K$. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals, we define their product to be

$$\mathfrak{a}\mathfrak{b} \coloneqq (ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}),$$

which is again a fractional ideal: If $\mathfrak{a} = (a_1, \dots, a_n)$ and $\mathfrak{b} = (b_1, \dots, b_m)$, then $\mathfrak{a}\mathfrak{b} = (a_i b_j \mid i = 1, \dots, n; j = 1, \dots, m)$ is also a finitely generated A-submodule.

Proposition 7.38. *The fractional ideals of a Dedekind ring A form an abelian group under multiplication.*

Proof. Let $K \coloneqq \operatorname{Quot}(A)$. Commutativity, associativity and the neutral element $A = (1)$ follow directly from the ring properties of A. What remains to show is the existence of inverses. For a given fractional ideal $\mathfrak{a}$ of A, we claim that

$$\mathfrak{a}^{-1} \coloneqq \{x \in K \mid x\mathfrak{a} \subseteq A\}$$

is its inverse. Observe that this is indeed an A-submodule of K.

(i) We first show $\mathfrak{a}^{-1} \neq (0)$. By assumption, $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = (b_1/s_1, \dots, b_n/s_n)$ for $b_i, s_i \in A$ with $s_i \neq 0$. Then $0 \neq s_1 \cdots s_n \in \mathfrak{a}^{-1}$ (we have $s_1 \cdots s_n(b_i/s_i) \in A$ for all i), so $\mathfrak{a}^{-1} \neq (0)$.

(ii) Next, we show that $\mathfrak{a}^{-1}$ is finitely generated. Since $\mathfrak{a} \neq (0)$, there exists a $0 \neq y \in \mathfrak{a}$. Then $Ay \subseteq \mathfrak{a}$, and hence $\mathfrak{a}^{-1} \subseteq \{x \in K \mid x \cdot Ay \subseteq A\} = Ay^{-1}$. Since A is noetherian, Ay^{-1} is noetherian A-module by Corollary 3.25, and thus the submodule $\mathfrak{a}^{-1}$ is finitely generated.

(iii) We now show the inverse property where we have to exploit the Dedekind property. Let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal. First note that we can extend the definition of $\mathfrak{p}$-adic valuation in the discrete valuation ring $A_\mathfrak{p}$ to $A_\mathfrak{p}$-submodules of K. For $\mathfrak{a} \neq (0)$, we obtain $\mathfrak{a}A_\mathfrak{p} = (\pi_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})}$ for a unique $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$.

We claim that $\mathfrak{a}^{-1}A_\mathfrak{p} = (\mathfrak{a}A_\mathfrak{p})^{-1} = (\pi_\mathfrak{p})^{-v_\mathfrak{p}(\mathfrak{a})}$. For the second equality, we saw in (ii) that for principal ideals $(y) = Ay$ with $y \in K^\times$, $(y)^{-1} = Ay^{-1}$ holds. In our case,

$$(\mathfrak{a}A_\mathfrak{p})^{-1} = ((\pi_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})})^{-1} = (\pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})})^{-1} = (\pi_\mathfrak{p}^{-v_\mathfrak{p}(\mathfrak{a})}) = (\pi_\mathfrak{p}^{-1})^{v_\mathfrak{p}(\mathfrak{a})} = (\pi_\mathfrak{p})^{-v_\mathfrak{p}(\mathfrak{a})},$$

where $v_\mathfrak{p}((\pi_\mathfrak{p}^{-1})) = v_\mathfrak{p}(\pi_\mathfrak{p}^{-1}) = -1$, so indeed $(\pi_\mathfrak{p}^{-1}) = (\pi_\mathfrak{p})^{-1}$.

For the first equality of the claim, $\mathfrak{a}^{-1}A_\mathfrak{p} \subseteq (\mathfrak{a}A_\mathfrak{p})^{-1}$ follows from the definition of $\mathfrak{a}^{-1}$, namely pass $x\mathfrak{a} \subseteq A$ to the localisation $x\mathfrak{a}A_\mathfrak{p} \subseteq A_\mathfrak{p}$ for all $x \in \mathfrak{a}^{-1}$. Conversely, let $x \in (\mathfrak{a}A_\mathfrak{p})^{-1}$, i. e. for all $a \in \mathfrak{a}$, we have $xa \in A_\mathfrak{p}$. If we write $\mathfrak{a} = (a_1, \dots, a_n)$ and $xa_i = b_i/s_i$ with $b_i \in A$ and $s_i \in A \setminus \mathfrak{p}$ for all $i = 1, \dots, n$, then $a_i \in A$ for all i. We deduce $s_1 \cdots s_n x \in \mathfrak{a}^{-1}$, whence $x = (s_1 \cdots s_n x)/(s_1 \cdots s_n) \in \mathfrak{a}^{-1}A_\mathfrak{p}$. This proves the claim.

In conclusion, $(\mathfrak{a}\mathfrak{a}^{-1})A_\mathfrak{p} = (\mathfrak{a}A_\mathfrak{p})(\mathfrak{a}^{-1}A_\mathfrak{p}) = (\mathfrak{a}A_\mathfrak{p})(\mathfrak{a}A_\mathfrak{p})^{-1} = A_\mathfrak{p}$ for all $\mathfrak{p}$ (the first equality holds as we noted in Theorem 7.36). Lemma 7.34 implies that $\mathfrak{a}\mathfrak{a}^{-1} = A$. □

Example 7.39. The Dedekind property has to hold for this proof to work. Consider $A = k[X, Y]$, which is not Dedekind because $\dim(A) = 2$, e. g. $(0) \subset (X) \subset (X, Y)$. Consider $\mathfrak{a} = (X, Y) \subseteq A$. If we define $\mathfrak{a}^{-1} \coloneqq \{x \in k(X, Y) \mid x\mathfrak{a} \subseteq A\}$, then $\mathfrak{a}^{-1} = k[X, Y]$, hence $\mathfrak{a}^{-1}\mathfrak{a} = (X, Y) \subset k[X, Y]$.

Corollary 7.40. *Let A be a Dedekind ring. For every fractional ideal $\mathfrak{a}$ of A, there are unique $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$, which are almost all 0, such that*

$$\mathfrak{a} = \prod_{(0) \neq \mathfrak{p} \subset A} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}.$$

In other words: Let $\mathcal{I}_A$ be the group of fractional ideals of A. Then $\mathcal{I}_A \cong \bigoplus_{\mathfrak{p} \neq (0)} \mathbb{Z}[\mathfrak{p}]$, where $\mathbb{Z}[\mathfrak{p}]$ is the free abelian group with one generator $\mathfrak{p}$.

Proof. Pick any $0 \neq x \in \mathfrak{a}^{-1} \cap A$ (we can pick any $0 \neq x \in \mathfrak{a}^{-1}$ by Proposition 7.38 and multiply with its denominator). Then Ax and $x\mathfrak{a}$ are ideals in A, so they admit prime factorisations $\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x)}$ and $\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x\mathfrak{a})}$, resp., according to Theorem 7.36. We obtain

$$\mathfrak{a} = (x^{-1}x)\mathfrak{a} = (Ax)^{-1}(x\mathfrak{a}) = \prod_{\mathfrak{p} \neq (0)} \mathfrak{p}^{v_\mathfrak{p}(x\mathfrak{a}) - v_\mathfrak{p}(x)} = \prod_{\mathfrak{p} \neq (0)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}.$$

Uniqueness follows after passing to the discrete valuation ring $A_\mathfrak{p}$, i. e. $\mathfrak{a}A_\mathfrak{p} = (\pi_\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{a})}$. □

7.7 Ideal Class Group

Definition 7.41. Let A be a Dedekind ring, let $K \coloneqq \mathrm{Quot}(A)$, and let $\mathcal{I}_A$ be the abelian group of fractional ideals of A. Then $\mathfrak{a} \in \mathcal{I}_A$ is **principal** if there exists an $x \in K^\times$ such that $\mathfrak{a} = (x) \coloneqq Ax$. This defines the subgroup $\mathcal{P}_A \subseteq \mathcal{I}_A$ of principal fractional ideals. We call $\mathrm{Cl}_A \coloneqq \mathcal{I}_A/\mathcal{P}_A$ the **ideal class group** of A.

Proof. (From me.) We can easily convince ourself that $\mathcal{P}_A$ is indeed an abelian subgroup. Since $\mathcal{I}_A$ is abelian, $\mathcal{P}_A$ is normal, so Cl_A defines a group again. □

Remark 7.42. The following hold true:

(i) $\mathrm{Cl}_A = \{1\}$ if and only if every $\mathfrak{a} \in \mathcal{I}_A$ is principal if and only if every prime ideal $\mathfrak{p} \subset A$ is principal (Corollary 7.40) if and only if A is a principal ideal domain (Theorem 7.36).

In this sense, Cl_A measures the extent to which A is not a principal ideal domain.

(ii) $(x) = (y)$ for $x, y \in K^\times$ if and only if $(xy^{-1}) = (1)$ if and only if $x = uy$ for some $u \in A^\times$.

This implies the exactness in $K^\times$ (meaning $(x) = (1)$ if and only if $x \in A^\times$) of the following exact sequence:

$$1 \longrightarrow A^\times \hookrightarrow K^\times \xrightarrow{x \mapsto (x)} \mathcal{P}_A \hookrightarrow \mathcal{I}_A \twoheadrightarrow \mathrm{Cl}_A \longrightarrow 1$$

Example 7.43. Consider the Dedekind ring $A = \mathbb{Z}[\sqrt{-5}]$, which is not a principal ideal domain as we have seen in Example 2.53. For example, the ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$ is not principal.

($\mathfrak{p}$ is not principal since if $\mathfrak{p} = (p)$ for some $p \in \mathbb{Z}[\sqrt{-5}]$, then $p \mid 2, 1+\sqrt{-5}$. This implies $N(p) \mid \gcd(N(2), N(1+\sqrt{-5})) = 2$. But the norm of any p is never 2 because $x^2 + 5y^2 = 2$ has no solution in $\mathbb{Z}^2$. It follows that $N(p) = 1$ which, however, leads to $p \in \mathbb{Z}[\sqrt{-5}]^\times$ and $\mathfrak{p} = \mathbb{Z}[\sqrt{-5}]$, contradicting

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{Z}[T]/(2, T^2+5, T+1) \cong \mathbb{F}_2[T]/((T+1)^2, T+1) \cong \mathbb{F}_2[T]/(T+1) \cong \mathbb{F}_2 \neq 0.$$

The above calculation also shows that $\mathfrak{p}$ is maximal.)

We compute

$$\mathfrak{p}^2 = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) = (4, 2+2\sqrt{-5}, 2\sqrt{-5}) = (4, 2, 2\sqrt{-5}) = (2).$$

Thus $\mathfrak{p}$ is of order 2 in Cl_A, meaning $\mathfrak{p}^2$ is principal, and the inverse of $\mathfrak{p}$ is

$$\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p} = \left(1, \frac{1+\sqrt{-5}}{2}\right).$$

In fact, one can show that $\mathrm{Cl}_A \cong \mathbb{Z}/2$.

For the remaining subsection, we will state some interesting theorems and conjectures in number theory (without proof). This one is one of the most fundamental results in classical algebraic number theory.

Theorem 7.44 (Dedekind)**.** *Let $K/\mathbb{Q}$ be a finite field extension, and let $\mathcal{O}_K \subseteq K$ be the ring of integers. Then $\mathrm{Cl}_{\mathcal{O}_K}$ is finite. We call $h_K := |\mathrm{Cl}_{\mathcal{O}_K}|$ the **class number** of K.*

The number h_K (i. e. in which circumstances can h_K attain certain values) is still an active field of research, but some partial results are known. The following was already conjectured by Gauss.

Theorem 7.45 (**Stark-Heegner theorem**, 1967)**.** *There are precisely nine imaginary-quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ and $h_K = 1$. These are*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

The following is still an open problem.

Problem 7.46 (**class number problem**, conjecture)**.** There exist infinitely many real-quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$ and $h_K = 1$.

Remark 7.47. The ideal class group also appears in the geometric setting of **elliptic curves**. Let k be a field with $\mathrm{char}(k) \neq 2, 3$. Let $f(x) \in k[x]$ be a separable polynomial of degree 3. Then $A := k[x, y]/(y^2 - f(x))$ is a Dedekind domain and is an example of an elliptic curve in the plane.

Theorem 7.48 (group structure on points of an elliptic curve)**.** *Let $A = k[X, Y]/(Y^2 - f(X))$, where k is a field with $\mathrm{char}(k) \neq 2, 3$ and $f(X) \in k[X]$ is a separable polynomial of degree 3. Then there is a bijection*

$$\{(x, y) \in k^2 \mid y^2 = f(x)\} \cup \{\infty\} \to \mathrm{Cl}_A, \qquad (x, y) \mapsto \mathfrak{p}_{x,y} := (X - x, Y - y) \mapsto [(X - x, Y - y)],$$

where the $\mathfrak{p}_{x,y} \subset A$ are prime ideals.

Remark 7.49. As formulating and disproving conjectures in research mathematics is founded on evidence, there are often times huge databases containing all sorts of information on concrete examples. In the realm of number theory, such a database is [LMF]. For example, we can search for algebraic number fields as mentioned above under the category *Fields → Number fields*.

If we search for quadratic *CM fields* of degree 2 with class number 1, we indeed obtain a list of nine number fields, consistent with the Stark-Heegner theorem 7.45. On the other hand, if we are searching for non-CM fields of degree 2 with class number 1, we obtain a staggering number of (currently) 177 159 number fields, supporting the conjecture for the class number problem 7.46.

7.8 The Splitting of Primes

Lect. 23
10.07.23

Recall the main theorem on Dedekind rings (Theorem 7.36): Let A be a Dedekind ring, and let $(0) \neq \mathfrak{a} \subseteq A$ be an ideal. Then there exists a unique factorisation $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ into prime ideals $(0) \neq \mathfrak{p}_i \subset A$ with $\mathfrak{p}_i \neq \mathfrak{p}_j$ for all $i \neq j$ and $e_i \geq 1$ for all i.

Observation 7.50. Let $A \subseteq B$ be a finite ring extension of Dedekind rings (like $\mathbb{Z} \subseteq \mathcal{O}_K$), and let $(0) \neq \mathfrak{p} \subset A$ be prime ideal. By the prime factorisation in Dedekind rings (Theorem 7.36), we may factor

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

into prime ideals in B with $\mathfrak{P}_i \neq \mathfrak{P}_j$ for all $i \neq j$ and $e_i \geq 1$. Since Dedekind rings are one-dimensional by definition, we have $\mathfrak{P}_i \not\subseteq \mathfrak{P}_j$ for all $i \neq j$, i. e. they are all maximal, implying $\mathfrak{P}_i + \mathfrak{P}_j = B$ for all $i \neq j$. So the Chinese remainder theorem 8.5 yields

$$B/\mathfrak{p}B = B/\mathfrak{P}_1^{e_1} \times \cdots \times B/\mathfrak{P}_r^{e_r}$$

In each component $B/\mathfrak{P}_i^{e_i}$, the only prime ideal in B containing $\mathfrak{P}_i^{e_i}$ is $\mathfrak{P}_i$ (recall from Exercise 8.52 that prime ideals in the product are of the form $B \times \cdots \times \mathfrak{P}_i \times \cdots \times B$). Hence we have a bijection

$$\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\} \cong \operatorname{Spec}(B/\mathfrak{p}B) \cong \{\mathfrak{P} \in \operatorname{Spec}(B) \mid \mathfrak{p} \subseteq \mathfrak{P}\}.$$

We deduce that $\mathfrak{p} \subseteq \mathfrak{P}_i \cap A$ for all $i = 1, \ldots, r$. Again because of $\dim(A) = 1$, $\mathfrak{p}$ is maximal and we have $\mathfrak{p} = \mathfrak{P}_i \cap A$ for all $i = 1, \ldots, r$.

Conversely, let $(0) \neq \mathfrak{P} \subset B$ be a prime and maximal ideal. By finiteness of $A \subseteq B$ and by Corollary 5.13, $\mathfrak{p} \coloneqq \mathfrak{P} \cap A$ is a prime and maximal ideal of A. Hence $\mathfrak{P} \mid \mathfrak{p}B$ by what was said before (we have $\mathfrak{p} \subseteq \mathfrak{P}$, so $\mathfrak{P} \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$).

Thus the following definition applies to all $(0) \neq \mathfrak{P} \subset B$.

Definition 7.51. Let $A \subseteq B$ be a finite ring extension of Dedekind rings. Let $(0) \neq \mathfrak{P} \subset B$ be a prime ideal, and let $\mathfrak{p} \coloneqq \mathfrak{P} \cap A$ be a prime ideal in A. Assume that $\mathfrak{p}B = \mathfrak{P}^e\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ is the **splitting** of $\mathfrak{p}$ in B with $\mathfrak{P}_i \neq \mathfrak{P}$ and $e, e_i \geq 1$ for all $i = 1, \ldots, r$. We define $e(\mathfrak{P}) \coloneqq e$ as the **ramification index** of $\mathfrak{P}$. We call $f(\mathfrak{P}) \coloneqq [B/\mathfrak{P} : A/\mathfrak{p}]$ the **inertia degree** of $\mathfrak{P}$, which is the degree of the finite field extension $(B/\mathfrak{P})/(A/\mathfrak{p})$.

Remark 7.52. Why do we call it *ramification*? Consider the ring extension $A = \mathbb{C}[t] \subseteq B = \mathbb{C}[z]$, given by $t = z^e$. Then for $\mathfrak{p} = (t)$, we have $\mathfrak{p}B = (z)^e$. The ring extension $A \subseteq B$ corresponds to the complex map $\mathbb{C} \leftarrow \mathbb{C}$, $z^e \leftarrow\!\shortmid z$ (see Example 5.18). The number e describes the number of branches on the Riemann surface of the map $t \mapsto t^{1/e}$ near $t = 0$.

Proposition 7.53. *Let $A \subseteq B$ be a finite ring extension of Dedekind rings. Put $K \coloneqq \operatorname{Quot}(A)$ and $L \coloneqq \operatorname{Quot}(B)$. Given a prime ideal $(0) \neq \mathfrak{p} \subset A$ and a splitting $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, then*

$$\sum_{i=1}^{r} e_i f_i = [L : K],$$

where $e_i = e(\mathfrak{P}_i)$ and $f_i \coloneqq f(\mathfrak{P}_i)$ for all $i = 1, \ldots, r$.

Remark 7.54. (From me.) A maybe useful statement: Let $A \subseteq B$ be a finite ring extension of integral domains. Then $\operatorname{Quot}(B) = (A \setminus \{0\})^{-1}B$.

Proof: Put $S \coloneqq A \setminus \{0\}$. Since $\operatorname{Quot}(A) = S^{-1}A \subseteq S^{-1}B$ is also finite, and since $\operatorname{Quot}(A)$ is a field and $S^{-1}B$ an integral domain, $S^{-1}B$ is a field as well by Proposition 5.12. We thus have $B \subseteq S^{-1}B \subseteq \operatorname{Quot}(B)$. By definition, $\operatorname{Quot}(B)$ is the smallest field containing B, hence $S^{-1}B = \operatorname{Quot}(B)$.

Proof. We know that $A_\mathfrak{p}$ is a discrete valuation ring. Let $B_\mathfrak{p} \coloneqq (A \setminus \mathfrak{p})^{-1}B$, which is finite ($A \subseteq B$ is finite) and torsion-free ($B_\mathfrak{p} \subseteq L$ is a subring of a field) as an $A_\mathfrak{p}$-module. Say $B_\mathfrak{p} \cong A_\mathfrak{p}^{\oplus d}$ by the structure theorem 3.52 (recall that $A_\mathfrak{p}$ is a local principal ideal domain, Theorem 7.23). Then, by the Chinese remainder theorem 8.5,

$$[L : K] = d = \dim_{A/\mathfrak{p}}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \dim_{A/\mathfrak{p}}(B/\mathfrak{P}_1^{e_1} \times \cdots \times B/\mathfrak{P}_r^{e_r}) = \sum_{i=1}^{r} \dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}).$$

Here, the first equality follows from tensoring $B_\mathfrak{p} \cong A_\mathfrak{p}^{\oplus d}$ with $K = \operatorname{Quot}(A)$. With Remark 7.54, we then obtain the following chain of isomorphisms of K-vector spaces:

$$L = (A \setminus \{0\})^{-1}B \cong B_\mathfrak{p} \otimes_{A_\mathfrak{p}} K \cong A_\mathfrak{p}^{\oplus d} \otimes_{A_\mathfrak{p}} K \cong K^{\oplus d}$$

The second equality follows from tensoring $B_\mathfrak{p} \cong A_\mathfrak{p}^{\oplus d}$ with $A/\mathfrak{p}$. Using Corollary 4.55, we obtain $B/\mathfrak{p}B = B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ and similarly for $A/\mathfrak{p}$ (also used in the third equality), whence a chain of isomorphisms of $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong A/\mathfrak{p}$-vector spaces follows:

$$B/\mathfrak{p}B = B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \cong B_\mathfrak{p} \otimes_{A_\mathfrak{p}} A/\mathfrak{p} \cong A_\mathfrak{p}^{\oplus d} \otimes_{A_\mathfrak{p}} A/\mathfrak{p} \cong (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})^{\oplus d} = (A/\mathfrak{p})^{\oplus d}.$$

It remains to see $\dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}) = e_i f_i$. Since B is a Dedekind ring, $B_{\mathfrak{P}_i}$ is a discrete valuation ring and, in particular, a principal ideal domain. Due to Exercise 8.10, we know that for all $n \geq 0$, $(\mathfrak{P}_i B_{\mathfrak{P}_i})^n/(\mathfrak{P}_i B_{\mathfrak{P}_i})^{n+1}$ is a one-dimensional $B_{\mathfrak{P}_i}/\mathfrak{P}_i B_{\mathfrak{P}_i}$-vector space. If we apply the homomorphism theorem to the canonical map $\mathfrak{P}_i^n \to (\mathfrak{P}_i B_{\mathfrak{P}_i})^n/(\mathfrak{P}_i B_{\mathfrak{P}_i})^{n+1}$, we obtain $\mathfrak{P}_i^n/\mathfrak{P}_i^{n+1} \cong (\mathfrak{P}_i B_{\mathfrak{P}_i})^n/(\mathfrak{P}_i B_{\mathfrak{P}_i})^{n+1}$ as $B/\mathfrak{P}_i$-vector spaces. Thus $\dim_{B/\mathfrak{P}_i}(\mathfrak{P}_i^n/\mathfrak{P}_i^{n+1}) = 1$ for all $n \geq 0$. By induction, the dimension formula for quotient spaces as well as Noether's isomorphism theorem give

$$\begin{aligned}\dim_{B/\mathfrak{P}_i}(B/\mathfrak{P}_i^{e_i}) &= \dim_{B/\mathfrak{P}_i}((B/\mathfrak{P}_i^{e_i})/(\mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i})) + \dim_{B/\mathfrak{P}_i}(\mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i}) \\ &= \dim_{B/\mathfrak{P}_i}(B/\mathfrak{P}_i^{e_i-1}) + 1 = (e_i - 1) + 1\end{aligned}$$

(note that $B/\mathfrak{P}_i^0 = B/B = 0$). By definition, $f_i = \dim_{A/\mathfrak{p}}(B/\mathfrak{P})$, thus $\dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}) = e_i f_i$. □

How can we understand and compute $e(\mathfrak{P})$ and $f(\mathfrak{P})$?

Proposition 7.55 (Dedekind-Kummer theorem). *Let $A \subseteq B$ be a finite ring extension of Dedekind rings. Put $K := \mathrm{Quot}(A)$ and $L := \mathrm{Quot}(B)$. Assume that B is **monogenic**, i. e. $B = A[\alpha]$ for some $\alpha \in L$. Let $g(T) := \min_{L/K}(\alpha, T) \in A[T]$ (Proposition 7.5).*

Let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal. Then the following are equivalent:

(i) *$\mathfrak{p}B$ splits as $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ in B with non-zero prime ideals $\mathfrak{P}_i \neq \mathfrak{P}_j$ for all $i \neq j$ and $e_i \geq 1$.*

(ii) *$\bar{g} := g \bmod \mathfrak{p}$ factors as $\bar{g} = g_1^{e_1} \cdots g_r^{e_r}$ in $(A/\mathfrak{p})[T]$ with irreducible g_i of degree $f_i = f(\mathfrak{P}_i)$ such that $(g_i) \neq (g_j)$ for all $i \neq j$.*

In fact, we can match $\mathfrak{P}_i$ and g_i by $\mathfrak{P}_i = \mathfrak{p}B + (\tilde{g}_i(\alpha))$ where $\tilde{g}_i \in A[T]$ is any lift of g_i.

Proof. $B = A[\alpha]$ implies $B \cong A[T]/(g(T))$. Thus, by Remark 2.3 and by the Chinese remainder theorem 8.5,

$$\prod_{j=1}^{s} B/\mathfrak{P}_j^{e_j'} \cong B/\mathfrak{p}B \cong A[T]/(\mathfrak{p}A[T] + (g)) \cong (A/\mathfrak{p})[T]/(\bar{g}) \cong \prod_{i=1}^{r} (A/\mathfrak{p})[T]/(g_i)^{e_i}, \tag{7.56}$$

where $\bar{g} = g_1^{e_1} \cdots g_r^{e_r}$ is the prime factorisation of $\bar{g} = g \bmod \mathfrak{p}$ (the factorisation exists since $(A/\mathfrak{p})[T]$ is a principal ideal domain), and where $\mathfrak{p}B = \mathfrak{P}_1^{e_1'} \cdots \mathfrak{P}_s^{e_s'}$ is a splitting of $\mathfrak{p}B$. We immediately see that $s = |\mathrm{Spec}(B/\mathfrak{p}B)| = r$ for the only prime ideal in $(A/\mathfrak{p})[T]/(g_i)^{e_i}$ is (g_i) for each i.

(Adapted from [Sut].) We next show that there is the equality of sets

$$\{\mathfrak{p}B + (\tilde{g}_i(\alpha)) \mid i = 1, \dots, r\} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}.$$

Observe that the (g_i) are pairwise different in $(A/\mathfrak{p})[T]/(\bar{g}) \cong A[T]/\mathfrak{p}A[T] + (g) \cong B/\mathfrak{p}B$, hence the $(\tilde{g}_i(\alpha))$ mod $\mathfrak{p}B$ and thus the $\mathfrak{p}B + (\tilde{g}_i(\alpha))$ are resp. pairwise different. Moreover, by Remark 2.3,

$$B/(\mathfrak{p}B + (\tilde{g}_i(\alpha))) \cong A[T]/(\mathfrak{p}A[T] + (g, \tilde{g}_i)) \cong (A/\mathfrak{p})[T]/(g_i) \tag{7.57}$$

since $g_i \mid \bar{g}$. As (g_i) is prime in $(A/\mathfrak{p})[T]$, the quotient rings are integral domains and $\mathfrak{p}B + (\tilde{g}_i(\alpha)) \in \mathrm{Spec}(B/\mathfrak{p}B)$. W. l. o. g. assume that $\mathfrak{p}B + (\tilde{g}_i(\alpha)) = \mathfrak{P}_i$ for all $i = 1, \dots, r$.

Lastly, we show that $e_i = e_i'$ and $\deg(g_i) = f_i = f(\mathfrak{P}_i)$ for all $i = 1, \dots, r$. (7.57) actually says a lot more: Since g_i is irreducible and (g_i) is even a maximal ideal, $(A/\mathfrak{p})[T]/(g_i)$ is a field extension of the field $A/\mathfrak{p}$, and its degree is $\deg(g_i)$. Thus

$$f(\mathfrak{P}_i) = [B/\mathfrak{P}_i : A/\mathfrak{p}] = [(A/\mathfrak{p})[T]/(g_i) : A/\mathfrak{p}] = \deg(f_i).$$

Consider the ideal $\mathfrak{q} := \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \prod_{i=1}^r (\mathfrak{p}B + (\tilde{g}_i(\alpha)))^{e_i}$. Distributing this product, we see that $\mathfrak{q} \subseteq \mathfrak{p}B$ since every summand has either one factor $\mathfrak{p}B$ or is generated by $\tilde{g}_1(\alpha)^{e_1} \cdots \tilde{g}_r(\alpha)^{e_r} \equiv g(\alpha) \equiv 0 \bmod \mathfrak{p}B$. Hence $e_i \leq e_i'$ for all i in order for $\mathfrak{q} \subseteq \mathfrak{p}B = \mathfrak{P}_1^{e_1'} \cdots \mathfrak{P}_r^{e_r'}$ to hold (this follows from the unique splitting of $\mathfrak{p}B$).

(From me.) Returning back to (7.56), we know from the proof in Proposition 7.53 that the $A/\mathfrak{p}$-dimension of the left-hand side is $\sum_{i=1}^{r} e_i' f_i$. With a similar argument as in Proposition 7.53, we can argue that the $A/\mathfrak{p}$-dimension of the right-hand side is $\sum_{i=1}^{r} e_i f_i$ (this time, we can apply Exercise 8.10 directly to the principal ideal domain $(A/\mathfrak{p})[T]$). Hence $\sum_{i=1}^{r} e_i' f_i = \sum_{i=1}^{r} e_i f_i$ if and only if $e_i = e_i'$. □

Example 7.58. Consider $A = \mathbb{Z} \subseteq B = \mathbb{Z}[\alpha] \cong \mathbb{Z}[T]/(T^3 - 2)$ with $\alpha^3 = 2$, which is a Dedekind ring extension (cf. Example 7.11). Consider the prime ideals $\mathfrak{p} = (2), (3), (5) \subseteq \mathbb{Z}$. Then we have

(i) $T^3 - 2 \equiv T^3 \mod (2)$, so $2B = (2, \alpha)^3 = (\alpha)^3$ (we have $\alpha^3 = 2$).

(ii) $T^3 - 2 \equiv (T-2)^3 \mod (3)$ (we used the Frobenius endomorphism and $n^p \equiv n \mod (p)$ for all $n \in \mathbb{Z}$ and prime numbers p). Then $3B = (3, \alpha - 2)^3$ (actually a principal ideal).

(iii) $T^3 - 2 \equiv (T-3)(T^2+3T-1) \mod (5)$, which is a prime factorisation. Thus $5B = (5, \alpha-3)(5, \alpha^2+3\alpha-1)$. Here, $e = f = 1$ for the left factor, and $e = 1$ and $f = 2$ for the right factor.

As it turns out, the splitting of a prime ideal $(0) \neq \mathfrak{p} \subset A$ is most of the time pretty 'flat', i. e. the ramification indices are 1. We will make this precise with the following definition.

Definition 7.59. Let $A \subseteq B$ be a finite ring extension of Dedekind rings. We say that a prime ideal $(0) \neq \mathfrak{p} \subset A$ **ramifies** in B if there exists some prime ideal $\mathfrak{P} \mid \mathfrak{p}B$ in B such that $e(\mathfrak{P}) \geq 2$.

Proposition 7.60. *Let $A \subseteq B$ be a finite ring extension of Dedekind rings. Put $K \coloneqq \mathrm{Quot}(A)$ and $L \coloneqq \mathrm{Quot}(B)$. If L/K is separable, then only finitely many prime ideals of A ramify in B.*

Proof.

(i) We proof the monogenic case first. Assume that $B \cong A[T]/(g)$ for some irreducible polynomial $g(T) \in A[T]$. Then also $L \cong K[T]/(g)$ by Remark 7.54. Since L/K is separable by assumption, $g \in K[T]$ is separable, i. e. it has no multiple roots in $\overline{K}$. By [Sch, Cor. 6.20], this is equivalent to g and g' being coprime in $K[T]$, i. e. $(g, g') = K[T]$ (g' denotes the formal derivative of g). Thus there are $h_1, h_2 \in K[T]$ such that $h_1 g + h_2 g' \in K^\times$. By clearing denominators, we may assume that $h_1, h_2 \in A[T]$, thus $a \coloneqq h_1 g + h_2 g' \in A \setminus \{0\}$.

There are only finitely many prime ideals $\mathfrak{p} \subset A$ that contain $(a) \neq (0)$ (see the proof of Theorem 7.36); these might ramify. For all other prime ideals $(0) \neq \mathfrak{q} \subset A$ with $a \notin \mathfrak{q}$ (if any), we have $(\bar{g}, \bar{g}') = (A/\mathfrak{q})[T]$ since $A/\mathfrak{q}$ is a field and thus $\bar{a} \in (A/\mathfrak{q})^\times = (A/\mathfrak{q})[T]^\times$. This means that $\bar{g} = g \bmod \mathfrak{q}$ is separable over $A/\mathfrak{q}$, so each irreducible factor of $\bar{g}$ has multiplicity 1. By the Dedekind-Kummer theorem 7.55, for each prime ideal $\mathfrak{Q} \mid \mathfrak{q}B$, it must be $e(\mathfrak{Q}) = 1$.

(ii) In the general case, by the primitive element theorem for the finite separable L/K, pick a primitive element $\alpha \in L$ such that $L = K(\alpha)$. By multiplying with the denominator, we may assume that $\alpha \in B$. Consider $A[\alpha] \subseteq B$. By assumption, B is finite over A, say $B = (b_1, \ldots, b_n)$ as an A-module. Then every b_i is of the form $b_i = x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1}$ with $x_j \in K$ and $d \coloneqq [L : K]$. We can clear denominators, i. e. there exists some $0 \neq s_i \in A$ such that $s_i b_i \in A[\alpha]$ for all $i = 1, \ldots, n$. Setting $0 \neq s \coloneqq s_1 \cdots s_n \in A$, we conclude that $sB \subseteq A[\alpha] \subseteq B$, implying $B[s^{-1}] \subseteq A[\alpha, s^{-1}] \subseteq B[s^{-1}]$.

So $A[s^{-1}] \subseteq B[s^{-1}]$ is a monogenic finite Dedekind ring extension, and we reduced the general case to the monogenic case. Thus only finitely many prime ideals $(0) \neq \mathfrak{p} \subset A[s^{-1}]$ ramify in $B[s^{-1}]$. As in the proof of Theorem 7.36, only finitely many prime ideals $\mathfrak{p} \subset A$ contain $s \neq 0$. Since the $\mathfrak{p} \subset A[s^{-1}]$ are precisely the prime ideals $\mathfrak{p} \subset A$ with $s \notin \mathfrak{p}$, in total, only finitely many prime ideals in A ramify in B. □

Example 7.61. Let $d \in \mathbb{Z}$ be square-free, and consider the finite ring extension $\mathbb{Z} \subseteq \mathcal{O}_K$ for $K \coloneqq \mathbb{Q}(\sqrt{d})$. We know that $\mathbb{Z} \subseteq \mathcal{O}_K$ is monogenic, and the minimal polynomial over $\mathbb{Q}$ of the primitive element is

$$g(T) \coloneqq \begin{cases} T^2 - d, & \text{if } d \equiv 2, 3 \mod (4), \\ T^2 - T + \dfrac{1-d}{4}, & \text{if } d \equiv 1 \mod (4) \end{cases}$$

(cf. Example 7.31). Then $\mathcal{O}_K \cong \mathbb{Z}[T]/(g(T))$. The *discriminant* of g is

$$D = \begin{cases} 4d, & \text{if } d \equiv 2,3 \mod (4), \\ d, & \text{if } d \equiv 1 \mod (4) \end{cases}$$

(recall that for a general quadratic polynomial $aT^2+bT+c \in \mathbb{Q}[T]$, the discriminant is defined as $D = b^2-4ac$).

Thus a prime number $p \in \mathbb{Z}$, or, more precisely, a prime ideal $(p) \subset \mathbb{Z}$, ramifies in $\mathcal{O}_K$ if and only if $g \bmod (p)$ is not separable, see the Dedekind-Kummer theorem 7.55. This happens if and only if the discriminant vanishes, i. e. $p \mid D$ (recall that we can factor a quadratic as $(x+y\sqrt{D})(x-y\sqrt{D})$ for suitable $x, y \in \mathbb{Q}$).

We now look at the symmetries of the splitting of primes.

Lemma 7.62 (prime avoidance lemma, [AtMac, Prop. 1.11]**).** *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subset A$ be prime ideals with $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ for all $i \neq j$, and let $\mathfrak{a} \subseteq A$ be an ideal with $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ for all $i = 1, \dots, r$. Then $\mathfrak{a} \nsubseteq \bigcup_{i=1}^r \mathfrak{p}_i$.*

Proof. We induct on r. The case $r = 1$ is trivial. Suppose $r > 1$. Then for each i, by the induction hypothesis, there exists some $x_i \in \mathfrak{a} \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. If we have $x_i \notin \mathfrak{p}_i$ for some i, then we are done. Otherwise $x_i \in \mathfrak{p}_i$ for all i. Then $\sum_{i=1}^r x_1 \cdots x_{i-1} x_{i+1} \cdots x_r \in \mathfrak{a} \setminus \bigcup_{i=1}^r \mathfrak{p}_i$, and we are also done. □

The following holds not only for Dedekind ring extensions.

Proposition 7.63. *Let $A \subseteq B$ be a finite ring extension. Let G be a finite group acting on B by ring automorphisms such that $A = B^G$ for the G-invariants. If $\mathfrak{P}_1, \mathfrak{P}_2 \subset B$ are prime ideals such that $\mathfrak{P}_1 \cap A = \mathfrak{P}_2 \cap A =: \mathfrak{p}$, then there is some $\sigma \in G$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. In other words: Given a prime ideal $\mathfrak{p} \subset A$, the action of G on all prime ideals above $\mathfrak{p}$ is transitive.*

Proof. First we note that for any prime ideal $\mathfrak{P} \subset B$, the sets $\sigma(\mathfrak{P})$ are prime ideals for all $\sigma \in G$ too. The reason is that each σ induces a ring automorphism on B.

Also, $\mathfrak{p} = (0)$ is not a problem since this implies $\mathfrak{P}_1 = \mathfrak{P}_2 = (0)$.

According to Exercise 8.43, there are only finitely many prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r \subset B$ containing $\mathfrak{p}$. By assumption, $A \subseteq B$ is also integral, so Corollary 5.14 implies that $\mathfrak{P}_i \nsubseteq \mathfrak{P}_j$ for all $i \neq j$. By the prime avoidance lemma 7.62, there exists an $x \in \mathfrak{P}_1 \setminus (\mathfrak{P}_2 \cup \cdots \cup \mathfrak{P}_r)$. It follows that for all $\sigma \in G$, we have $\sigma(x) \in \sigma(\mathfrak{P}_1) \setminus (\sigma(\mathfrak{P}_2) \cup \cdots \cup \sigma(\mathfrak{P}_r))$ (reason being that σ is invertible, and that taking preimages distributes over taking unions and intersections of sets).

Now observe that the *norm* $N := \prod_{\sigma \in G} \sigma(x)$ is G-invariant since for each $\sigma \in G$, left-multiplication $\sigma \colon G \to G$ is bijective on G. Moreover, the product N contains $1(x) = x$ with the identity $1 \in G$, hence $N \in \mathfrak{P}_1$. Hence $N \in \mathfrak{P}_1 \cap B^G = \mathfrak{P}_1 \cap A = \mathfrak{p}$. Thus for every i, we obtain $N \in \mathfrak{p} \subseteq \mathfrak{P}_i$, so by the prime ideal property, there exists some $\sigma \in G$ such that $\sigma(x) \in \mathfrak{P}_i$. Observe that $\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P}_1 \cap A) = \sigma(\mathfrak{P}_1) \cap A$, so $\sigma(\mathfrak{P}_1) \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. Since $\sigma(x)$ only lies in $\sigma(\mathfrak{P}_1)$, but not in $\sigma(\mathfrak{P}_2), \dots, \sigma(\mathfrak{P}_r)$, we necessarily have $\mathfrak{P}_i = \sigma(\mathfrak{P}_1)$. □

Corollary 7.64. *Let $A \subseteq B$ be a finite ring extension of Dedekind rings. Put $K := \operatorname{Quot}(A)$ and $L := \operatorname{Quot}(B)$. Assume that L/K is a Galois extension. Let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal, and let $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ be its splitting. Then $e_1 = \cdots = e_r$ and $f(\mathfrak{P}_1) = \cdots = f(\mathfrak{P}_r)$.*

Proof. First note that L/K is finite as $A \subseteq B$ is finite. From [Sch, Thm. 7.8], we know that $G := \operatorname{Gal}(L/K)$ is a finite group with $L^G = K$. Similarly to Exercise 8.58, we can show that B is stable under the action of G on L, and $B^G = A$.

For every $\sigma \in G$, we obtain a factorisation

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \mathfrak{p}B = \sigma(\mathfrak{p}B) = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r},$$

where $\mathfrak{p}B = \sigma(\mathfrak{p}B)$ because $\sigma(\mathfrak{p}B) = \{\sigma(p)\sigma(b) \mid p \in \mathfrak{p}, b \in B\}$, $\mathfrak{p} \subset A = B^G$ and σ is an automorphism. By uniqueness of the factorisation (Theorem 7.36), we have $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$ for some i, implying $e_1 = e_i$. Proposition 7.63 says that G acts transitively on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. So for any $\mathfrak{P}_i \neq \mathfrak{P}_j$, we pick some $\sigma \in G$ such that $\mathfrak{P}_i = \sigma(\mathfrak{P}_j)$, and by the above reasoning, $e_i = e_j$. This gives $e_1 = \cdots = e_r$.

Continuing the line of thought, go back to the point where $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$ for some i. Then the isomorphism $\sigma \colon B \to B$ induces an isomorphism $B/\mathfrak{P}_1 \to B/\sigma(\mathfrak{P}_1) = B/\mathfrak{P}_i$, hence $f_1 = [B/\mathfrak{P}_1 : A/\mathfrak{p}] = [B/\mathfrak{P}_i : A/\mathfrak{p}] = f_i$. By the same reasoning as above, we have $f_1 = \cdots = f_r$. □

Remark 7.65. (From me.) In this case, the splitting reads as

$$\mathfrak{p}B = \left(\prod_{\sigma \in G} \sigma(\mathfrak{P}) \right)^e$$

for any $\mathfrak{P} \in \operatorname{Spec}(B/\mathfrak{p}B)$ and suitable $e \geq 1$.

Remark 7.66. (Form me.) Instead of assuming that L/K being Galois, we can take the same assumptions as in Proposition 7.63, namely let G be a finite group acting on B by ring automorphisms such that $B^G = A$. We can then extend the group action to L and observe that $L^G = K$. By [Sch, Thm. 7.6] (a result due to Artin), this already implies that L/K is Galois with $G = \operatorname{Gal}(L/K)$.

This is a funny criterion to check whether the corresponding field extension of a Dedekind ring extension is Galois.

7.9 Quadratic Norm Equations

Lect. 24
13.07.23

For the final few subsections, we want to combine everything we have learned about Dedekind rings, prime splittings and the ideal class group in order to solve *quadratic norm equations*. We already solved such a quadratic norm equation: Recall from Proposition 1.55 that $Z[\mathrm{i}]$ is a principal ideal domain. Then we deduced in Theorem 2.5 that $x^2 + y^2 = p$ has a solution if and only if $p \equiv 1, 2 \mod (4)$. We will see that $p \neq 2$ splits in $\mathbb{Z}[\mathrm{i}]$ if and only if $p \equiv 1 \mod (4)$.

Observation 7.67. Let $d \in \mathbb{Z}$ be square-free, $K \coloneqq \mathbb{Q}(\sqrt{d})$, and let $\mathcal{O}_K \subseteq K$ be the ring of integers. In this setting, we know that the norm over $K/\mathbb{Q}$ is

$$N = N_{K/\mathbb{Q}} \colon K \to \mathbb{Q}, \qquad x + y\sqrt{d} \mapsto x^2 - dy^2 \quad \text{with } x, y \in \mathbb{Q}.$$

It restricts to a function $N \colon \mathcal{O}_K \to \mathbb{Z}$ which defines a quadratic form in two variables $x, y \in \mathbb{Z}$. More concretely, if we set

$$\alpha \coloneqq \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3 \mod (4), \\ \dfrac{1 + \sqrt{d}}{2}, & \text{if } d \equiv 1 \mod (4), \end{cases}$$

then $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha$ as a $\mathbb{Z}$-module. In this basis, the norm is given by

$$N(x + y\alpha) = \begin{cases} x^2 - dy^2, & \text{if } d \equiv 2, 3 \mod (4), \\ x^2 + xy + \dfrac{1-d}{4} y^2, & \text{if } d \equiv 1 \mod (4), \end{cases} \in \mathbb{Z}[x, y]. \tag{7.68}$$

Problem 7.69. The basic question is: For which $n \in \mathbb{Z}$ can we solve $N(z) = n$ with $z \in \mathcal{O}_K$? This equation is called the **norm equation** for $\mathcal{O}_K$ and is part of *Diophantine geometry*, i. e. the study of polynomial equations over $\mathbb{Z}$.

Lemma 7.70. *Let $K/\mathbb{Q}$ be a number field. Let $(0) \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal with prime factorisation $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then the following quantities agree:*

(i) *The cardinality $|\mathcal{O}_K/\mathfrak{a}|$.*

(ii) *The product $p_1^{e_1 f_1} \cdots p_r^{e_r f_r}$ where $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$ and $f_i \coloneqq f(\mathfrak{p}_i) = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_{p_i}]$.*

(iii) *The unique integer $\mathcal{N}(\mathfrak{a}) \in \mathbb{Z}_{>0}$ such that $(\mathcal{N}(\mathfrak{a})) = (N_{\mathcal{O}_K/\mathbb{Z}}(a) \mid a \in \mathfrak{a})$ (which is like the greatest common divisor).*

*We denote any quantity above by $\mathcal{N}(\mathfrak{a})$ and call it the **norm** of $\mathfrak{a}$.*

Proof. (From me.)

- (i) = (ii): In the proof of Proposition 7.53, we have seen that $\dim_{\mathbb{Z}/p_i}(\mathcal{O}_K/\mathfrak{p}_i^{e_i}) = e_i f_i$. Thus by the Chinese remainder theorem 8.5, we have

$$|\mathcal{O}_K/\mathfrak{a}| = \prod_{i=1}^r |\mathcal{O}_K/\mathfrak{p}_i^{e_i}| = \prod_{i=1}^r |\mathbb{Z}/p_i|^{\dim_{\mathbb{Z}/p_i}(\mathcal{O}_K/\mathfrak{p}_i^{e_i})} = \prod_{i=1}^r p_i^{e_i f_i}.$$

- (i) = (iii): (This equality is missing. Any idea would be welcomed. I think one has to use that for principal ideals, $\mathcal{N}((\alpha)) = |N_{\mathcal{O}_K/\mathbb{Z}}(\alpha)| = |\mathcal{O}_K/\alpha\mathcal{O}_K|$. Then, somehow, consider each principle ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ for prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ in the discrete valuation ring.) □

Definition 7.71. We generalise the definition of the norm map $N\colon \mathcal{O}_K \to \mathbb{Z}$ from (7.68) to ideal classes of $\mathcal{O}_K$: Let $K/\mathbb{Q}$ be a number field. For all ideals $(0) \neq \mathfrak{a} \subseteq \mathcal{O}_K$, we define

$$N_{\mathfrak{a}}\colon \mathfrak{a} \to \mathbb{Z}, \qquad z \mapsto N(z)/\mathcal{N}(\mathfrak{a}) \in \mathbb{Z}.$$

Notice that this is well-defined since by Lemma 7.70, $\mathcal{N}(\mathfrak{a}) \mid N(z)$ for all $z \in \mathfrak{a}$.

Remark 7.72. Like N, the norm $N_{\mathfrak{a}}$ defines a quadratic form in two variables over $\mathbb{Z}$. Observe that up to a $\mathbb{Z}$-linear change of coordinates, $N_{\mathfrak{a}}$ only depends on the coset $[\mathfrak{a}] \in \mathrm{Cl}_{\mathcal{O}_K}$. The reason is that two ideals in this cosets differ only by some principal ideal factor $(\pi) \subseteq \mathcal{O}_K$, and in the definition of $N_{\mathfrak{a}}$, we have $N(\pi z)/\mathcal{N}(\pi\mathfrak{a}) = N(z)/\mathcal{N}(\mathfrak{a})$ (both norms are multiplicative).

Example 7.73. Consider $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. As mentioned in Example 7.43, in fact we have $h_K = 2$ and $\mathrm{Cl}_{\mathbb{Z}[\sqrt{-5}]} = \{[\mathbb{Z}[\sqrt{-5}]], [(2, 1+\sqrt{-5})]\}$. We want to calculate the norm w. r. t. the ideal classes.

(i) We already know $N_{\mathcal{O}_K}(x + y\sqrt{-5}) = x^2 + 5y^2$.

(ii) Let $\mathfrak{a} := (2, 1+\sqrt{-5})$. What about $N_{\mathfrak{a}}$? For this, we need a $\mathbb{Z}$-basis of $\mathfrak{a}$. Since $\mathfrak{a} = (2, 1+\sqrt{-5})$ as a $\mathbb{Z}[\sqrt{-5}]$-module, we have

$$\mathfrak{a} = (2, 1+\sqrt{-5}, 2\cdot\sqrt{-5}, (1+\sqrt{-5})\cdot\sqrt{-5} = -5+\sqrt{-5}) = (2, 1+\sqrt{-5})$$

as a $\mathbb{Z}$-module. Furthermore, $\mathcal{N}(\mathfrak{a}) = \gcd(N(2), N(1+\sqrt{-5})) = 2$. Thus

$$N_{\mathfrak{a}}(2x + (1+\sqrt{-5})y) = \frac{4x^2 + 4xy + 6y^2}{2} = 2x^2 + 2xy + 3y^2.$$

Note that in both norm equations, it is not a coincidence that the discriminant of the bivariate polynomial is -20 (i. e. the discriminant of the quadratic polynomial that we obtain when setting $x = 1$ or $y = 1$).

We now restrict to norm equations $N_{\mathfrak{a}}(z) = p$ with a prime number $p \in \mathbb{Z}$.

Proposition 7.74. *Let $K/\mathbb{Q}$ be a number field. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal, and let $p \in \mathbb{Z}$ be a prime number. Then $N_{\mathfrak{a}}(z) = \pm p$ has a solution $z \in \mathfrak{a}$ if and only if $p\mathcal{O}_K \in \{\mathfrak{p}^2, \mathfrak{p}\bar{\mathfrak{p}}\}$ with $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $[\mathfrak{p}] \in \{[\mathfrak{a}], [\mathfrak{a}]^{-1}\}$ in $\mathrm{Cl}_{\mathcal{O}_K}$.*

Proof. Assume that $z \in \mathfrak{a}$ such that $N_{\mathfrak{a}}(z) = \pm p$. Since $|N(z)| = \mathcal{N}((z))$, by definition, we obtain $p = |N_{\mathfrak{a}}(z)| = \mathcal{N}((z))/\mathcal{N}(\mathfrak{a}) = \mathcal{N}(z\mathfrak{a}^{-1})$. Note that $z\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ since $(z) \subseteq \mathfrak{a}$. So by Lemma 7.70, $\mathfrak{p} := z\mathfrak{a}^{-1}$ is prime with $\mathfrak{p} \mid p\mathcal{O}_K$ and $f(\mathfrak{p}) = 1$. As $[K : \mathbb{Q}] = 2$, Proposition 7.53 implies that either $p\mathcal{O}_K = \mathfrak{p}^2$ (in this case, $2 = e(\mathfrak{p})f(\mathfrak{p}) = 2\cdot 1$) or $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \neq \bar{\mathfrak{p}} \subset \mathcal{O}_K$ (in this case, $2 = e(\mathfrak{p})f(\mathfrak{p}) + e(\bar{\mathfrak{p}})f(\bar{\mathfrak{p}}) = 1+1$). We obtain $(z) = \mathfrak{p}\mathfrak{a}$, hence $[\mathfrak{p}] = [(z)]\cdot[\mathfrak{a}^{-1}] = [\mathfrak{a}^{-1}] = [\mathfrak{a}]^{-1}$ in both cases, and $[\bar{\mathfrak{p}}] = [\mathfrak{a}]$ in the latter case.

Conversely, assume that $p\mathcal{O}_K \in \{\mathfrak{p}^2, \mathfrak{p}\bar{\mathfrak{p}}\}$ and $[\mathfrak{p}] \in \{[\mathfrak{a}], [\mathfrak{a}]^{-1}\}$. Note that $1 = [p\mathcal{O}_K] = [\mathfrak{p}]^2$ or $1 = [p\mathcal{O}_K] = [\mathfrak{p}]\cdot[\bar{\mathfrak{p}}]$, hence $[\mathfrak{p}] = [\mathfrak{p}]^{-1}$ or $[\mathfrak{p}] = [\bar{\mathfrak{p}}]^{-1}$, resp. So w. l. o. g., we may assume that $[\mathfrak{p}] = [\mathfrak{a}]^{-1}$ (otherwise consider $\mathfrak{p}^{-1}$ or $\bar{\mathfrak{p}}$, resp.). This means that $(z) := \mathfrak{p}\mathfrak{a} \subseteq \mathcal{O}_K$ is a principal ideal, hence $z \in \mathfrak{a}$ and $N_{\mathfrak{a}}(z) = \pm\mathcal{N}((z))/\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{p}\mathfrak{a}\mathfrak{a}^{-1}) = \pm\mathcal{N}(\mathfrak{p}) = \pm p$ (the last equality follows from Proposition 7.53 and from an analogous exhaustion of cases). □

Example 7.75. According to Example 7.61, the discriminant of $\mathbb{Z}[\sqrt{-5}]$ is -20. As the only prime divisors of -20 are 2 and 5, the only primes that ramify in $\mathbb{Z}[\sqrt{-5}]$ are (2) and (5) via $2\mathbb{Z}[\sqrt{-5}] = (2, 1+\sqrt{-5})^2$ and $5\mathbb{Z}[\sqrt{-5}] = (\sqrt{-5})^2$. Recall Example 7.73.

(i) $x^2 + 5y^2 = 29$ has a solution $x = 3$, $y = 2$. Since $(29) \subset \mathbb{Z}$ does not ramify, its image in $\mathbb{Z}[\sqrt{-5}]$ splits into $29\mathbb{Z}[\sqrt{-5}] = \mathfrak{p}\bar{\mathfrak{p}}$ with principal $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ because $[\mathfrak{p}] = [\bar{\mathfrak{p}}] = [\mathbb{Z}[\sqrt{-5}]]$.

(ii) $2x^2 + 2xy + 3y^2 = 3$ or 7 have solutions, e. g. $x = 0$, $y = 1$ or $x = 1$, $y = 1$, resp. Hence $3\mathbb{Z}[\sqrt{-5}]$ and $7\mathbb{Z}[\sqrt{-5}]$ split into non-principal ideals (they are non-principal since the factors lie in the class group $[(2, 1+\sqrt{-5})]$ or $[(2, 1+\sqrt{-5})]^{-1}$).

7.10 A Theorem of Gauss

Warning: The following adds a tremendous amount of new information!

Definition 7.76. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. We call

$$D := \begin{cases} 4d, & \text{if } d \equiv 2,3 \mod (4), \\ d, & \text{if } d \equiv 1 \mod (4), \end{cases}$$

the **fundamental discriminant** of K.

This is the -20 we calculated earlier in Example 7.73.

Theorem 7.77 (Gauss 1978)**.** *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free, let $\mathcal{O}_K \subseteq K$ be the ring of integers, and let D be the fundamental discriminant of K. There exists a group homomorphism*

$$\chi \colon (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$$

such that for every prime number $p \nmid D$, the ideal $p\mathcal{O}_K$ splits if and only if $\chi(p) = 1$.

We will not prove this.

Remark 7.78. This is closely related to **law of quadratic reciprocity** by Gauss, which provides an algorithm for computing χ (and which we will not dive into).

Example 7.79. We use Proposition 7.74 extensively.

(i) Let $d = -1$. Then $D = -4$ and $\mathcal{O}_K = \mathbb{Z}[\mathrm{i}]$ with trivial ideal class group since $\mathbb{Z}[\mathrm{i}]$ is a principal ideal domain (Proposition 1.55 and Remark 7.42). So $p \neq 2$ splits in $\mathbb{Z}[\mathrm{i}]$ if and only if $N(z) = x^2 + y^2 = p$ has a solution if and only if $p \equiv 1 \mod (4)$ (Theorem 2.5). Hence

$$\chi(p) = \begin{cases} 1, & p \equiv 1 \mod (4), \\ -1, & p \equiv 3 \mod (4). \end{cases}$$

(We exclude $p \equiv 2 \mod (4)$ since $p \neq 2$.)

(ii) Let $d = -2$. Then $D = -8$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ with trivial ideal class group since $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain (Proposition 1.55 and Remark 7.42). So $p \neq 2$ splits in $\mathbb{Z}[\sqrt{-2}]$ if and only if $N(z) = x^2 + 2y^2 = p$ has a solution if and only if $p \equiv 1,3 \mod (8)$. Hence

$$\chi(p) = \begin{cases} 1, & p \equiv 1,3 \mod (8), \\ -1, & p \equiv 5,7 \mod (8). \end{cases}$$

(iii) Let $d = -5$. Then $D = -20$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ with $\mathrm{Cl}_{\mathbb{Z}[\sqrt{-5}]} = \{[\mathbb{Z}[\sqrt{-5}]], [(2, 1 + \sqrt{-5})]\}$ (cf. Example 7.73). So $p \neq 2,5$ splits in $\mathbb{Z}[\sqrt{-5}]$ if and only if $N_{\mathbb{Z}[\sqrt{-5}]}(z) = x^2 + 5y^2 = p$ or $N_{(2,1+\sqrt{-5})}(z) = 2x^2 + 2xy + 3y^2 = p$ has a solution if and only if $p \equiv 1,3,7,9 \mod (20)$. Hence

$$\chi(p) = \begin{cases} 1, & p \equiv 1,3,7,9 \mod (20), \\ -1, & p \equiv 11,13,17,19 \mod (20). \end{cases}$$

(The residue classes are $(\mathbb{Z}/20)^\times \cong (\mathbb{Z}/4)^\times \times (\mathbb{Z}/5)^\times$.)

(iv) Let $d = 2$. Then $D = 8$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, which is, in fact, a principal ideal domain, and hence has trivial ideal class group. So $p \neq 2$ splits in $\mathbb{Z}[\sqrt{2}]$ if and only if $N(z) = x^2 - 2y^2 = p$ has a solution if and only if $p \equiv 1,7 \mod (8)$. Hence

$$\chi(p) = \begin{cases} 1, & p \equiv 1,7 \mod (8), \\ -1, & p \equiv 3,5 \mod (8). \end{cases}$$

Note that we can solve for both signs since the norm is multiplicative and since $-1 = 1^2 - 2 \cdot 1^2 = N(1 + \sqrt{2})$.

Remark 7.80. If $d > 0$, for a given prime $p \in \mathbb{Z}$, we cannot solve the norm equation $N(z) = p$ by brute-forcing all possible solutions since the norm is not positive definite. But if $d < 0$, this is possible.

7.11 The Hilbert Class Field

Problem 7.81. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free, and let $\mathcal{O}_K$ be the ring of integers. By Theorem 7.77 and Gauss's law of quadratic reciprocity, we may determine which prime numbers $p \in \mathbb{Z}$ split in $\mathcal{O}_K$. Then Proposition 7.74 tells us that there a *suitable* ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $N_{\mathfrak{a}}(z) = \pm p$ has a solution $z \in \mathcal{O}_K$.

We want to improve on that by determining the $p \in \mathbb{Z}$ such that the *general* equation $N_{\mathfrak{a}}(z) = N(z) = \pm p$ with $\mathfrak{a} = \mathcal{O}_K$ has a solution $z \in \mathcal{O}_K$.

Definition 7.82. A finite number field extension L/K is **unramified** if no prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ is ramified over $\mathcal{O}_K$, i. e. $e(\mathfrak{P}) = 1$ for all $\mathfrak{P} \subset \mathcal{O}_L$.

We will not prove the following theorem.

Theorem 7.83 (Furtwängler 1906)**.** *Let $K/\mathbb{Q}$ be a number field. Then there exists a unique finite Galois extension L/K (such that all archimedean primes split, and) such that for all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$, the following property holds: $\mathfrak{p}$ is principal if and only if $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$, i. e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_{[L:K]}$ with prime ideals $\mathfrak{P}_i \subset \mathcal{O}_L$ and $\mathfrak{P}_i \neq \mathfrak{P}_j$ for all $i \neq j$.*

Definition 7.84. The field L in Theorem 7.83 is called the **Hilbert class field** of K. It satisfies the following:

(i) $\mathrm{Gal}(L/K) \cong \mathrm{Cl}_{\mathcal{O}_K}$.

(ii) It is the maximal abelian unramified extension of K.

Corollary 7.85. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. Let L/K be the Hilbert class field extension, and write $L \cong \mathbb{Q}[T]/(f(T))$ with $f \in \mathbb{Z}[T]$. Let $0 \neq s \in \mathbb{Z}$ be such that $\mathcal{O}_L[s^{-1}] \cong \mathbb{Z}[s^{-1}, T]/(f(T))$. Then for all prime numbers $p \nmid s$, the equation $N(z) = \pm p$ has a solution $z \in \mathcal{O}_K$ if and only if $(f \bmod p) \neq 0$ has a root in $\mathbb{F}_p$.*

Proof. First a comment on the existence of f and s: By definition of Hilbert class fields, L/K is separable, so $L/\mathbb{Q}$ is separable ($K/\mathbb{Q}$ is separable if $d \neq 0$, and $K = \mathbb{Q}$ if $d = 0$). Furthermore, $\mathcal{O}_K \subseteq \mathcal{O}_L$ is a finite Dedekind ring extension, hence $\mathbb{Z} \subseteq \mathcal{O}_L$ is so as well. As we have seen in Proposition 7.60, there exists a $0 \neq s \in \mathbb{Z}$ such that $\mathbb{Z}[s^{-1}] \subseteq \mathcal{O}_L[s^{-1}]$ is monogenic, thus $\mathcal{O}_L[s^{-1}] \cong \mathbb{Z}[s^{-1}, T]/(f(T))$ and $L \cong \mathbb{Q}[T]/(f(T))$ for some $f(T) \in \mathbb{Z}[s^{-1}, T]$. By clearing denominators, we may assume $f \in \mathbb{Z}[T]$.

The proof will be the following sequence of equivalent statements (here, $\mathfrak{p} \neq \bar{\mathfrak{p}}$ is not necessary):

- $N(z) = \pm p$ has a solution $z \in \mathcal{O}_K$.
- $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_K$ and $\mathfrak{p}$ is principal (Proposition 7.74 and $[\mathfrak{p}] = [\mathcal{O}_K] = [\mathcal{O}_K]^{-1}$ in $\mathrm{Cl}_{\mathcal{O}_K}$).
- $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_K$ and $\mathfrak{p}$ completely splits in $\mathcal{O}_L$ (Theorem 7.83).
- $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_K$ and there exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ above $\mathfrak{p}$ with $f(\mathfrak{P} \mid \mathfrak{p}) = 1$.

  (If $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_{[L:K]}$, then $f(\mathfrak{P}_1) = \cdots = f(\mathfrak{P}_{[L:K]}) = 1$ by Proposition 7.53. Conversely, if $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, then $\mathfrak{p}\mathcal{O}_L = (\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{P}))^e$ with $|\mathrm{Gal}(L/K)| = [L : K]$ and $e \geq 1$ since L/K is Galois and Corollary 7.64. Because $f(\mathfrak{P}) = 1$, Proposition 7.53 implies $e = 1$.)
- There exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ above p with $f(\mathfrak{P} \mid p) = 1$.

  (We have
  $$f(\mathfrak{P} \mid p) = [\mathcal{O}_L/\mathfrak{P} : \mathbb{F}_p] = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] \cdot [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = f(\mathfrak{P} \mid \mathfrak{p}) f(\mathfrak{p} \mid p) \tag{7.86}$$
  for all prime ideals $\mathfrak{P} \subset \mathcal{O}_L$ above p, where $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Moreover, $f(\mathfrak{p} \mid p) = 1$ if and only if $p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}$.

  Suppose that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and $f(\mathfrak{P} \mid \mathfrak{p}) = 1$. Then, by Proposition 7.53, either $2 = f(\mathfrak{p} \mid p) + f(\bar{\mathfrak{p}} \mid p)$ if $\mathfrak{p} \neq \bar{\mathfrak{p}}$, or $2 = 2f(\mathfrak{p} \mid p)$ if $\mathfrak{p} = \bar{\mathfrak{p}}$. In both cases, $f(\mathfrak{p} \mid p) = 1$, hence $f(\mathfrak{P} \mid p) = 1$ by (7.86) (cf. Proposition 7.74). Conversely, suppose that $f(\mathfrak{P} \mid p) = 1$. Then $f(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{p} \mid p) = 1$ by (7.86). Thus, similarly to the previous argument, Proposition 7.53 implies that $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with possibly $\mathfrak{p} = \bar{\mathfrak{p}}$.)

- $f \bmod p$ has a root in $\mathbb{F}_p$.

  (By assumption, $\mathbb{Z}[s^{-1}] \subseteq \mathcal{O}_L[s^{-1}]$ is monogenic. Since $p \nmid s$, we have $s \bmod p \neq 0$, so $\mathbb{F}_p = \mathbb{F}_p[s^{-1}]$. Hence by the Dedekind-Kummer theorem 7.55, $f \bmod p \in \mathbb{F}_p[T] = \mathbb{F}_p[s^{-1}, T]$ has a linear factor, i. e. a root, if and only if there exists a prime ideal $\mathfrak{P}[s^{-1}] \subset \mathcal{O}_L[s^{-1}]$ above p such that $f(\mathfrak{P}[s^{-1}] \mid p) = 1$. This is equivalent to the existence of a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ above p such that $f(\mathfrak{P} \mid p) = 1$ since $\mathcal{O}_L[s^{-1}]/\mathfrak{P}[s^{-1}] \cong [(s \bmod \mathfrak{P})^{-1}] = \mathcal{O}_L/\mathfrak{P}$. Note that the last equality follows because $s \notin (p) = \mathfrak{P} \cap \mathbb{Z}$, so $s \bmod \mathfrak{P} \neq 0$.) □

Example 7.87. Consider $K = \mathbb{Q}(\sqrt{-5})$. We know from previous examples that $|\mathrm{Cl}_{\mathbb{Z}[\sqrt{-5}]}| = 2$, so the Hilbert class field L of K is quadratic. One would check that $L = K(\mathrm{i}) = \mathbb{Q}(\sqrt{-5}, \mathrm{i})$.

So for prime numbers $p \neq 2, 5$, as we have seen in Corollary 7.85, $x^2 + 5y^2 = p$ has a solution if and only if p splits in $\mathbb{Z}[\sqrt{-5}]$ and in $\mathbb{Z}[\mathrm{i}]$ (since in this case, each factor of $p\mathbb{Z}[\sqrt{-5}]$ split in $\mathcal{O}_L$). This happens if and only if $p \equiv 1, 3, 7, 9 \mod (20)$ and $p \equiv 1 \mod (4)$ (see Example 7.79), i. e. $p \equiv 1, 9 \mod (20)$.

This also implies that that $2x^2 + 2xy + 3y^2 = p$ has a solution if and only if $p \equiv 3, 7 \mod (20)$ (see Example 7.79 again).

This is the end. A personal note from our lecturer:

Thank you for this great course! I hope you enjoyed it and wish you the best for your future studies!
– A. Mihatsch –

Reviewed Peer-reviewed

8 Exercises

8.1 Introduction

Exercise 8.1. True or false? Two of the following questions are very hard, so if you are stuck with one question, just continue with the next.

(i) There are two non-isomorphic groups of order 4.

(ii) There are two non-isomorphic groups of order 5.

(iii) $x^3 - x^2 + x + 1 \in \mathbb{F}_3[x]$ is irreducible.

(iv) $x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ is irreducible.

(v) There is a field of order 27.

(vi) There is a field of order 24.

(vii) An ideal $I \subseteq R$ is an R-module.

(viii) An ideal $\mathfrak{m}$ of R is maximal if and only if $R/\mathfrak{m}$ is an integral domain.

(ix) $\mathbb{Q}$ is a free $\mathbb{Z}$-module.

(x) Let $f\colon K \to R$ be a ring homomorphism, where K is a field and $R \neq 0$. Then f is injective.

(xi) Let K and L be two fields such that there are field homomorphisms $K \to L$ and $L \to K$. Then $K \cong L$.

(xii) For all ring homomorphisms $\psi\colon R \to S$ and all $s \in S$, there exists precisely one $\psi'\colon R[X] \to S$ such that $\psi'|_R = \psi$ and $\psi'(X) = s$.

(xiii) $\mathbb{Z}[X]$ is a unique factorisation domain.

(xiv) $\mathbb{Z}[X]$ is a principal ideal domain.

(xv) Algebraic closures are unique up to isomorphism.

(xvi) Let K be a field and $\overline{K}$ be its algebraic closure. Then $1 < [\overline{K} : K] < \infty$ implies $[\overline{K} : K] = 2$.

Remark: An *R-module* is a generalisation of a vector space, where the underlying field is replaced by the ring R. It is *free* if it has a basis, i. e. an R-linearly independent generating systems.

Solution.

(i) True: $\mathbb{Z}_4 \ncong V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, since $\operatorname{ord}(1) = 4$ in $\mathbb{Z}_4$, but $\operatorname{ord}(1,1) = 2$ in V_4.

(ii) False: Let G be a group with $|G| = 5$. Consider $\langle x \rangle \leq G$ for some $1 \neq x \in G$. By Lagrange, we have $|\langle x \rangle| \in \{1, 5\}$. Since $x \neq 1$, $\langle x \rangle = G$, i. e. G is cyclic. Cyclic groups are unique and we have $G \cong \mathbb{Z}_5$.

(iii) True: Suppose that the polynomial is not irreducible. Then it will decompose into at least one factor of degree 1. But this polynomial has no zeros in $\mathbb{F}_3$.

(iv) False: We have $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ in $\mathbb{Q}[X]$.

(v) True: $\mathbb{F}_{27}$ since $27 = 3^3$. More explicitly, we can consider $\mathbb{F}_3[x]/(x^3 - x^2 + x + 1)$, which is a field with 27 elements. (Let $\mathfrak{a} \coloneqq (x^3 - x^2 + x + 1)$. Then $1 + \mathfrak{a}$, $x + \mathfrak{a}$, $x^2 + \mathfrak{a}$ is an $\mathbb{F}_3$-basis of this field, giving $3^3 = 27$ elements.)

(vi) False: Suppose that K is a field with $|K| = 24$. Since $\operatorname{char}(K) = p$ is prime (otherwise we have $(1 + \cdots + 1)(1 + \cdots + 1) = 0$, but K has no zero divisors) and $\mathbb{F}_p$ is isomorphic to some subfield of K, we can regard K as a finite-dimensional $\mathbb{F}_p$-vector space. Thus the number of linear combinations, i. e. $|K|$, is a p-power, a contradiction.

(vii) True: I is already an additive abelian group. By the ideal property, I is closed under scalar multiplication with R. The other axioms follow from R.

(viii) False: An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field. Or an ideal $\mathfrak{m}$ is prime if and only if $R/\mathfrak{m}$ is an integral domain.

(ix) False: Assume there are two generating elements $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$. Then $\frac{p}{q}qr - \frac{r}{s}sp = 0$, i. e. these elements are $\mathbb{Z}$-linearly dependent. Thus any basis can only have on element $\frac{p}{q}$. But $\frac{p}{q}\mathbb{Z} \neq \mathbb{Q}$, since there cannot be fractions with denominator greater 1. In the end $\mathbb{Q}$ is not free over $\mathbb{Z}$.

(x) True: $\ker(f)$ is an ideal of K, and the only ideals are 0 and K. Since $0 \neq 1$ in R, we have $f(1) \neq 0$ and thus $1 \notin \ker(f)$. Hence $\ker(f) = 0$ and f is injective.

(xi) False: Consider

$$K \coloneqq \overline{\mathbb{Q}(x_1, x_2, \dots)} \hookrightarrow L \coloneqq \overline{\mathbb{Q}(x_1, x_2, \dots,)(x_0)} \hookrightarrow \overline{\mathbb{Q}(x_0, x_1, \dots)} \cong \overline{\mathbb{Q}(x_1, x_2, \dots)},$$

where we adjoin infinitely many variables. The embeddings are obvious (the natural inclusion map). The isomorphism is a simple index shift. Thus we have injective field homomorphisms between K and L, but $K \ncong L$ since $L = K(x_0)$ and x_0 is transcendental over K.

(xii) True: This is the universal property for polynomial rings $R[x]$.

(xiii) True: This follows from Gauss's lemma (if R is a unique factorisation domain, then so is $R[x]$).

(xiv) False: $R[x]$ is a principal ideal domain if and only if R is field if and only if $R[x]$ is euclidean. Now $\mathbb{Z}$ is not a field.

Alternatively: Consider $(2, x) \neq \mathbb{Z}[x]$ and suppose that there is a polynomial $p \in \mathbb{Z}[x]$ such that $(p) = (2, x)$. Then we must have $p \mid 2$ and $p \mid x$, which is only possible for $p = \pm 1$. This contradicts $(p) \neq \mathbb{Z}[x]$. Therefore $(2, x)$ is not a principal ideal.

(xv) True, see [Sch, Cor. 6.4].

(xvi) Actually true, but the proof is quite involved (Arthur-Schreier theorem). Fields K with the property $1 < [\overline{K} : K] < \infty$ are called *real closed fields*.

Exercise 8.2.

(i) Find all R-free ideals of a ring R.

(ii) By the universal property of the polynomial ring $R[X]$, we can view a polynomial $f \in R[X]$ as a function $f\colon R \to R$ (the evaluation map). However, we might lose some information if we do so, e. g. the polynomial $x^2 + x \in \mathbb{F}_2$ is 0 as a function, but not the zero polynomial.

Find all fields K such that two polynomials in $K[X]$ are the same if and only if they are the same as functions. Do algebraically closed fields have this property?

Solution.

(i) Let I be a free ideal. Suppose that $a, b \in I$ are two generating elements. Since $ab - ba = 0$, they are linearly dependent, thus the basis must consist of one element, say $a \in I$. Furthermore, a is a zero divisor if and only if there is some $0 \neq b \in R$ such that $ab = 0$, i. e. a is linearly dependent. Thus all free ideals are $I = (a)$ with $a \in R$ not a zero divisor and 0.

(ii) If K is finite, then this property does not hold: Then $\prod_{a \in K}(x - a) \in K[x]$ is 0 as a function, but not the zero polynomial.

Now assume that K is infinite. We consider two polynomials $p, q \in K[x]$ such that they are equal as functions, i. e. $p - q$ is the zero function. If we can show that a polynomial is the zero polynomial if it is the zero function, we are done.

Consider $p \in K[x]$ such that $p(x) = 0$ for all $x \in K$. Thus p has infinitely many roots. This necessarily implies $p = 0$ as a polynomial (for $p \neq 0$ can have at most $\deg(p) < \infty$ roots).

This is true for all algebraically closed fields K. Assume that K is finite. Then $\prod_{a \in K}(x - a) + 1 \in K[x]$ has no root in K and hence does not split into linear factors, a contradiction. Therefore K must be infinite.

8.2 Rings and Ideals

Exercise 8.3 (01.1)**.** Determine the nilradical, the Jacobson radical and the units for each ring A below.

(i) k a field and $A = k[T]$.

(ii) k a field and $A = k[\varepsilon, T]/(\varepsilon^2)$.

(iii) k a field, $n \geq 1$ and $A = k[\![T_1, \ldots, T_n]\!]$.

To solve this exercise, we use the following statement.

Proposition 8.4. *Let $A \neq 0$ be a ring. Then $x \in \operatorname{jac}(A)$ if and only if $1 - xy \in A^\times$ for all $y \in A$.*

Proof. (From [AtMac, ch. 1].) Let $x \in \operatorname{jac}(A)$, and suppose that $1 - xy \notin A^\times$ for some $y \in A$. By Corollary 2.20, $1 - xy \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$. But $x \in \operatorname{jac}(A) \subseteq \mathfrak{m}$, so $xy \in \mathfrak{m}$ and thus $(1 - xy) + xy = 1 \in \mathfrak{m}$, a contradiction by Lemma 1.25.

Conversely, let $x \notin \operatorname{jac}(A)$, say $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$. By definition of maximal ideals, we must have $\mathfrak{m} + (x) = A$, thus $m + xy = 1$ for some $m \in \mathfrak{m}$ and $y \in A$. Hence $1 - xy = m \in \mathfrak{m}$ and $1 - xy \notin A^\times$ by Lemma 1.25. □

Solution.

(i) From [Sch, Exercise 5.20.10], we know that $f = \sum_{i=0}^{n} a_i T^i \in A$ is a unit if and only if $f \in k^\times$, so $k[T]^\times = k^\times$.

Furthermore, also known from [Sch, Exercise 5.20.10], $f \in \operatorname{nil}(A)$ if and only if all a_i are nilpotent. As the only nilpotent element in k is 0, we have $\operatorname{nil}(A) = 0$.

Finally, we have $1 - ab \in k^\times$ for some $a, b \in A$ if and only if $ab \in k$ and $ab \neq 1$. Therefore, by Proposition 8.4, $f \in \operatorname{jac}(A)$ if and only if $f = 0$ (this already follows from $fg \in k$ for all $g \in A$). This gives $\operatorname{jac}(A) = 0$.

(ii) Observe $A \cong k[T] \oplus \varepsilon k[T]$. Recall that a ring map maps units to units. Consider the evaluation $k[\varepsilon, T] \to k[T]$ for $\varepsilon = 0$. Its kernel (ε) contains (ε^2). Hence, by the homomorphism theorem, $\phi\colon A \to k[T]$, $f + \varepsilon g \mapsto f$ is a well-defined ring map.

Let $f+\varepsilon g \in A^\times$ with $f,g \in k[T]$. Then $\phi(f+\varepsilon g) = f \in k[T]^\times = k^\times$ by (i), hence $A^\times \subseteq k^\times \oplus \varepsilon k[T]$. Conversely, $(f+\varepsilon g)(f^{-1} - \varepsilon g f^{-2}) = 1$ for all $f \in k^\times$ and $g \in k[T]$, hence $k^\times \oplus \varepsilon k[T] \subseteq A^\times$.

We will show that $(\varepsilon) = \operatorname{nil}(A) = \operatorname{jac}(A)$.

Let $\varepsilon f \in (\varepsilon)$ with $f \in A$. Then $(\varepsilon f)^2 = \varepsilon^2 f^2 = 0$, hence $\varepsilon f \in \operatorname{nil}(A)$, i. e. $(\varepsilon) \subseteq \operatorname{nil}(A)$.

Let $f \in \operatorname{nil}(A)$, say $f^n = 0$ for some $n \geq 0$. Then $\bar{f}^n = 0$ in the field $A/\mathfrak{m}$ for any maximal ideal $\mathfrak{m} \subset A$ (Corollary 1.29). Therefore $\bar{f} = 0$, i. e. $f \in \mathfrak{m}$. This shows $\operatorname{nil}(A) \subseteq \operatorname{jac}(A)$ (this generally holds for any ring A).

Let $f+\varepsilon g \in \operatorname{jac}(A)$ with $f,g \in k[T]$. Then, by Proposition 8.4, $1-(f+\varepsilon g) \in A^\times$. We already know $A^\times$, so $1-f \in k^\times$, hence $f \in k$. If $f \in k^\times$, then $1 - f^{-1}(f+\varepsilon g) = \varepsilon f^{-1} g \notin A^\times$. Thus necessarily, $f = 0$ and $\varepsilon g \in (\varepsilon)$, so $\operatorname{jac}(A) \subseteq (\varepsilon)$.

(iii) From Proposition 1.47 it follows that $f \in k[\![T_1]\!]^\times$ if and only if the coefficient of zeroth degree is in $k^\times$. By induction, $f \in A^\times$ if and only if the coefficient of zeroth degree is in $k^\times$.

We prove the following statement: Let A be any ring with a unique maximal ideal $\mathfrak{m} \subset A$. Then $A[\![T]\!]$ has a unique maximal ideal, namely $(\mathfrak{m}, T)$.

$A[\![T]\!]/(\mathfrak{m},T) \cong A/\mathfrak{m}$ is a field due to Corollary 1.29, and again by Corollary 1.29, $(\mathfrak{m},T)$ is maximal in $A[\![T]\!]$. Suppose there would be another maximal ideal $\mathfrak{n} \subset A[\![T]\!]$. Choose any $f = \sum_{i=0}^\infty a_i T^i \in \mathfrak{n} \setminus (\mathfrak{m},T)$ (such an f must exist as otherwise, by maximality, $\mathfrak{n} = (\mathfrak{m},T)$), in particular, $a_0 \notin \mathfrak{m}$. Clearly, $f \notin A[\![T]\!]^\times$, so by Proposition 1.47, $a_0 \notin A^\times$. Thus there exists some maximal ideal $\bar{\mathfrak{n}} \subset A$ such that $a_0 \in \bar{\mathfrak{n}}$. But this implies that there are two maximal ideals $\mathfrak{m}$ and $\bar{\mathfrak{n}}$ in A, a contradiction.

(*Alternative:* We can prove that $A[\![T]\!]$ is local w. r. t. $\mathfrak{m} + (T)$ more easily. We know from Example 2.21 that $A^\times = A \setminus \mathfrak{m}$. From Proposition 1.47, it follows that $A[\![T]\!]^\times = A[\![T]\!] \setminus (\mathfrak{m},T)$, so by Example 2.21 again, $A[\![T]\!]$ is local.)

Back to the actual problem. We know from Proposition 1.50 that (T_1) is the only maximal ideal of $k[\![T_1]\!]$. By induction, $(T_1,\dots,T_n)$ is the only maximal ideal of A, thus $\operatorname{jac}(A) = (T_1,\dots,T_n)$.

Let $f \in A \setminus \{0\}$ and consider any non-zero coefficient $a \in k^\times$ of f of minimal total degree $i_1 + \cdots + i_n$. Then for any $m \geq 0$, by induction, the coefficient of total degree $m(i_1+\cdots+i_n)$ in f^m is $a^m \neq 0$, hence $f^m \neq 0$, hence $f \notin \operatorname{nil}(A)$. In conclusion, $\operatorname{nil}(A) = 0$.

Exercise 8.5 (**Chinese remainder theorem**, 01.2)**.** Let A be a ring and $\mathfrak{a},\mathfrak{b} \subseteq A$ two ideals, such that $\mathfrak{a}+\mathfrak{b} = A$. Then the ring map

$$A/\mathfrak{a}\cap\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}, \qquad r+\mathfrak{a}\cap\mathfrak{b} \mapsto (r+\mathfrak{a}, r+\mathfrak{b})$$

is an isomorphism. Moreover, show $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Solution. Since $\mathfrak{a}+\mathfrak{b} = A$, there are some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a+b = 1$.

Let $\phi\colon \pi_\mathfrak{a} \times \pi_\mathfrak{b}\colon A \to A/\mathfrak{a} \times A/\mathfrak{b}$, which is a ring map. Then ϕ is surjective: Let $(r+\mathfrak{a}, s+\mathfrak{b}) \in A/\mathfrak{a} \times A/\mathfrak{b}$. We obtain

$$r+\mathfrak{a} = ra+rb+\mathfrak{a} = rb+\mathfrak{a} = rb+sa+\mathfrak{a} \qquad \text{and} \qquad s+\mathfrak{b} = sa+sb+\mathfrak{b} = sa+\mathfrak{b} = rb+sa+\mathfrak{b}.$$

Thus $\phi(rb+sa) = (r+\mathfrak{a}, s+\mathfrak{b})$. Furthermore, $\ker\phi = \ker\pi_\mathfrak{a} \cap \ker\pi_\mathfrak{b} = \mathfrak{a}\cap\mathfrak{b}$. By the homomorphism theorem, the proposed isomorphism follows.

Now to the second claim. For all $x \in \mathfrak{a}\cap\mathfrak{b}$, we have $xa, xb \in \mathfrak{a}\mathfrak{b}$, hence $x = xa+xb \in \mathfrak{a}\mathfrak{b}$. Conversely, all generators xy of $\mathfrak{a}\mathfrak{b}$ with $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ lie in $\mathfrak{a}\cap\mathfrak{b}$, thus $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$.

Exercise 8.6 (01.3)**.** Let A be a ring. We call $e \in A$ an **idempotent** if $e^2 = e$. We denote the set of all idempotents of A by $\operatorname{idem}(A)$.

(i) Let A be a ring. Show that the map $e \mapsto (A_1 \coloneqq eA, A_2 \coloneqq (1-e)A)$ induces a bijection between $\operatorname{idem}(A)$ and decompositions $A \cong A_1 \times A_2$ as rings.

(ii) Let $A = \mathbb{Z}/133$. Determine $\operatorname{idem}(A)$.

Solution.

(i) Let ϕ be the map from the problem statement, mapping $e \in \operatorname{idem}(A)$ to a decomposition $eA \times (1-e)A$ as rings. We have $1-e \in \operatorname{idem}(A)$, as $(1-e)^2 = 1-2e+e^2 = 1-e$. Hence eA and $(1-e)A$ are indeed rings with identities e and $1-e$, resp. Furthermore, $A \cong eA \times (1-e)A$ is indeed a decomposition due to the ring map $a \mapsto (ea, (1-e)a)$ and its inverse $(ea_1, (1-e)a_2) \mapsto ea_1 + (1-e)a_2$ (notice that $e(1-e) = 0$).

Let ψ be the map associating any decomposition $A \cong A_1 \times A_2$ as rings, given by an isomorphism $f\colon A_1 \times A_2 \to A$, to $e := f(1,0) \in \operatorname{idem}(A)$. Indeed, $e^2 = f(1^2, 0) = f(1,0) = e \in \operatorname{idem}(A)$.

We claim that ϕ and ψ are inverses of each other (the decomposition is unique up to isomorphism), proving ϕ is a bijection.

Let $e \in \operatorname{idem}(A)$. Then ϕ gives a decomposition $A \cong eA \times (1-e)A$ with an isomorphism $f\colon eA \times (1-e)A \to A$, $(ea_1, (1-e)a_2) \mapsto ea_1 + (1-e)a_2$. As e is the identity in eA, ψ gives $f(e,0) = e \in \operatorname{idem}(A)$.

Let $A \cong A_1 \times A_2$ be a decomposition as rings with an isomorphism with an isomorphism $f\colon A_1 \times A_2 \to A$. Then ψ gives $e := f(1,0) \in \operatorname{idem}(A)$. Thereafter ϕ gives the decomposition $A \cong eA \times (1-e)A$. This is isomorphic to $A_1 \times A_2$ since f induces the isomorphisms $eA = (e) \cong ((1,0)) = A_1 \times 0$ and $(1-e)A = (1-e) \cong ((0,1)) = 0 \times A_2$ of ideals.

(ii) For any decomposition $A \cong A_1 \times A_2$, we have $|A| = |A_1| \cdot |A_2|$. Since A is a cyclic group, A_1 and A_2 are isomorphic to cyclic cosets of A. As $|A| = 133 = 7 \cdot 19$, the only decompositions $A \cong \mathbb{Z}/p \times \mathbb{Z}/q$ are $(p,q) \in \{(1,133), (7,19), (19,7), (133,1)\}$. Now by (i), the idempotents $e \in \operatorname{idem}(A)$ are given by $eA \cong \mathbb{Z}/k$ for $k = 1, 7, 19, 133$, and in particular, e corresponds to the multiplicative identity element in $\mathbb{Z}/k$.

For the case $k = 1$, we have $0A \cong \mathbb{Z}/1$. Indeed, $0 \in \operatorname{idem}(A)$.

For the case $k = 133$, we have $1A \cong \mathbb{Z}/133 = A$. Indeed, $1 \in \operatorname{idem}(A)$.

For the case $k = 7$, we observe that $\operatorname{ord}(1) = 7$ in the abelian group $\mathbb{Z}/7$. The only $e \in A$ with $\operatorname{ord}(e) = 7$ in A are $e = 19n$ for $1 \le n \le 6$. If $e \in \operatorname{idem}(A)$, then a necessary condition is $(19n)^2 \equiv 19n \mod (133)$. Since $\gcd(19n, 133) = 19$, we have $5n \equiv 19n \equiv 1 \equiv 15 \mod (7)$, thus $n \equiv 3 \mod (7)$. Indeed, $e = 19 \cdot 3 = 57 \in \operatorname{idem}(A)$.

For the case $k = 19$, we observe that $\operatorname{ord}(1) = 19$ in the abelian group $\mathbb{Z}/19$. The only $e \in A$ with $\operatorname{ord}(e) = 19$ in A are $e = 7n$ for $1 \le n \le 18$. If $e \in \operatorname{idem}(A)$, then a necessary condition is $(7n)^2 \equiv 7n \mod (133)$. Since $\gcd(7n, 133) = 7$, we have $7n \equiv 1 \equiv 77 \mod (19)$, thus $n \equiv 11 \mod (19)$. Indeed, $e = 7 \cdot 11 = 77 \in \operatorname{idem}(A)$.

In conclusion, $\operatorname{idem}(A) = \{0, 1, 57, 77\}$.

Exercise 8.7 (01.4)**.** Let k be a field and $k \to A$ a ring homomorphism, such that A is finite-dimensional over k.

(i) Show that A is a field if A is an integral domain.

(ii) Deduce that each prime ideal in A is maximal.

(iii) Deduce that if $A \neq 0$ is reduced, then A is isomorphic to a finite product of finite field extensions l/k.

Solution.

(i) Since $A \neq 0$, let $x \in A \setminus \{0\}$. Consider the ring map $\phi\colon A \to A$, $a \mapsto xa$. Since x is not a zero divisor, we have $\ker(\phi) = 0$, i. e. ϕ is injective. We can interpret ϕ as a k-linear map as well, so by the rank-nullity theorem, $\operatorname{rk}(\phi) = \dim(A)$, hence ϕ is bijective. In particular, some $y \in A$ exists such that $xy = \phi(y) = 1$. Therefore every $x \in A \setminus \{0\}$ is a unit and A is a field.

(ii) Let $\mathfrak{p} \subset A$ be a prime ideal. From Lemma 2.11, we know that $A/\mathfrak{p}$ is an integral domain. Thus, by (i), $A/\mathfrak{p}$ is a field, hence, by Corollary 1.29, $\mathfrak{p}$ is maximal.

(iii) If $\dim(A) = 1$, then $A \cong k$ as k-vector spaces and we are done. In this case, by Lemma 1.27, (0) is the only maximal ideal. So from now on, we suppose that all maximal ideals are non-zero.

Suppose there are distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset A$, which are all non-zero and maximal by (ii). We claim that $\mathfrak{p}_m + \bigcap_{i=1}^{m-1} \mathfrak{p}_i = A$ for all $2 \le m \le n$.

By maximality, we have $\mathfrak{p}_i \subset \mathfrak{p}_i + \mathfrak{p}_j = A$ for all $i \neq j$. Hence for all $2 \leq m \leq n$,

$$A \subseteq \prod_{i=1}^{m-1} (\mathfrak{p}_i + \mathfrak{p}_m) \subseteq \mathfrak{p}_m + \prod_{i=1}^{m-1} \mathfrak{p}_i \subseteq \mathfrak{p}_m + \bigcap_{i=1}^{m-1} \mathfrak{p}_i \subseteq A.$$

The second inclusion follows from $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} \subseteq \mathfrak{ab} + \mathfrak{ac}$ and $\mathfrak{ab} \subseteq \mathfrak{a}$ for all ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$ (expanding the product of ideals, all but one ideal have $\mathfrak{p}_m$ as a factor). This proves the claim.

We now claim that there are at most $\dim(A)$ distinct prime ideals. Suppose there were at least $n = \dim(A) + 1$ distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq A$. By induction on the Chinese remainder theorem 8.5, we obtain $\prod_{i=1}^n A/\mathfrak{p}_i \cong A/\bigcap_{i=1}^n \mathfrak{p}_i$. But $A/\mathfrak{p}_i \neq 0$ for all $1 \leq i \leq n$, so

$$\dim(A) + 1 \leq \sum_{i=1}^{n} \dim(A/\mathfrak{p}_i) = \dim\left(\prod_{i=1}^{n} A/\mathfrak{p}_i\right) = \dim\left(A/\bigcap_{i=1}^{n} \mathfrak{p}_i\right) \leq \dim(A),$$

a contradiction. Hence there are at most $\dim(A)$, in particular finitely many prime ideals in A.

Now suppose that $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subseteq A$ are all prime ideals. We still have $\prod_{i=1}^n A/\mathfrak{p}_i \cong A/\bigcap_{i=1}^n \mathfrak{p}_i$. $\mathfrak{p}_i$ is maximal by (ii), so $A/\mathfrak{p}_i$ is a field for all $1 \leq i \leq n$ due to Corollary 1.29. Furthermore, $A/\mathfrak{p}_i$ is isomorphic to a finite field extension l_i/k for all $1 \leq i \leq n$. On the other hand, since A is reduced, $0 = \mathrm{nil}(A) = \bigcap_{i=1}^n \mathfrak{p}_i$ by Proposition 2.22. In conclusion, we obtain $\prod_{i=1}^n l_i \cong A$.

8.3 Computing Spectra

Exercise 8.8 (02.1)**.** We define $\zeta := \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$.

(i) Show that ζ is a primitive third root of unity.

(ii) Show that the norm (for the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$) of an element $x + y\zeta \in \mathbb{Q}(\zeta)$ with $x, y \in \mathbb{Q}$ is given by $x^2 - xy + y^2$, and that this is non-negative for all $x, y \in \mathbb{Q}$.

(iii) Following the discussion of $\mathbb{Z}[\mathrm{i}]$ from sec. 2.2, show that a prime $p \neq 3$ is of the form $p = x^2 - xy + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \mod (3)$.

Definition 8.9. The **norm** of a finite field extension l/k is the map $N\colon l \to l$ defined as $N(a) := \det(f)$, where $f\colon l \to l$, $x \mapsto ax$ is a k-linear map on l.

Solution.

(i) We have $\zeta^2 = \frac{1}{2}(-1 - \sqrt{-3}) \neq 1$, but $\zeta^3 = 1$.

(ii) Since ζ is a root of unity, we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(3) = 2$, and $\mathbb{Q}(\zeta)$ has the canonical $\mathbb{Q}$-basis $B := (1, \zeta)$. Let $x + y\zeta \in \mathbb{Q}(\zeta)$ and define $f\colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$, $a \mapsto (x + y\zeta)a$. Since $f(1) = x + y\zeta$ and $f(\zeta) = x\zeta - y(1 + \zeta)$, the corresponding matrix of f w.r.t. B is $\left(\begin{smallmatrix} x & -y \\ y & x-y \end{smallmatrix}\right)$ with determinant $N(x + y\zeta) = x^2 - xy + y^2$.

Since $x^2 + y^2 \geq \max \geq xy$, so $N(x + y\zeta) \geq 0$. Similarly for $x \leq y$.

(iii) Suppose a prime $p \neq 3$ is of the form $p = x^2 - xy + y^2$ for some $x, y \in \mathbb{Z}$. Then $p \equiv (x + y)^2 \mod (3)$ is a square modulo (3). The quadratic residue classes modulo (3) are $0^2 \equiv 0$ and $1^2 \equiv 2^2 \equiv 1$. Since $p \neq 3$, we have $p \equiv 1 \mod (3)$.

Now to the converse. We have $\mathbb{Z}[\zeta] \cong \mathbb{Z}[T]/(T^2 + T + 1)$. We claim that $T^2 + T + 1 \in \mathbb{F}_p[T]$ is one of the following:

- $(T + 2)^2$, if $p = 3$,
- $(T - \alpha)(T - \alpha^2)$, if $p \equiv 1 \mod (3)$, where $\alpha \in \mathbb{F}_p^\times$ such that $\alpha^3 = 1$ and $\alpha \neq 1$,
- irreducible, if $p \equiv 2 \mod (3)$.

The case $p = 3$ is clear, so assume $p \neq 3$. In particular, 1 is not a root of $T^2 + T + 1$.

Let $\mathbb{F}_p^\times = \langle \eta \rangle$, so $\operatorname{ord}(\eta) = p - 1$. Then $0 \neq \alpha \in \mathbb{F}_p$ is a root of $T^2 + T + 1$ if and only if $\alpha \neq 1$ is a root of $T^3 - 1$, i. e. $\alpha^3 = 1$. If we write $\alpha = \eta^k \neq 1$ for $0 < k < p - 1$, then this is equivalent to $3 \mid p - 1$. In conclusion, $T^2 + T + 1$ is irreducible if and only if $p \equiv 2 \mod (3)$.

In the case $p \equiv 1 \mod (3)$, $T^2 + T + 1$ has a root $1 \neq \alpha \in \mathbb{F}_p$ with $\alpha^3 = 1$. We observe that α^2 is a root too, so $T^2 + T + 1 = (T - \alpha)(T - \alpha^2)$.

We obtain

$$\operatorname{MaxSpec}(\mathbb{Z}[\zeta]) = \coprod_{p \text{ prime}} \begin{cases} (3, \zeta + 2), & \text{if } p = 3, \\ (p, \zeta - \alpha), (p, \zeta - \alpha^2) \text{ with } \alpha^3 \equiv 1 \not\equiv \alpha \mod (p), & \text{if } p \equiv 1 \mod (3), \\ (p), & \text{if } p \equiv 2 \mod (3). \end{cases}$$

Observe that $\mathbb{Z}[\zeta] \cong \mathbb{Z}[\zeta_6]$, which is a principal ideal domain according to Corollary 1.56. Let $(\pi) \in \operatorname{MaxSpec}(\mathbb{Z}[\zeta])$ with some prime element $\pi \in \mathbb{Z}[\zeta]$. Assume that $(\pi) \cap \mathbb{Z} = (p)$ with $p \equiv 1 \mod (3)$. Since $\pi \neq 0$ in $\mathbb{Z}[\zeta]/(p)$ (otherwise we would have $(\zeta - a) = (0)$ or $(\zeta - a^2) = (0)$ in $\mathbb{Z}[\zeta]/(p)$), we have $p \nmid \pi$ in $\mathbb{Z}[\zeta]$, thus π is a proper divisor of p, i. e. $\frac{p}{\pi} \notin \mathbb{Z}[\mathrm{i}]^\times$.

We claim that $N(\pi) = p$ and we are done. By multiplicativity, $N(\pi)N(\frac{p}{\pi}) = N(p) = p^2$ holds, so $N(\pi) \in \{1, p, p^2\}$. If $N(\pi) = 1$ or $N(\frac{p}{\pi}) = 1$, then π or $\frac{p}{\pi}$ are units, a contradiction (in this case, the norm describes the determinant of an invertible matrix, which corresponds to left-multiplication by π or $\frac{p}{\pi}$). Hence $N(\pi) = N(\frac{p}{\pi}) = p$.

Exercise 8.10 (02.2)**.**

(i) Let A be a principal ideal domain that is not a field, and let $\mathfrak{m} \subset A$ be a maximal ideal. Prove that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a one-dimensional vector space over $A/\mathfrak{m}$ for any $n \geq 0$.

(ii) Let $A = \mathbb{C}[X, Y]$ and $\mathfrak{m} = (X, Y)$. Compute $\dim_{A/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ for $n \geq 0$. Deduce that A is not a principal domain.

(iii) Let $A = \mathbb{Z}[\sqrt{-3}]$. Show that A has a unique maximal ideal $\mathfrak{m}$ with $\mathfrak{m} \cap \mathbb{Z} = (2)$. Compute $\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. Deduce that A is not a principal ideal domain.

Solution.

(i) Let $V := \mathfrak{m}^n/\mathfrak{m}^{n+1}$ and $k := A/\mathfrak{m}$, which is a field by Corollary 1.29.

Scalar multiplication is defined to be $k \times V \to V$, $\bar{a}(x + \mathfrak{m}^{n+1}) = ax + \mathfrak{m}^{n+1}$. This is well-defined: For $\bar{a} = \bar{b}$, we have $b - a \in \mathfrak{m}$. Thus, for all $x \in \mathfrak{m}^n$, $(b - a)x = bx - ax \in \mathfrak{m}^{n+1}$, and hence $\bar{a}(x + \mathfrak{m}^{n+1}) = \bar{b}(x + \mathfrak{m}^{n+1})$.

Since A is a principal ideal domain, there is some prime element $p \in A$ such that $\mathfrak{m} = (p)$, see Theorem 1.38 (iii). Since A is not a field, $p \neq 0$ by Lemma 1.27. Observe that $p^n \notin \mathfrak{m}^{n+1} = (p^{n+1})$, as otherwise $p^{n+1} \mid p^n$, i. e. $p \in A^\times$. Thus $V = (p^n)/\mathfrak{m}^{n+1} \neq 0$.

Consider the ring map $A \twoheadrightarrow V$, $1 \mapsto p^n + \mathfrak{m}^{n+1}$. The kernel is $\mathfrak{m} = (p)$, thus $k = A/\mathfrak{m} \cong V$ as rings and hence as fields by the homomorphism theorem. In particular, $\dim_k(V) = 1$.

(ii) Notice that $A/\mathfrak{m} \cong \mathbb{C}$ is a field, and thus $\mathfrak{m}$ is maximal.

We claim that $\mathfrak{m}^n = (X^i Y^{n-i} \mid 0 \leq i \leq n)$. By definition, $\mathfrak{m}^0 = A = (1)$. Furthermore, we have $\mathfrak{m}^{n+1} = (X, Y)\mathfrak{m}^n = (X^i Y^{n+1-i} \mid 0 \leq i \leq n + 1)$ by induction.

Observe that $(X^i Y^{n-i})/\mathfrak{m}^{n+1} \cong \mathbb{C} X^i Y^{n-i}$ for all $0 \leq i \leq n$, hence $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong \bigoplus_{i=0}^n \mathbb{C} X^i Y^{n-i}$ as $\mathbb{C}$-vector spaces, thus $\dim_{\mathbb{C}}(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = n + 1$. In particular, by (i), A is not a principal ideal.

(iii) As $T^2 + 3$ is the minimal polynomial of $\sqrt{-3}$ over $\mathbb{Z}$, we have $\mathbb{Z}[\sqrt{-3}] \cong \mathbb{Z}[T]/(T^2 + 3)$. This polynomial splits into $(T + 1)^2 = T^2 + 1$ in $\mathbb{F}_2[T]$. Following Observation 2.4, the only $\mathfrak{m}$ with $\mathfrak{m} \cap \mathbb{Z} = (2)$ is thus $\mathfrak{m} = (2, 1 + \sqrt{-3})$. This implies $\mathfrak{m}^2 = (4, 2 + 2\sqrt{-3})$.

We claim that $2, 1 + \sqrt{-3} \notin \mathfrak{m}^2$. To prove this, consider the norm $N(x + y\sqrt{-3}) = x^2 + 3y^2$ for all $x + y\sqrt{-3} \in A$ on $\mathbb{Z}[\sqrt{-3}]$. Then $16 \mid N(a)$ in $\mathbb{Z}$ for all $a \in \mathfrak{m}^2$, since for any $a, b, c, d \in \mathbb{Z}$, we have

$$\begin{aligned} \frac{1}{4} N(4(a + b\sqrt{-3}) + (2 + 2\sqrt{-3})(c + d\sqrt{-3})) &= N(2a + 2b\sqrt{-3} + (1 + \sqrt{-3})(c + d\sqrt{-3})) \\ &= (2a + c - 3d)^2 + 3(2b + c + d)^2 \equiv (c^2 + d^2 + 2cd) + 3(c^2 + d^2 + 2cd) \equiv 0 \mod (4). \end{aligned}$$

But $N(2) = N(1+\sqrt{-3}) = 4$, so by multiplicativity of the norm, the claim follows.

We now claim that $A/\mathfrak{m} \cong \mathbb{F}_2$. For all $x + y\sqrt{-3} \in A$ with $x, y \in \mathbb{Z}$, we have $x + y\sqrt{-3} \equiv x - y \mod (1+\sqrt{-3})$ with $x - y \in \mathbb{Z}$, so $A/\mathfrak{m} \cong \mathbb{Z}/2 \cong \mathbb{F}_2$.

We clearly see that $2 + \mathfrak{m}^2$ and $1 + \sqrt{-3} + \mathfrak{m}^2$ are $\mathbb{F}_2$-linearly independent, therefore they form a basis of $\mathfrak{m}/\mathfrak{m}^2$. Finally, $\dim_{\mathbb{F}_2}(\mathfrak{m}/\mathfrak{m}^2) = 2$, and A is not a principal ideal domain by (i).

Exercise 8.11 (02.3)**.** Let A be a unique factorisation domain.

(i) Show that for any prime element $\pi \in A$, the ideal $\mathfrak{p} \coloneqq (\pi)$ is prime with $\operatorname{ht}(\mathfrak{p}) = 1$.

(ii) Conversely, let $(0) \neq \mathfrak{p} \subset A$ be a prime ideal such that $\operatorname{ht}(\mathfrak{p}) = 1$. Show that $\mathfrak{p} = (\pi)$ for some prime element $\pi \in A$.

(iii) Assume that each prime ideal $(0) \neq \mathfrak{p} \subset A$ satisfies $\operatorname{ht}(\mathfrak{p}) = 1$. Show that A is a principal ideal domain.

Solution.

(i) From $\pi \notin A^\times$ it follows that $\mathfrak{p} \neq A$ by Lemma 1.25. Moreover, let $ab \in \mathfrak{p}$, i. e. $\pi \mid ab$. Since π is prime, we have $\pi \mid a$ or $\pi \mid b$, thus $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Therefore $\mathfrak{p}$ is prime.

Let $(0) \neq \mathfrak{q} \subseteq \mathfrak{p}$ be a prime ideal of A. Then there is some $0 \neq q \in \mathfrak{q}$ with prime factorisation $q = \pi_1 \cdots \pi_n$. By induction, some π_i lies in $\mathfrak{q}$ as $\mathfrak{q}$ is a prime ideal. W. l. o. g. let $\pi_1 \in \mathfrak{q} \subseteq \mathfrak{p}$, thus $\pi \mid \pi_1$. Since we are in a unique factorisation domain, we have $\pi = \pi_1$ up to units, therefore $\mathfrak{p} = (\pi_1) \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. This shows $\operatorname{ht}(\mathfrak{p}) = 1$.

(ii) Pick any $0 \neq p \in \mathfrak{p}$. As before, there is some prime factor $\pi \in A$ of p in $\mathfrak{p}$, hence $(0) \neq (\pi) \subseteq \mathfrak{p}$. Since $\operatorname{ht}(\mathfrak{p}) = 1$, we have $\mathfrak{p} = (\pi)$.

(iii) By (ii), all prime ideals are principal w. r. t. a prime element.

Obviously, $A = (1)$ and (0) are principal. So let $(0) \neq \mathfrak{a} \subset A$ be a proper ideal. By Corollary 2.19, there is a maximal ideal (π) with a prime element $\pi \in A$ and $\mathfrak{a} \subseteq (\pi)$.

Consider $\tilde{\mathfrak{a}} \coloneqq \{a \in A \mid \pi a \in \mathfrak{a}\}$, which is an ideal. Obviously $\tilde{\mathfrak{a}}(\pi) \subseteq \mathfrak{a}$ by definition. Conversely, $\mathfrak{a} \subseteq \tilde{\mathfrak{a}}(\pi)$ since A is a unique factorisation domain and $\pi \mid a$ for all $a \in \mathfrak{a}$. Therefore if $\tilde{\mathfrak{a}} = (1)$, then $\mathfrak{a} = (\pi)$ is principal and we are done.

Otherwise we continue with $\tilde{\mathfrak{a}}$ by induction. This process cannot take on indefinitely, since any $0 \neq a \in \mathfrak{a}$ has only finitely many prime factors, and in each step, we split off one prime factor.

Exercise 8.12 (02.4)**.**

(i) Let $A \neq 0$ be a ring. Show that A has minimal prime ideals.

Hint: You will have to use Zorn's lemma.

(ii) Determine the minimal prime ideals of $\mathbb{Z}[X, Y]/(XY)$.

Solution.

(i) Let Σ be the set of all prime ideals in A. We can partially order Σ w. r. t. inclusion. Since $A \neq 0$, by Krull's theorem 2.18, there exists a maximal ideal $\mathfrak{m} \subset A$, which is also prime, so $\mathfrak{m} \in \Sigma \neq \varnothing$. Suppose that $S \subseteq \Sigma$ is a chain.

We claim that the ideal $\bigcap_{\mathfrak{p} \in S} \mathfrak{p}$ is prime. For all $x, y \notin \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$, by the chain condition, there is some prime ideal $\mathfrak{p} \in S$ such that $x, y \notin \mathfrak{p}$. Then $xy \notin \mathfrak{p}$, hence $xy \notin \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$.

Thus each chain S has a lower bound $\bigcap_{\mathfrak{p} \in S} \mathfrak{p} \in \Sigma$, and Zorn's lemma implies that there is a minimal prime ideal in Σ.

(ii) Let $\mathfrak{p} \subset \mathbb{Z}[X, Y]/(XY) =: A$ be a prime ideal. Then $\bar{X}\bar{Y} = 0 \in \mathfrak{p}$ implies $\bar{X} \in \mathfrak{p}$ or $\bar{Y} \in \mathfrak{p}$, hence $(\bar{X}) \subseteq \mathfrak{p}$ or $(\bar{Y}) \subseteq \mathfrak{p}$, resp.

By Noether's isomorphism theorem, we obtain $A/(\bar{X}) \cong \mathbb{Z}[X, Y]/(X) \cong \mathbb{Z}[Y]$. As the latter is an integral domain, so are the former quotients. By Lemma 2.11, $(\bar{X})$ is prime in A, and similarly $(\bar{Y})$ in A. Hence $(\bar{X})$ and $(\bar{Y})$ are all minimal prime ideals.

Exercise 8.13 (03.1)**.** Let A be a principal ideal domain. The arguments for $A = \mathbb{Z}$ in Proposition 2.28 work verbatim to show that $\operatorname{Spec}(A[T])$ consists of the following:

(a) (0) (height 0).

(b) (f) with irreducible $f \in A[T]$ (height 1).

(c) (π, g) with prime $\pi \in A$ and $g \in A[T]$ such that the image of g in $A/\pi[T]$ is irreducible (height 2).

(i) Assume that A has infinitely many prime ideals. Prove the height of the prime ideals, and that each maximal ideal of $A[T]$ has height 2.

(ii) Let k be a field and set $A \coloneqq k[\![u]\!]$. Show that $A[u^{-1}]$ is a field. Deduce that, in contrast to (i), the height 1 ideal $(uT - 1) \subseteq A[T]$ is maximal.

Solution.

(i) (a) Obviously, (0) is the only prime ideal of height 0. As A has infinitely many prime ideals, A is not a field due to Lemma 1.27, hence (0) is not maximal.

(b) A is in particular a unique factorisation domain. By Gauss's lemma, $A[T]$ is a unique factorisation domain as well, and thus irreducible $f \in A[T]$ are prime elements. Then $\operatorname{ht}((f)) = 1$ follows from Exercise 8.11.

(f) is not maximal: If $f \in A$, then $(f) \subset (f, T) \subset A[T]$ since $T \notin (f)$ and $A[T]/(f, T) \cong A/f \neq 0$ (as A is a principal ideal domain, $(f) \subset A$ is maximal, hence A/f is a field due to Corollary 1.29). If $f \notin A$, let $p \in A$ be a prime not dividing the leading coefficient of f, which is possible since there are infinitely many prime ideals, and thus infinitely many primes. Then $(f) \subset (f, p) \subset A[T]$ since $p \notin (f)$ and $\bar{f} \in A/p[T]$ is not a unit (use Lemma 1.25 and the fact that $A/p[T]^\times = (A/p)^\times$ as A/p is a field).

(c) By Noether's isomorphism theorem, $A[T]/(\pi, g) \cong (A/\pi[T])/\bar{g}$. A/π is a field, so $A/\pi[T]$ is a principal ideal domain. Since $\bar{g}$ is irreducible, $(\bar{g}) \subset A/\pi[T]$ is maximal and the quotient rings are fields due to Corollary 1.29. Thus (π, g) is maximal.

We claim that (π, g) is not principal. By way of contradiction, suppose $(\pi, g) = (h)$ for some $h \in A[T]$. Then $h \mid \pi$ and $h \mid g$. Since π is prime, either $h = \pi$ or $h = 1$. The case $h = 1$ cannot occur since (π, g) is maximal. In the case $h = \pi$, the image of g in $A/\pi[T]$ is 0, a contradiction.

So Exercise 8.11 implies $\operatorname{ht}((\pi, g)) \geq 2$. If $\operatorname{ht}((\pi, g)) \geq 3$, then there is some prime ideal (ρ, h) of the same type with $(\rho, h) \subset (\pi, g)$. But this contradicts the maximality of (ρ, h). Therefore $\operatorname{ht}((\pi, g)) = 2$.

(ii) Let $\varphi\colon A \to A[u^{-1}]$ be the localisation. Let $0 \neq f = u^{-n} \sum_{i=0}^{\infty} a_i u^i \in A[u^{-1}]$ be arbitrary. We choose the minimal $m \geq 0$ such that $a_m \neq 0$. Then $\varphi^{-1}(u^{n-m} f) = \sum_{i=0}^{\infty} a_{i+m} u^i \in A$ is a unit according to Proposition 1.47 since $a_m \in k^\times$. As ring maps map units to units, $u^{n-m} f$ and therefore f are units in $A[u^{-1}]$.

By construction in Proposition 2.34, $A[u^{-1}] \cong A[T]/(uT - 1)$ is a field, hence $(uT - 1)$ is maximal by Corollary 1.29.

Exercise 8.14 (03.2)**.** Let k be an algebraically closed field and let

$$\varphi\colon k[x, y] \to k[u, v], \qquad x \mapsto u, \qquad y \mapsto uv.$$

(i) Use Exercise 8.13 to show that the maximal ideals of $k[x, y]$ are precisely $\mathfrak{m}_{\lambda,\mu} \coloneqq (x - \lambda, y - \mu)$ for all $\lambda, \mu \in k$.

(ii) Show that φ induces an isomorphism $k[x, y][x^{-1}] \to k[u, v][u^{-1}]$.

(iii) For each $(\lambda, \mu) \in k^2$, calculate $\operatorname{Spec}(\varphi)^{-1}(\mathfrak{m}_{\lambda,\mu})$.

Solution.

(i) Set $A \coloneqq k[x]$, which is a principal ideal. Since k is algebraically closed, the prime elements are precisely $x - \lambda \in A$ for all $\lambda \in k$. These are infinitely many, since no finite field is algebraically closed. Furthermore for all $\lambda \in k$, the evaluation map $A \to k$, $x \mapsto \lambda$ is surjective with kernel $(x - \lambda)$, therefore $A/(x-\lambda) \cong k$ by the homomorphism theorem. Thus the irreducible elements in $A/(x-\lambda)[y] \cong k[y]$ are precisely $y - \mu$ for all $\mu \in k$. By Exercise 8.13, the maximal ideals in $A[y] \cong k[x,y]$ are precisely $(x - \lambda, y - \mu)$ for all $\lambda, \mu \in k$.

(ii) Let $\psi\colon k[u,v] \to k[x,y][x^{-1}]$, $u \mapsto x$, $v \mapsto x^{-1}y$. The ring map ψ is chosen in such a way that the upper left triangle in the following diagram commutes:

$$\begin{array}{ccc} k[x,y] & \xrightarrow{\iota_{x,y}} & k[x,y][x^{-1}] \\ \downarrow{\scriptstyle\varphi} & \overset{\psi}{\nearrow} & \uparrow{\scriptstyle\exists!\chi'} \;\downarrow{\scriptstyle\exists!\chi} \\ k[u,v] & \xrightarrow{\iota_{u,v}} & k[u,v][u^{-1}] \end{array}$$

$\iota_{x,y}$ and $\iota_{u,v}$ are the universal inclusion maps. $\iota_{u,v} \circ \varphi$ maps $x \mapsto u \in k[u,v][u^{-1}]$. So by the universal property of localisations, this composition gives rise to a unique ring map χ such that the outer square commutes. Observe that $\chi|_{k[x,y]} = \varphi$. Similarly, ψ maps $u \to x \in k[x,y][x^{-1}]$, so ψ gives rise to a unique ring map χ' such that ψ factors through χ'.

We now show that χ and χ' are inverses of each other. To do that, note that $\chi' \circ \chi \circ \iota_{x,y} = \chi' \circ \iota_{u,v} \circ \varphi = \psi \circ \varphi = \iota_{x,y}$, so $\iota_{x,y}$ factors through $\chi' \circ \chi$. But by the universal property of localisations, $\iota_{x,y}$ can only factor trivially, so $\chi' \circ \chi = \mathrm{id}$. Similarly, $\chi \circ \chi' \circ \iota_{u,v} = \chi \circ \psi = \iota_{u,v}$. The last equality holds since χ maps $x^{-1} \mapsto u^{-1}$. By the universal property, $\chi \circ \chi' = \mathrm{id}$.

(iii) Observation 2.68 and Example 2.14 say that

$$\mathrm{Spec}(\varphi)^{-1}(\mathfrak{m}_{\lambda,\mu}) = \{\mathfrak{q} \in \mathrm{Spec}(k[u,v]) \mid \varphi(\mathfrak{m}_{\lambda,\mu}) \subseteq \mathfrak{q}\} \cong \mathrm{Spec}(k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu}))).$$

Notice that always $\varphi(k[u,v] \setminus \mathfrak{m}_{\lambda,\mu}) \cap \mathfrak{q} = \varnothing$. Otherwise there would be some $s \notin \mathfrak{m}_{\lambda,\mu}$ with $\varphi(s) \in \mathfrak{q}$. Hence $\mathfrak{m} + (s) \subseteq \varphi^{-1}(\mathfrak{q})$, and by maximality, $\varphi^{-1}(\mathfrak{q}) = k[u,v]$. But this would imply that $\varphi(1) = 1 \in \mathfrak{q}$, a contradiction.

We have three cases to consider.

(a) If $\lambda \neq 0$, then

$$k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu})) = k[u,v]/(u - \lambda, uv - \mu) = k[u,v]/(u - \lambda, v - \mu/\lambda) \cong k.$$

In this case, $\mathrm{Spec}(k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu}))) = \{(0)\}$, corresponding to $\mathrm{Spec}(\varphi)^{-1}(\mathfrak{m}_{\lambda,\mu}) = \{(\varphi(\mathfrak{m}_{\lambda,\mu}))\}$.

(b) If $\lambda = 0$ and $\mu \neq 0$, then

$$k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu})) = k[u,v]/(u, uv - \mu) = k[u,v]/(u,\mu) \cong k[v]/(\mu) \cong 0.$$

In this case, $\mathrm{Spec}(k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu}))) = \varnothing$, corresponding to $\mathrm{Spec}(\varphi)^{-1}(\mathfrak{m}_{\lambda,\mu}) = \varnothing$.

(c) If $\lambda = \mu = 0$, then

$$k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu})) = k[u,v]/(u, uv) = k[u,v]/(u) \cong k[v].$$

Since $k[v]$ is a principal ideal domain, and since k is algebraically closed, we have $\mathrm{Spec}(k[v]) = \{(0), (v-\lambda) \mid \lambda \in k\}$. These correspond to $\mathrm{Spec}(k[u,v]/(\varphi(\mathfrak{m}_{\lambda,\mu}))) = \{(0)/(u), (v-\lambda)/(u) \mid \lambda \in k\}$, which in turn correspond to $\mathrm{Spec}(\varphi)^{-1}(\mathfrak{m}_{\lambda,\mu}) = \{(u), (u, v - \lambda) \mid \lambda \in k\}$.

Exercise 8.15 (03.3)**.** Let A be a ring of Krull dimension $n \coloneqq \dim(A)$. Show that

$$n + 1 \leq \dim(A[T]) \leq 2n + 1.$$

Solution. There are two inequalities to show.

(i) Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a proper chain of prime ideals in A of maximal length. We show that

$$\mathfrak{p}_0 A[T] \subset \cdots \subset \mathfrak{p}_n A[T] \subset \mathfrak{p} A[T] + (T)$$

is a proper chain of prime ideals in $A[T]$. This implies $n+1 \leq \dim(A[T])$.

The $\mathfrak{p}_i A[T]$ are indeed prime: Since $\mathfrak{p}_i$ is prime, by Lemma 2.11, $A/\mathfrak{p}_i$ is an integral domain, hence $(A/\mathfrak{p}_i)[T]$ is an integral domain. The canonical ring map $A[T] \twoheadrightarrow (A/\mathfrak{p}_i)[T]$ is apparently surjective with kernel $\mathfrak{p}_i A[T]$. Thus by the homomorphism theorem, $A[T]/\mathfrak{p}_i A[T] \cong (A/\mathfrak{p}_i)[T]$ is an integral domain, and Lemma 2.11 implies that $\mathfrak{p}_i A[T]$ is prime.

$\mathfrak{p}_n A[T] + (T)$ is prime: By Noether's isomorphism theorem, we obtain

$$A[T]/(\mathfrak{p}_n A[T] + (T)) \cong (A[T]/(T))/((\mathfrak{p}_n A[T] + (T))/(T)) \cong A/\mathfrak{p}_n.$$

Since $\mathfrak{p}_n$ is prime, Lemma 2.11 implies that the above quotients are integral domains, so $\mathfrak{p}_n A[T] + (T)$ is prime.

The inclusions are proper: Observe that $\mathfrak{p}_i A[T] \cap A = \mathfrak{p}_i$ (this does not hold in general) since for any $\sum_{j=0}^{r} p_0 f_0 \in \mathfrak{p}_i A[T]$ with $p_j \in \mathfrak{p}_i$ and $f_j \in A[T]$, the absolute coefficient lies in $\mathfrak{p}_i$. Hence $\mathfrak{p}_i A[T] \subset \mathfrak{p}_{i+1} A[T]$ since $\mathfrak{p}_i \subset \mathfrak{p}_{i+1}$. Furthermore, $T \notin \mathfrak{p}_n A[T]$ since $1 \notin \mathfrak{p}_n$ (Lemma 1.25). Thus $\mathfrak{p}_n A[T] \subset \mathfrak{p}_n A[T] + (T)$.

(ii) A general observation: Proper inclusion of ideals are stable under taking quotients or localisations. Namely, for an arbitrary ring B, consider ideals $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{c} \subseteq B$ and a subset $S \subseteq B$. If $\mathfrak{b}/\mathfrak{a} = \mathfrak{c}/\mathfrak{a}$, then $\mathfrak{c} \subseteq \mathfrak{b} + \mathfrak{a} = \mathfrak{b}$, a contradiction. If $\mathfrak{b}[S^{-1}] = \mathfrak{c}[S^{-1}]$, then $\mathfrak{c} \subseteq (\mathfrak{b}\overline{S}) \subseteq \mathfrak{b}$, a contradiction.

Now we claim that for consecutive prime ideals $\mathfrak{q}_1 \subset \mathfrak{q}_2$ in $A[T]$, if $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A =: \mathfrak{p}$ in A, then $\mathfrak{q}_1 = \mathfrak{p}A[T]$. This can be seen by passing to the residue field $\kappa(\mathfrak{p})$.

By the previous observation, we obtain $\mathfrak{q}_1\kappa(\mathfrak{p}) \subset \mathfrak{q}_2\kappa(\mathfrak{p}) \subset A[T]\kappa(\mathfrak{p}) \cong \kappa(\mathfrak{p})[T]$. The ideals $\mathfrak{q}_1\kappa(\mathfrak{p})$ are prime because

$$A[T]\kappa(\mathfrak{p})/\mathfrak{q}_1\kappa(\mathfrak{p}) = (A_{\mathfrak{p}}[T]/\mathfrak{p}A_{\mathfrak{p}}[T])/(\mathfrak{q}_{1,\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}[T]) \cong A_{\mathfrak{p}}[T]/\mathfrak{q}_{1,\mathfrak{p}} \cong (A[T]/\mathfrak{q}_1)_{\mathfrak{p}/\mathfrak{q}_1}$$

by Noether's isomorphism theorem and Lemma 2.54. The right-hand side is an integral domain since it is a subring of the field of fractions of the integral domain $A[T]/\mathfrak{q}_1$ (see Example 2.49). By Lemma 2.11, $\mathfrak{q}_1\kappa(\mathfrak{p})$ is prime, and similarly $\mathfrak{q}_2\kappa(\mathfrak{p})$.

$\kappa(\mathfrak{p})[T]$ is a polynomial ring over a field, hence it is a principal ideal domain with $\dim(\kappa(\mathfrak{p})[T]) = 1$. Then necessarily $(0) = \mathfrak{q}_1\kappa(\mathfrak{p}) \cong (\mathfrak{q}_1/\mathfrak{p}A[T])_{\mathfrak{p}/\mathfrak{p}A[T]}$. As we have seen in the previous part, $\mathfrak{p}A[T]$ is prime, so $(\mathfrak{q}_1/\mathfrak{p}A[T])_{\mathfrak{p}/\mathfrak{p}A[T]}$ is a localisation in the integral domain $A[T]/\mathfrak{p}A[T]$. Hence this localisation is (0) if and only if $\mathfrak{q}_1/\mathfrak{p}A[T] = (0)$, i. e. $\mathfrak{q}_1 \subseteq \mathfrak{p}A[T]$. If we would not have equality, then $\mathfrak{p}A[T] = \mathfrak{q}_2$ as $\mathfrak{q}_2$ is the minimal prime above $\mathfrak{q}_1$. But this would imply that $\mathfrak{q}_2\kappa(\mathfrak{p}) = (0)$, a contradiction. Thus $\mathfrak{q}_1 = \mathfrak{p}A[T]$, proving the claim.

As a conclusion, three consecutive prime ideals $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \mathfrak{q}_3 \subset A[T]$ such that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{q}_3 \cap A$ are impossible.

Let $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_m$ be a proper chain of consecutive prime ideals in $A[T]$, e. g. as part of a maximally long chain of prime ideals. Then the chain

$$\mathfrak{q}_0 \cap A \subseteq \cdots \subseteq \mathfrak{q}_m \cap A$$

is a chain of prime ideals in A (Lemma 2.12), which can contain at most $\lceil \frac{m+1}{2} \rceil$ distinct prime ideals. In particular, $m := \dim(A[T])$ is finite and bounded by $\lceil \frac{m+1}{2} \rceil \leq n+1$. This implies $m \leq 2n+1$.

Exercise 8.16 (03.4)**.** Let A be a ring, and let $S \subseteq T \subseteq A$ be multiplicative subsets.

(i) Let $\iota_S \colon A \to S^{-1}A$ be the natural ring map. Show that $\iota_S^{-1}((S^{-1}A)^\times) = S^{\mathrm{sat}}$.

(ii) Show that there exists a unique ring map $\iota \colon S^{-1}A \to T^{-1}A$ such that $\iota \circ \iota_S = \iota_T$, where $\iota_T \colon A \to T^{-1}A$ is the natural ring map.

(iii) Deduce that ι is an isomorphism if and only if $T^{\mathrm{sat}} = S^{\mathrm{sat}}$.

Solution.

(i) Let $a \in \iota_S^{-1}((S^{-1}A)^\times)$, i. e. there exists some $\frac{b}{c} \in S^{-1}A$ such that $\frac{a}{1} \cdot \frac{b}{c} = 1$. By definition, there exists some $s \in S$ such that $sab = sc \in S \subseteq S^{\mathrm{sat}}$. This implies $a \in S^{\mathrm{sat}}$.

Conversely, let $s \in S^{\mathrm{sat}}$. Then there exists some $a \in A$ such that $as \in S$. Otherwise $S^{\mathrm{sat}} \setminus \{as \mid a \in A\} \subset S^{\mathrm{sat}}$, which contains S, would be saturated, contradicting the minimality of S^{sat}. Since $\iota_S(as) \in (S^{-1}A)^\times$, there is some $\frac{b}{c} \in S^{-1}A$ such that $\frac{as}{1} \cdot \frac{b}{c} = \frac{a}{1} \cdot \frac{sb}{c} = 1$. Thus $a \in \iota_S^{-1}((S^{-1}A)^\times)$.

(ii) Since $S \subseteq T$, we know that $\iota_T(S) \subseteq (T^{-1}A)^\times$. Thus by the universal property of localisations, ι_T factors uniquely through ι_S, meaning $\iota \circ \iota_S = \iota_T$ for a unique $\iota \colon S^{-1}A \to T^{-1}A$.

(iii) Assume that ι is an isomorphism. Then $T^{\mathrm{sat}} = \iota_T^{-1}((T^{-1}A)^\times) = \iota_S^{-1}(\iota^{-1}((T^{-1}A)^\times)) = \iota_S^{-1}((S^{-1}A)^\times) = S^{\mathrm{sat}}$ by (i).

Conversely, suppose that $S^{\mathrm{sat}} = T^{\mathrm{sat}}$. Then $\iota_S(T) \subseteq \iota_S(T^{\mathrm{sat}}) = \iota_S(S^{\mathrm{sat}}) \subseteq (S^{-1}A)^\times$ by Remark 2.37. The universal property of localisations implies that ι_S factors uniquely through ι_T, namely through $\iota' \colon T^{-1}A \to S^{-1}A$ with $\iota' \circ \iota_T = \iota_S$.

Again by the universal property, ι_S factors uniquely through ι_S via $\mathrm{id}_{S^{-1}A}$. But we also have $\iota_S = \iota' \circ \iota \circ \iota_S$, hence $\iota' \circ \iota = \mathrm{id}_{S^{-1}A}$. Similarly $\iota \circ \iota' = \mathrm{id}_{T^{-1}A}$, thus ι is an isomorphism.

8.4 Modules

Exercise 8.17 (04.1)**.** Let A be a ring.

(i) Assume that $f_n \in A[\![T]\!]$ with $n \geq 0$ is a sequence of elements such that $f_n \in (T)^n$ for all $n \geq 0$. Show that there exists a unique element $f \in A[\![T]\!]$ such that $f - \sum_{k=0}^n f_k \in (T)^{n+1}$ for all $n \geq 0$.

(ii) Assume that A is noetherian. Show that $A[\![T]\!]$ is noetherian.

Solution.

(i) Let $f_n = \sum_{i=n}^\infty a_{in} T^i$ for all $n \geq 0$ and $f = \sum_{i=0}^\infty b_i T^i$. Then we have

$$f - \sum_{k=0}^n f_k \equiv \sum_{i=0}^n b_i T^i - \sum_{k=0}^n \sum_{i=k}^n a_{ik} T^i = \sum_{i=0}^n \left(b_i - \sum_{k=0}^i a_{ik} \right) T^i \equiv 0 \mod (T)^{n+1}.$$

Thus the only f satisfying the desired property is given by $b_i \coloneqq \sum_{k=0}^i a_{ik}$ for all $i \geq 0$.

(ii) We imitate the proof of Hilbert's basis theorem 3.30, but with coefficients of least degree.

Let $\mathfrak{a} \subseteq A[\![T]\!]$ be any ideal. Consider the ideal

$$\mathfrak{b} \coloneqq \{a \in A \mid \text{there exists } aT^n + \cdots \in \mathfrak{a}\} \subseteq A.$$

As A is noetherian, $\mathfrak{b} = (a_1, \ldots, a_r)$ is finitely generated. For each $i = 1, \ldots, r$, pick $f_i = a_i T^{n_i} + \cdots \in \mathfrak{a}$ with n_i minimal. Put $n \coloneqq \max\{n_1, \ldots, n_r\}$. We claim that for every $g \in \mathfrak{a}$, there exists some $g_0 \in A[T]$ with $\deg(g_0) < n$ such that $g - g_0 \in (f_1, \ldots, f_r)$.

Set g_0 as the image of g in $A[\![T]\!]/(T)^n$. We proceed with $g - g_0 \in (T)^n$, so w. l. o. g., assume $g = bT^m + \cdots \in (T)^m$ with $m \geq n$. Since $b \in \mathfrak{b}$, we can write $b = x_1 a_1 + \cdots + x_r a_r$ with $x_i \in A$. We define $g_m \coloneqq \sum_{i=1}^r x_i T^{m-n_i} f_i \in (f_1, \ldots, f_r)$, so that $g_m \in (T)^m$ and $g - g_m \in (T)^{m+1}$. Now we proceed with $g - g_m$, and by induction, we obtain a sequence $g_m \in (f_1, \ldots, f_n)$ for all $m \geq n$ with $g_m \in (T)^m$. By (i), we can define $g' \coloneqq \sum_{m=n}^\infty g_m \in (f_1, \ldots, f_n)$. The g_m are chosen in such a way that $g' \equiv g \mod (T)^m$ for all $m \geq n$, so $g = g'$.

Now consider the A-module $M = \bigoplus_{i=0}^{n-1} AT^i \cong A^{\oplus n}$, which is finitely generated. By Corollary 3.25, M is noetherian, so $M \cap \mathfrak{a} = (g_1, \ldots, g_s)$ is finitely generated. By the above claim, $\mathfrak{a} = (f_1, \ldots, f_r, g_1, \ldots, g_s)$ is finitely generated.

Exercise 8.18 (04.2)**.**

(i) Let A be a ring of power series in $\mathbb{C}[\![z]\!]$ with a positive radius of convergence. Show that A is noetherian.

(ii) Show that the ring of holomorphic functions $\mathbb{C} \to \mathbb{C}$ is not noetherian.

Hint: One possible approach is to use the relation $\sin(2x) = 2\sin(x)\cos(x)$.

Solution.

(i) Let $(0) \neq \mathfrak{a} \subseteq A$ be an ideal and $f = \sum_{i=n}^{\infty} a_i z^i \in \mathfrak{a} \setminus \{0\}$ with $a_n \in \mathbb{C}^\times$. Then we can write $f = z^n g$ for a suitable $g \in \mathbb{C}[\![z]\!]$. Since g has the same coefficients as f, g has the same convergence radius as f (recall from complex analysis that the convergence radius of f is $1/\limsup_{i\to\infty}|a_i|^{1/i}$), hence $g \in A$. By Proposition 1.47, $g \in \mathbb{C}[\![z]\!]^\times$, therefore $g^{-1} \in \mathbb{C}[\![z]\!]$ exists. We claim that g^{-1} has positive convergence radius, so $g^{-1} \in A$, and thus $g \in A^\times$.

Let $g = \sum_{i=0}^{\infty} b_i z^i$ with $b_0 \neq 0$ and $g^{-1} = \sum_{i=0}^{\infty} c_i z^i$ such that $gg^{-1} = 1$. W. l. o. g. we may assume $b_0 = 1$, after dividing g by b_0. Thus we recursively obtain $c_0 = b_0$ and $c_i = \sum_{k=0}^{i-1} b_k c_{i-k}$ for all $i \geq 1$. Since g converges uniformly and absolutely on any closed ball inside its convergence radius, g as a complex function is continuous and vanishes at 0. Therefore we can find some $\varepsilon > 0$ such that $\sum_{i=0}^{\infty}|b_i z^i| \leq 1$ for all $|z| \leq \varepsilon$. This yields $|c_i| \leq \varepsilon^{-i}$ by induction: We have $|c_0| = 1$ and

$$|c_i| \leq \sum_{k=0}^{i-1}|b_k c_{i-k}| \leq \varepsilon^{-i}\sum_{k=0}^{i-1}|b_k|\varepsilon^k \leq \varepsilon^{-i}.$$

We obtain $1/\limsup_{i\to\infty}|c_i|^{1/i} \geq \varepsilon$ for the convergence radius of g^{-1}.

Hence $f = z^n g$ with $g \in A^\times$ and $(f) = (z^n)$. This implies $\mathfrak{a} = \bigcup_{f\in\mathfrak{a}\setminus\{0\}}(f) = (z^k)$ for some suitable $k \geq 0$. In particular, $\mathfrak{a}$ is finitely generated.

(ii) We claim that the infinite chain $(\sin(x)) \subset (\sin(\frac{x}{2})) \subset \cdots \subset (\sin(2^{-n}x)) \subset \cdots$ exists. We only show $(\sin(x)) \subset (\sin(\frac{x}{2}))$, the other inclusions are analogous. Since $\sin(x) = 2\sin(\frac{x}{2})\cos(\frac{x}{2})$, we have $(\sin(x)) \subseteq (\sin(\frac{x}{2}))$. This inclusion is proper, as otherwise $\sin(x) \mid \sin(\frac{x}{2})$ for all $x \in \mathbb{C}$, and in particular for $x = \pi$, $0 \mid 1$, a contradiction.

Exercise 8.19 (**Cayley-Hamilton theorem**, 04.3)**.**

(i) Let $n \geq 1$, $A = \mathbb{Z}[a_{ij} \mid 1 \leq i, j \leq n]$ and $M := (a_{ij})_{ij} \in M_n(A)$. Recall that $\operatorname{char}(M, X) \in A[X]$ is the characteristic polynomial of M. Show that $\operatorname{char}(M, M) = 0$.

Hint: You may use the Cayley-Hamilton theorem from linear algebra.

(ii) Let $n \geq 1$, A be any ring and $M \in M_n(A)$. Show that $\operatorname{char}(M, M) = 0$.

Solution.

(i) Consider the canonical embedding $A \hookrightarrow \operatorname{Quot}(A)$ (A is an integral domain). Since $\operatorname{Quot}(A)$ is a field, by Cayley-Hamilton 8.19, $\operatorname{char}(M, M) = 0$. But this also holds in A since the embedding maps $M \mapsto M$.

(ii) There is always the map $\mathbb{Z} \to A$. By the universal property of polynomial rings, there is a map $B := \mathbb{Z}[X_{ij} \mid 1 \leq i, j \leq n] \to A$ evaluating $X_{ij} \mapsto a_{ij}$. By (i), $\operatorname{char}(M, M) = 0$ holds in B. The evaluation maps $0 \mapsto 0$, so $\operatorname{char}(M, M) = 0$ holds in A too.

Exercise 8.20 (04.4)**.** Let A be a principal ideal domain.

(i) Let $a \in A \setminus \{0\}$ and $\pi \in A$ prime. Set $B := A/a$. For any $n \geq 0$, show that

$$\dim_{A/\pi} \pi^n B/\pi^{n+1}B = \begin{cases} 0, & \text{if } \nu_\pi(a) \leq n, \\ 1, & \text{if } \nu_\pi(a) \geq n+1. \end{cases}$$

(ii) Assume that $M = A^r \oplus A/a_1 \oplus \cdots \oplus A/a_k$ and $N = A^s \oplus A/b_1 \oplus \cdots \oplus A/b_l$ with $a_1, \ldots, a_k, b_1, \ldots, b_l \in A \setminus \{0\}$ and $a_1 \mid \cdots \mid a_n$ as well as $b_1 \mid \cdots \mid b_l$. Show that if $M \cong N$ as A-modules, then $r = s$, $k = l$ and $a_i = b_i$ up to units.

Solution.

(i) If $\nu_\pi(a) \geq n+1$, then $\pi^{n+1} \mid a$, so $(a) \subseteq (\pi^{n+1}) \subseteq (\pi^n)$. Then by Noether's isomorphism theorem, we have $\pi^n B/\pi^{n+1}B \cong \pi^n A/\pi^{n+1}A$. As A is a principal ideal domain, (π) is maximal, so due to Exercise 8.10 (notice that A is not a field since there are primes in A), this has dimension 1.

If $\nu_\pi(a) \leq n$, then

$$(a, \pi^{n+1}) = \pi^{\nu_\pi(a)}(a/\pi^{\nu_\pi(a)}, \pi^{n+1-\nu_\pi(a)}) = \pi^{\nu_\pi(a)}A = (\pi^{\nu_\pi(a)})$$

since $a/\pi^{\nu_\pi(a)}$ has no prime factor π. Hence $\pi^n \in (a, \pi^{n+1})$, and thus $\pi^n B \subseteq \pi^{n+1}B = (a, \pi^{n+1})/a$. Therefore $\pi^n B/\pi^{n+1}B = 0$.

(ii) Pick any prime $\pi \in A$ and set $n \coloneqq \max\{\nu_\pi(a_k), \nu_\pi(b_l)\}$. By the divisibility condition, we have $\nu_\pi(a_i), \nu_\pi(b_j) \leq n$ for all $1 \leq i \leq k$ and $1 \leq j \leq l$. Since A is a principal ideal domain, $\pi A \subset A$ is maximal. So by (i) and Exercise 8.10, we obtain

$$r = r\dim(\pi^n A/\pi^{n+1}A) + \sum_{i=1}^{k} \dim((\pi^n A/a_i)/(\pi^{n+1}A/a_i)) = \dim(\pi^n M/\pi^{n+1}M)$$
$$= \dim(\pi^n N/\pi^{n+1}N) = \cdots = s.$$

Now we consider the quotient of M and N w. r. t. $A^r = A^s$, so w. l. o. g. we may assume $r = s = 0$.

Now pick any prime factor $\pi \in A$ of a_k, and set $n \coloneqq \nu_\pi(a_k)$. By (i), we obtain, similarly to the above,

$$0 = \dim(\pi^n M/\pi^{n+1}M) = \dim(\pi^n N/\pi^{n+1}N), \qquad 0 < \dim(\pi^{n-1}M/\pi^n M) = \dim(\pi^{n-1}N/\pi^n N).$$

The first relation implies $\nu_\pi(b_l) \leq n$, the second implies $\nu_\pi(b_l) \geq n$. We can do this for every prime factor of a_k and b_l, therefore both have the same prime factors and $a_k = b_l$ up to units. Now we consider the quotient of M and N w. r. t. $A/a_k = A/b_l$ and continue inductively.

If $A/a_1 \oplus \cdots \oplus A/a_m \cong 0$ with $m \leq k$ were left, then $A/a_i = 0$ for all $1 \leq i \leq m$. Hence they are negligible, and we can assume $k = l$.

Exercise 8.21 (05.1)**.** Let A be a ring, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ be ideals such that $\bigcap_{i=1}^n \mathfrak{a}_i = (0)$. Assume that each ring $A/\mathfrak{a}_i$ is noetherian. Show that A is noetherian.

Solution. We observe the following: If $A/\mathfrak{a}_i$ is noetherian as a ring, i. e. as an $A/\mathfrak{a}_i$-module, then it is also noetherian as an A-module. Say $\tilde{\mathfrak{a}} \coloneqq (\bar{a}_1, \ldots, \bar{a}_n) \subseteq A/\mathfrak{a}_i$ is any ideal. Then each element of $\tilde{\mathfrak{a}}$ is of the form $\bar{x}_1\bar{a}_1 + \cdots + \bar{x}_n\bar{a}_n = x_1\bar{a}_1 + \cdots + x_n\bar{a}_n$, so $\tilde{\mathfrak{a}}$ is finitely generated as an A-submodule.

We further claim that if M and N are noetherian A-modules, then so is $M \times N$. This is because $N \cong 0 \times N$ and $M \cong (M \times N)/(0 \times N)$ are noetherian submodules and quotient modules, resp. By Proposition 3.24, $M \times N$ is noetherian.

Back to the actual task. By induction $B \coloneqq \prod_{i=1}^n A/\mathfrak{a}_i$ is a noetherian A-module. Consider the A-linear map $\phi\colon A \to B$, $1 \mapsto (\bar{1}, \ldots, \bar{1})$. By the homomorphism theorem, we obtain $A \cong A/\bigcap_{i=1}^n \mathfrak{a}_i \cong \mathrm{im}(\phi)$, which is a submodule of B. Therefore A is noetherian due to Proposition 3.24.

Exercise 8.22 (05.2)**.** Consider the matrix

$$S \coloneqq \begin{pmatrix} -36 & 14 & -24 \\ 18 & 6 & 12 \end{pmatrix} \in M_{2\times 3}(\mathbb{Z}).$$

Determine its elementary divisors and the kernel/cokernel of the map $S\colon \mathbb{Z}^3 \to \mathbb{Z}^2$ (up to isomorphism).

Solution. We have

$$S \sim \begin{pmatrix} -72 & 2 & -48 \\ 18 & 6 & 12 \end{pmatrix} \sim \begin{pmatrix} -72 & 2 & -48 \\ 234 & 0 & 156 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 234 & 156 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & -78 & 156 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 78 & 0 \end{pmatrix},$$

hence the elementary divisors of S are 2 and 78. Using Lemma 3.42, we have

$$\ker(S) \cong \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle \cong \mathbb{Z} \qquad \text{and} \qquad \mathrm{coker}(S) \cong \mathbb{Z}^2/\left\langle \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 78 \end{pmatrix} \right\rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/78.$$

8.5 Basics in Homological Algebra

Exercise 8.23 (B05.3)**.** Let A be a ring and $\mathfrak{a} \subseteq A$ an ideal. Let M and N_i for all $i \in I$ be A-modules for some set I. Show that there are the following unique isomorphisms:

(i) $\bigoplus_{i\in I}(N_i \otimes_A M) \to (\bigoplus_{i\in I} N_i) \otimes_A M$, given by $(\dots, 0, n_i \otimes m, 0, \dots) \mapsto (\dots, 0, n_i, 0, \dots) \otimes m$.

(ii) $A/\mathfrak{a} \otimes_A M \to M/\mathfrak{a}M$, given by $(a + \mathfrak{a}) \otimes m \mapsto am + \mathfrak{a}M$.

Solution.

(i) By the universal property of tensor products, the A-bilinear map

$$\left(\bigoplus_{i\in I} N_i\right) \times M \to \bigoplus_{i\in I}(N_i \otimes_A M), \qquad ((n_i)_i, m) \mapsto (n_i \otimes m)$$

factors through the unique A-linear map

$$\Psi\colon \left(\bigoplus_{i\in I} N_i\right) \otimes_A M \to \bigoplus_{i\in I}(N_i \otimes_A M), \qquad (n_i)_i \otimes m \mapsto (n_i \otimes m)_i.$$

Conversely, for each $i \in I$ by the universal property, the A-bilinear map

$$N_i \times M \to \left(\bigoplus_{i\in I} N_i\right) \otimes_A M, \qquad (n_i, m) \mapsto (\dots, 0, n_i, 0, \dots) \otimes m$$

factors through the unique A-linear map

$$\Phi_i\colon N_i \otimes_A M \to \left(\bigoplus_{i\in I} N_i\right) \otimes_A M, \qquad n_i \otimes m \mapsto (\dots, 0, n_i, 0, \dots) \otimes m.$$

By the universal property of direct sums (the coproduct in the category of A-modules), there is a unique A-linear map

$$\Phi\colon \bigoplus_{i\in I}(N_i \otimes_A M) \to \left(\bigoplus_{i\in I} N_i\right) \otimes_A M, \qquad n_i \otimes m \mapsto (\dots, 0, n_i, 0, \dots) \otimes m$$

such that each Φ_i factors through Φ (via $\Phi_i = \Phi \circ \iota_i$ with the canonical inclusion ι_i).

We easily check that, by bilinearity of tensor products, $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are both the identity map on elementary tensors, and thus on the whole tensor product. Hence Φ is a unique A-linear isomorphism.

(ii) We have the following chain of isomorphisms:

$$\begin{aligned}\operatorname{Hom}_A(A/\mathfrak{a} \otimes_A M, P) &\cong \operatorname{Bihom}_A(A/\mathfrak{a}, M; P) \cong \operatorname{Hom}_A(A/\mathfrak{a}, \operatorname{Hom}_A(M, P)) \cong \operatorname{Hom}_{A/\mathfrak{a}}(M, P)\\ &\cong \operatorname{Hom}_A(M/\mathfrak{a}M, P),\end{aligned}$$

given by

$$f \mapsto [(\bar{a}, m) \mapsto f(\bar{a} \otimes m)] \mapsto [\bar{a} \mapsto f(\bar{a} \otimes -)] \mapsto [\bar{a}m \mapsto f(\bar{a} \otimes m)] \mapsto [a\bar{m} \mapsto f(\bar{a} \otimes m)].$$

The first isomorphism follows from the universal property of tensor products, the second one is Remark 4.2. Therefore $M/\mathfrak{a}M$ fulfils the same universal property as $A/\mathfrak{a} \otimes_A M$, and since the tensor product is unique up to unique isomorphism, they are isomorphic via the unique isomorphism $\bar{a} \otimes m \mapsto a\bar{m}$.

Exercise 8.24 (B05.4)**.** Let A be a ring and M and N be A-modules. A bilinear map $(-,-)\colon M \times M \to N$ is called *symmetric* if $(m_1, m_2) = (m_2, m_1)$ for all $m_1, m_2 \in M$. It is called *alternating* if $(m, m) = 0$ for all $m \in M$.

(i) Construct an A-module $\operatorname{Sym}^2_A(M)$ and a symmetric bilinear map $\iota\colon M \times M \to \operatorname{Sym}^2_A(M)$ with the following universal property: For every A-module N and for every symmetric bilinear map $(-,-)\colon M \times M \to N$, there exists a unique A-linear map $\Phi\colon \operatorname{Sym}^2_A(M) \to N$ such that $(-,-) = \Phi \circ \iota$.
Construct similarly an A-module $\Lambda^2_A(M)$ with a universal alternating bilinear map $\gamma\colon M \times M \to \Lambda^2_A(M)$.

(ii) Show that $\operatorname{Sym}^2_A(A^n)$ and $\Lambda^2_A(A^n)$ are free A-modules of ranks $\frac{1}{2}n(n+1)$ and $\frac{1}{2}n(n-1)$, resp. (*rank* is the cardinality of the free generating set of these A-modules).

Solution.

(i) We define
$$\operatorname{Sym}^2_A(M) \coloneqq M \otimes_A M / \langle m_1 \otimes m_2 - m_2 \otimes m_1 \mid m_1, m_2 \in M \rangle.$$
Furthermore, let
$$\iota\colon M \times M \to M \otimes_A M \to \operatorname{Sym}^2_A(M)$$
be the composition of the universal bilinear map before the canonical A-linear projection. Then ι is symmetric as $\iota(m_1, m_2) = \overline{m_1 \otimes m_2} = \overline{m_2 \otimes m_1} = \iota(m_2, m_1)$ for all $m_1, m_2 \in M$.
This fulfils the proposed universal property: By the universal property of tensor products, $(-,-)$ factors through a unique A-linear map $\Psi\colon M \otimes_A M \to N$. Since $(-,-)$ is symmetric, we have $\Psi(m_1 \otimes m_2 - m_2 \otimes m_1) = (m_1, m_2) - (m_2, m_1) = 0$ for all $m_1, m_2 \in M$. This shows that $\langle m_1 \otimes m_2 - m_2 \otimes m_1 \rangle \subseteq \ker(\Psi)$, hence by the universal property of quotients, Ψ factors through a unique A-linear map $\Phi\colon \operatorname{Sym}^2_A(M) \to N$. In total, $(-,-)$ factors through the unique Φ.
The case for alternating bilinear maps is analogous. We define
$$\Lambda^2_A(M) \coloneqq M \otimes_A M / \langle m \otimes m \mid m \in M \rangle \qquad \text{and} \qquad \gamma\colon M \times M \to M \otimes_A M \to \Lambda^2_A(M)$$
in the natural way. Notice that γ is alternating as $\gamma(m, m) = \overline{m \otimes m} = 0$ for all $m \in M$.
This fulfils the universal property: $(-,-)$ factors through a unique A-linear map $\Psi\colon M \otimes_A M \to N$ with $\Psi(m \otimes m) = (m, m) = 0$ for all $m \in M$. Thus Ψ factors through a unique A-linear map $\Phi\colon \Lambda^2_A(M) \to N$.

(ii) The idea is to look at the matrix depiction which every bilinear map admits. For symmetric $(-,-)$, the matrix is symmetric and thus is fully defined by its upper triangular structure (including the principal diagonal). For alternating $(-,-)$, notice that they are skew-symmetric (for all $m_1, m_2 \in M$ we have $0 = (m_1 + m_2, m_1 + m_2) = (m_1, m_2) + (m_2, m_1)$) and definite ($(m, m) = 0$ for all $m \in M$). The corresponding matrix is thus fully defined by its proper upper triangular structure (with principal diagonal 0).
We first consider $\operatorname{Sym}^2_A(A^n)$. The symmetric A-bilinear map
$$A^n \times A^n \to A^{n(n+1)/2}, \qquad (e_i, e_j) \mapsto \begin{cases} e_{ij}, & \text{if } i \le j, \\ e_{ji}, & \text{if } i > j, \end{cases}$$
factors through the unique A-linear map
$$\Phi\colon \operatorname{Sym}^2_A(A^n) \to A^{n(n+1)/2}, \qquad e_i \otimes e_j \mapsto \begin{cases} e_{ij}, & \text{if } i \le j, \\ e_{ji}, & \text{if } i > j, \end{cases}$$
by the universal property in (i). Moreover, we define the A-linear map
$$\Psi\colon A^{n(n+1)/2} \to \operatorname{Sym}^2_A(A^n), \qquad e_{ij} \mapsto e_i \otimes e_j \quad \text{for } 1 \le i \le j \le n.$$
Now we have $\Phi(\Psi(e_{ij})) = e_{ij}$ and
$$\Psi(\Phi(e_i \otimes e_j)) = \begin{cases} e_i \otimes e_j, & \text{if } i \le j, \\ e_j \otimes e_i = e_i \otimes e_j, & \text{if } i > j. \end{cases}$$
Thus Φ and Ψ are inverses on generators and thus on the whole A-modules. Hence Φ is an isomorphism, and $\operatorname{Sym}^2_A(A^n) \cong A^{n(n+1)/2}$.

The case $\Lambda^2_A(A^n)$ is very similar. We consider the alternating A-bilinear map

$$A^n \times A^n \to A^{n(n-1)/2}, \qquad (e_i, e_j) \mapsto \begin{cases} e_{ij}, & \text{if } i < j, \\ -e_{ji}, & \text{if } i > j, \\ 0, & \text{if } i = j. \end{cases}$$

Notice that $(e_i + e_j, e_i + e_j) = (e_i + e_i) + (e_i, e_j) + (e_j, e_i) + (e_j, e_j) = 0$ for all $1 \leq i, j \leq n$. This map factors through the unique A-linear map

$$\Phi\colon \Lambda^2_A(A^n) \to A^{n(n-1)/2}, \qquad e_i \otimes e_j \mapsto \begin{cases} e_{ij}, & \text{if } i < j, \\ -e_{ji}, & \text{if } i > j, \\ 0, & \text{if } i = j, \end{cases}$$

by the universal property in (i). Moreover, we define the A-linear map

$$\Psi\colon A^{n(n-1)/2} \to \Lambda^2_A(A^n), \qquad e_{ij} \mapsto e_i \otimes e_j \quad \text{for } 1 \leq i < j \leq n.$$

Now we have $\Phi(\Psi(e_{ij})) = e_{ij}$ and

$$\Psi(\Phi(e_i \otimes e_j)) = \begin{cases} e_i \otimes e_j, & \text{if } i < j, \\ -e_j \otimes e_i = e_i \otimes e_j, & \text{if } i > j, \\ 0, & \text{if } i = j. \end{cases}$$

Thus Φ is an isomorphism, and $\Lambda^2_A(A^n) \cong A^{n(n-1)/2}$.

Exercise 8.25 (06.1)**.** Let A be a ring, $f \in A$ regular, $\mathfrak{a} = (f)$ and $\mathfrak{b} \subseteq A$ an ideal. Show that the natural map $\mathfrak{a} \otimes_A \mathfrak{b} \to \mathfrak{ab}$, $a \otimes b \mapsto ab$ is an isomorphism.

Solution. Let ϕ be the map from the problem statement. Then ϕ is surjective, since $\mathfrak{ab} = \{fb \mid b \in \mathfrak{b}\}$ and $\phi(f \otimes b) = fb$. Furthermore, ϕ is injective, since $\mathfrak{a} \otimes_A \mathfrak{b} = \{f \otimes b \mid b \in \mathfrak{b}\}$ by bilinearity, and the multiplication map $\phi(f \otimes -)\colon \mathfrak{b} \to \mathfrak{ab}$, $b \mapsto fb$ is injective because f is regular and Remark 1.18.

Exercise 8.26 (06.2)**.** Let A be a ring, and let M and N_i for $i \in I$ be A-modules with any set I.

(i) Assume that M is finitely generated (resp. finitely presented). Show that the natural map

$$M \otimes_A \left(\prod_{i \in I} N_i \right) \to \prod_{i \in I} (M \otimes_A N_i), \qquad m \otimes (n_i)_i \mapsto (m \otimes n_i)_i$$

is surjective (resp. bijective).

(ii) Take $A = \mathbb{Z}[X_i \mid i \geq 0]$ and $J = (X_i \mid i \geq 0)$. Show that the natural map $A/J \otimes_A A[\![T]\!] \to A/J[\![T]\!]$ is not surjective.

Remark: Notice that $A[\![T]\!] = \prod_{i \geq 0} AT^i$.

We need the following statement for this problem.

Proposition 8.27. *Direct products are exact: Assume that for all $i \in I$,*

$$M_i \xrightarrow{f_i} N_i \xrightarrow{g_i} P_i$$

is an exact sequence of A-modules for all $i \in I$. Then

$$\textstyle\prod_{i \in I} M_i \xrightarrow{(f_i)_i} \prod_{i \in I} N_i \xrightarrow{(g_i)_i} \prod_{i \in I}$$

is an exact sequence.

Proof. Notice that by the universal property of direct products, the unique map $(f_i)_i \colon \prod_{i\in I} M_i \to \prod_{i\in I} N_i$ is given by $(m_i)_i \mapsto (f_i(m_i))_i$, and similarly $(g_i)_i$.

Observe that by construction, $\operatorname{im}((f_i)_i) = \prod_{i\in I} \operatorname{im}(f_i)$ and $\ker((g_i)_i) = \prod_{i\in I} \ker(g_i)$. Thus through the exactness at N_i, we have $\prod_{i\in I} \operatorname{im}(f_i) = \prod_{i\in I} \ker(g_i)$. This proves the exactness at $\prod_{i\in I} N_i$. □

Solution.

(i) Let M be finitely generated, i. e. $A^{\oplus n} \twoheadrightarrow M \to 0$ is exact for some $n \in \mathbb{N}$. Consider the following diagram:

$$\begin{array}{ccccc} A^{\oplus n} \otimes_A \left(\prod_{i\in I} N_i\right) & \longrightarrow\!\!\!\!\rightarrow & M \otimes_A \left(\prod_{i\in I} N_i\right) & \longrightarrow & 0 \\ \downarrow & & \vdots & & \\ \prod_{i\in I}(A^{\oplus n} \otimes_A N_i) & \longrightarrow\!\!\!\!\rightarrow & \prod_{i\in I}(M \otimes_A N_i) & \longrightarrow & 0 \end{array}$$

The rows are exact since tensor products and direct products are right-exact. The vertical arrows are given by the universal property of direct products, which are unique such that the diagram

$$\begin{array}{ccc} a \otimes (n_i)_i & \longmapsto & m \otimes (n_i)_i \\ \downarrow & & \downarrow \\ (a \otimes n_i)_i & \longmapsto & (m \otimes n_i)_i \end{array}$$

commutes. By Proposition 4.25, we have

$$A^{\oplus n} \otimes_A \left(\prod_{i\in I} N_i\right) \cong \left(A \otimes_A \left(\prod_{i\in I} N_i\right)\right)^{\oplus n} \cong \left(\prod_{i\in I} N_i\right)^{\oplus n},$$
$$\prod_{i\in I}(A^{\oplus n} \otimes_A N_i) \cong \prod_{i\in I}(A \otimes_A N_i)^{\oplus n} \cong \prod_{i\in I} N_i^{\oplus n}.$$

Recall that direct sums and finite direct products are isomorphic, and that direct products commute. Hence the two right-hand sides are isomorphic, and the left vertical arrow in the commutative diagram is actually an isomorphism. This map is in particular surjective. Since the square commutes, the dashed arrow must be surjective as well.

Let M be finitely presented, i. e. $A^{\oplus m} \to A^{\oplus n} \to M \to 0$ is exact for some $m, n \in \mathbb{N}$. Similarly to the above, we obtain the commutative diagram

$$\begin{array}{ccccccccc} A^{\oplus m} \otimes_A \left(\prod_{i\in I} N_i\right) & \longrightarrow & A^{\oplus n} \otimes_A \left(\prod_{i\in I} N_i\right) & \longrightarrow\!\!\!\!\rightarrow & M \otimes_A \left(\prod_{i\in I} N_i\right) & \longrightarrow & 0 & \longrightarrow & 0 \\ \downarrow\cong & & \downarrow\cong & & \vdots & & \downarrow & & \downarrow \\ \prod_{i\cap I}(A^{\oplus m} \otimes_A N_i) & \longrightarrow & \prod_{i\in I}(A^{\oplus n} \otimes_A N_i) & \longrightarrow\!\!\!\!\rightarrow & \prod_{i\in I}(M \otimes_A N_i) & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

with exact rows. Here, we extended the diagram to the right with one term of 0s in each row. Since the outer four vertical arrows are isomorphisms, by the five lemma exercise 8.35, the dashed arrow is an isomorphism as well.

(ii) We claim that $\bar{1} \otimes \sum_{i=0}^{\infty} X_i T^i \in A/J \otimes_A A[\![T]\!]$ is not 0. Suppose that it is 0. By Exercise 8.23, we have $A/J \otimes_A A[\![T]\!] \cong A[\![T]\!]/JA[\![T]\!]$, and this isomorphism maps $\bar{1} \otimes \sum_{i=0}^{\infty} X_i T^i \mapsto \sum_{i=0}^{\infty} X_i T^i + JA[\![T]\!]$, which must be 0 as well. This means $\sum_{i=0}^{\infty} X_i T^i \in JA[\![T]\!]$, i. e. $\sum_{i=0}^{\infty} X_i T^i = \sum_{i=1}^{n} X_{k_i} m_i$ with $k_i \geq 0$ and $m_i \in A[\![T]\!]$, since we can write every element from J as a finite A-linear combination of indeterminants. Then $X_i \in (X_{k_1}, \ldots, X_{k_n}) \subseteq A$ for each $i \geq 0$, which is impossible as n is finite.

We observe that under the map from the problem statement, we have $\bar{1} \otimes \sum_{i=0}^{\infty} X_i T^i \mapsto \sum_{i=0}^{\infty} \bar{X}_i T^i = 0$, so the kernel of this map is non-trivial, and hence this map is not injective.

Exercise 8.28 (06.3)**.** Let k be a field, K/k an algebraic field extension, and $\bar{k}$ the algebraic closure of k.

(i) If $V \hookrightarrow W$ is a k-linear injection of k-vector spaces, show that $V \otimes_k \bar{k} \to W \otimes_k \bar{k}$ is a $\bar{k}$-linear injection.

(ii) Show that K/k is separable if and only if the ring $K \otimes_k \bar{k}$ is reduced.

Solution.

(i) $\bar{k}$ is a k-vector space, and thus flat by Example 4.67. Proposition 4.71 gives the statement.

(ii) Let K/k be separable. Suppose that $K \otimes_k \bar{k}$ is not reduced, i. e. there exists a nilpotent element $\sum_{i=1}^r a_i \otimes b_i \in K \otimes_k \bar{k}$. Define $k' \coloneqq k(a_1, \dots, a_r) \subseteq K$. Then k'/k is algebraic and hence finite. Moreover, k'/k is separable, so by Example 4.46, $k' \otimes_k \bar{k} \cong \prod_{i=1}^{[k':k]} \bar{k}$ is reduced. This contradicts $\sum_{i=1}^r a_i \otimes b_i \in k' \otimes_k \bar{k} \subseteq K \otimes_k \bar{k}$ (for the inclusion, see (i)).

Conversely, let $K \otimes_k \bar{k}$ be reduced. Suppose that there is some inseparable $\alpha \in K$. Since K/k is algebraic, there exists $f(T) \coloneqq \min_{K/k}(\alpha, T) = \prod_{i=1}^r (T - a_i)^{d_i}$ with $a_i \in \bar{k}$, $a_i \neq a_j$ for all $i \neq j$ and $d_i \geq 2$ for at least one i, say $d_1 \geq 2$. By a similar reasoning to Example 4.46, we obtain

$$k(\alpha) \otimes_k \bar{k} \cong k[T]/(f(T)) \otimes_k \bar{k} \cong \bar{k}[T]/(f(T)) \cong \prod_{i=1}^r \bar{k}[T]/(T - a_i)^{d_i}.$$

Since $d_1 \geq 2$, there is a nilpotent element in the right-hand side, namely $(T - a_i, 0, \dots, 0)$. Thus $k(\alpha) \otimes_k \bar{k} \subseteq K \otimes_k \bar{k}$ (we used (i) again) are both not reduced, a contradiction.

Exercise 8.29 (06.4)**.** Let $A \neq 0$ be a ring, and let I be an **invertible** A-module, i. e. there exists an A-module J such that $I \otimes_A J \cong A$. Let $\varphi \colon M \to N$ be an A-linear map.

(i) Show that φ is zero (resp. injective, resp. surjective) if and only if $\varphi \otimes \mathrm{id}_I \colon M \otimes_A I \to N \otimes_A I$ is so.

(ii) Show that I is finitely generated.

Solution.

(i) On surjectivity: Since tensoring is right-exact, if φ is surjective, then $\varphi \otimes \mathrm{id}_I$ is surjective as well. If $\varphi \otimes \mathrm{id}_I$ is surjective, then $\varphi \otimes \mathrm{id}_I \otimes \mathrm{id}_J \cong \varphi$ is surjective because $M \otimes_A I \otimes_A J \cong M$ and similar for N by assumption.

On zero maps: Similar to the above, $\varphi \cong \varphi \otimes \mathrm{id}_I \otimes \mathrm{id}_J = 0$ if and only if $\varphi \otimes \mathrm{id}_I = 0$.

On injectivity: This is more difficult. Consider the canonical inclusion $\iota \colon \ker(\varphi) \hookrightarrow M$. Then $\varphi \circ \iota = 0$. By functoriality of the tensor product (Observation 4.9), we have $(\varphi \otimes \mathrm{id}_I) \circ (\iota \otimes \mathrm{id}_I) = 0$. Suppose that $\varphi \otimes \mathrm{id}_I$ is injective. Then $\iota \otimes \mathrm{id}_I$ must be zero. Tensoring with J yields that $0 = \iota \otimes \mathrm{id}_I \otimes \mathrm{id}_J \cong \iota$. But ι is injective, so $\ker(\varphi) = 0$. The converse is analogous by considering $\iota \colon \ker(\varphi \otimes \mathrm{id}_I) \hookrightarrow M \otimes_A \mathrm{id}_I$.

(ii) By assumption, an isomorphism $\varphi \colon I \otimes_A J \to A$ exists. Let $\varphi^{-1}(1) = \sum_{i=1}^n a_i \otimes b_i \in I \otimes_A J$. We define the A-linear map $\psi \colon A^{\oplus n} \otimes_A J \to I \otimes_A J$, $e_i \otimes j \mapsto a_i \otimes j$. Then $\varphi \circ \psi \colon A^{\oplus n} \otimes_A J \to A$ is surjective since 1 generates A and $(\varphi \circ \psi)(\sum_{i=1}^n e_i \otimes b_i) = 1$. φ is an isomorphism, hence ψ is surjective. By (i), a surjection $A^{\oplus n} \twoheadrightarrow I$ exists.

Exercise 8.30 (07.1)**.** Let $A \to B$ be a ring map, let M be an A-module, and let N be a B-module.

(i) Show that the map

$$\Phi \colon \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_B(B \otimes_A M, N), \qquad \varphi \mapsto (b \otimes m \mapsto b\varphi(m))$$

is a well-defined isomorphism.

(ii) Show that the map

$$\Phi \colon M \otimes_A N \to (M \otimes_A B) \otimes_B N, \qquad m \otimes n \mapsto (m \otimes 1) \otimes n$$

is a well-defined isomorphism.

(iii) Deduce that

$$S^{-1}M_1 \otimes_A S^{-1}M_2 \cong S^{-1}M_1 \otimes_{S^{-1}A} S^{-1}M_2$$

for two A-modules M_1 and M_2 and a multiplicative subset $S \subseteq A$.

Solution.

(i) Φ is well-defined: Obviously, $B \times M \to N$, $(b, m) \mapsto b\varphi(m)$ is A-bilinear, so by the universal property of tensor products, $\Phi(\varphi)$ is A-linear. Moreover, $\Phi(\varphi)(\lambda b \otimes m) = \lambda b\varphi(m) = \lambda\Phi(\varphi)(b \otimes m)$ for all elementary tensors $b \otimes m \in B \otimes_A M$ and $\lambda \in B$. Thus $\Phi(\varphi)$ is B-linear.

Φ is A-linear: We have

$$\Phi(\lambda\varphi + \psi)(b \otimes m) = b(\lambda\varphi + \psi)(m) = \lambda b\varphi(m) + b\psi(m) = \lambda\Phi(\varphi)(b \otimes m) + \Phi(\psi)(b \otimes m)$$

for all $\lambda \in A$ and $\varphi, \psi \in \mathrm{Hom}_A(M, N)$, where $b \otimes m \in B \otimes_A M$.

Φ is injective: Let $\varphi \in \ker(\Phi)$. Then $b\varphi(m) = 0$ for all $b \in B$ and $m \in M$, and in particular for $b = 1$. Thus $\varphi = 0$.

Φ is surjective: Let $\psi \in \mathrm{Hom}_B(B \otimes_A M, N)$. We define $\varphi\colon M \to N$, $\varphi(m) \coloneqq \psi(1 \otimes m)$, which is A-linear. Then $\Phi(\varphi)(b \otimes m) = b\varphi(m) = b\psi(1 \otimes m) = \psi(b \otimes m)$ for all elementary tensors $b \otimes m \in B \otimes_A M$. Thus $\Phi(\varphi) = \psi$.

(ii) Φ is well-defined: By the properties of tensor products, $M \times N \to (M \otimes_A B) \otimes_B N$, $(m, n) \mapsto (m \otimes 1) \otimes n$ is A-bilinear. Therefore by the universal property of tensor products, Φ is A-linear.

We define the inverse

$$\Psi\colon (M \otimes_A B) \otimes_B N \to M \otimes_A N, \qquad (m \otimes b) \otimes n \mapsto m \otimes bn.$$

Ψ is well-defined: For each $n \in N$, $\Psi_n\colon M \otimes_A B \to M \otimes_A N$ is an A-linear map by the universal property of tensor products since $M \times B \to M \otimes_A N$, $(m, b) \mapsto m \otimes bn$ is A-bilinear. Then $\tilde{\Psi}\colon (M \otimes_A B) \times N \to M \otimes_A N$, $(m \otimes b, n) \mapsto \Psi_n(m \otimes b)$ is A-linear in the first variable by what was said before. $\tilde{\Psi}$ is also A-linear in the second variable since

$$\begin{aligned}\tilde{\Psi}(m \otimes b, \lambda n + n') &= \Psi_{\lambda n + n'}(m \otimes b) = m \otimes b(\lambda n + n') = \lambda(m \otimes bn) + m \otimes bn' \\ &= \lambda\Psi_n(m \otimes b) + \Psi_{n'}(m \otimes b) = \lambda\tilde{\Psi}(m \otimes b, n) + \tilde{\Psi}(m \otimes b, n')\end{aligned}$$

for all $\lambda \in A$, $n, n' \in N$ and $m \otimes b \in M \otimes_A B$. Thus $\tilde{\Psi}$ is A-bilinear and by the universal property of tensor products, Ψ exists and is A-linear.

Now we check that

$$\Psi(\Phi(m \otimes b)) = m \otimes b \qquad \text{and} \qquad \Phi(\Psi((m \otimes b) \otimes n)) = (m \otimes 1) \otimes bn = (m \otimes b) \otimes n,$$

so Φ and Ψ are inverses of each other.

(iii) By (ii) and Corollary 4.55 (iv), we have

$$\begin{aligned}S^{-1}M_1 \otimes_A S^{-1}M_2 &\cong (S^{-1}M_1 \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}M_2 \cong S^{-1}(M_1 \otimes_A A) \otimes_{S^{-1}A} S^{-1}M_2 \\ &\cong S^{-1}M_1 \otimes_{S^{-1}A} S^{-1}M_2.\end{aligned}$$

Exercise 8.31 (07.2)**.** Let A be a ring. We define the **support** of an A-module M as

$$\mathrm{supp}(M) \coloneqq \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_\mathfrak{p} \neq 0\}.$$

(i) Assume that M is finitely generated. Show that $\mathrm{supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M \otimes_A \kappa(\mathfrak{p}) \neq 0\}$.

(ii) Assume that M and N are finitely generated A-modules. Show that $\mathrm{supp}(M \otimes_A N) = \mathrm{supp}(M) \cap \mathrm{supp}(N)$.

Solution.

(i) We have to show that $M_\mathfrak{p} = 0$ if and only if $M \otimes_A \kappa(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$. By Remark 4.38, we can write

$$M \otimes_A \kappa(\mathfrak{p}) = M \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong M \otimes_A A_\mathfrak{p} \otimes_A A/\mathfrak{p} \cong M_\mathfrak{p} \otimes_A A/\mathfrak{p} \cong M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}.$$

If $M_\mathfrak{p} = 0$, then $M \otimes_A \kappa(\mathfrak{p}) = 0$.

Conversely, suppose that $M \otimes_A \kappa(\mathfrak{p}) \cong M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} = 0$. Since $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$ is local, we have $M_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}M_\mathfrak{p} = M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} = 0$. Nakayama's lemma 4.63 implies that $M_\mathfrak{p} = 0$.

(ii) We have to show that $(M \otimes_A N)_\mathfrak{p} = 0$ if and only if $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$. By Corollary 4.55, we have $(M \otimes_A N)_\mathfrak{p} \cong M_\mathfrak{p} \otimes_A N_\mathfrak{p}$. Thus if $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$, then $(M \otimes_A N)_\mathfrak{p} = 0$.

Conversely, suppose that $(M \otimes_A N)_\mathfrak{p} = 0$. By (i) and Exercise 8.30, this is equivalent to

$$0 = M \otimes_A (N \otimes_A \kappa(\mathfrak{p})) \cong (M \otimes_A \kappa(\mathfrak{p})) \otimes_{\kappa(\mathfrak{p})} (N \otimes_A \kappa(\mathfrak{p})).$$

This is a tensor product of $\kappa(\mathfrak{p})$-vector spaces.

We claim the following: Let V and W be k-vector spaces. If $V \otimes_k W = 0$, then $V = 0$ or $W = 0$.

Suppose that $0 \neq v \in V$ and $0 \neq w \in W$ exist. Pick bases $v \in \{v_i \mid i \in I\} \subseteq V$ and $w \in \{w_j \mid j \in J\} \subseteq W$. From linear algebra, we know that $v \otimes w$ is a basis vector of $V \otimes_k W$ (a basis is given by $\{v_i \otimes w_j \mid i \in I, j \in J\}$). In particular, $0 \neq v \otimes w \in V \otimes_k W$. This shows the claim.

It follows that $M \otimes_A \kappa(\mathfrak{p}) = 0$ or $N \otimes_A \kappa(\mathfrak{p}) = 0$, and by (i), $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$.

Exercise 8.32 (07.3)**.** Let A be a ring, let $S \subseteq A$ be a multiplicative subset, and let M and N be A-modules.

(i) Assume that M is a finitely presented A-module. Show that the map

$$S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N), \qquad \frac{\varphi}{s} \mapsto \left(\frac{m}{t} \mapsto \frac{\varphi(m)}{st}\right)$$

is a well-defined isomorphism.

(ii) Construct a counterexample to (i) if M is only assumed to be finitely generated.

The solution uses the following.

Proposition 8.33. *The contravariant* Hom *functor is left-exact: Let*

$$M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

be an exact sequence of A-modules. Then for all A-modules Q, the sequence

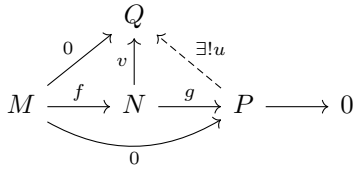
$$0 \longrightarrow \operatorname{Hom}_A(P,Q) \xrightarrow{\operatorname{Hom}(g,Q)} \operatorname{Hom}_A(N,Q) \xrightarrow{\operatorname{Hom}(f,Q)} \operatorname{Hom}_A(M,Q)$$

is exact. Here, $\operatorname{Hom}_A(M,Q)$ is the space of all A-linear maps $M \to Q$, which naturally form an A-module via $(u+v)(x) = u(x) + v(x)$ and $(au)(x) = au(x)$ for all $x \in M$. The map $\operatorname{Hom}(f,Q)\colon \operatorname{Hom}_A(N,Q) \to \operatorname{Hom}_A(M,Q)$ is pre-composition, i. e. $\operatorname{Hom}(f,Q)(u) = u \circ f\colon M \to Q$.

Proof.

- Exactness in $\operatorname{Hom}_A(P,Q)$: Let $u \in \ker(\operatorname{Hom}(g,Q))$, i. e. $u \circ g = 0$. Since g is surjective by exactness in P, we must have $u = 0$. Hence $\operatorname{Hom}(g,Q)$ is injective.
- Exactness in $\operatorname{Hom}_A(N,Q)$: Let $v \in \operatorname{im}(\operatorname{Hom}_A(g,Q))$, i. e. there exists some $u \in \operatorname{Hom}_A(P,Q)$, such that $v = u \circ g$. Then $\operatorname{Hom}(f,Q)(v) = v \circ f = u \circ g \circ f$. By exactness in N, we know $g \circ f = 0$, hence $v \circ f = 0$, meaning $v \in \ker(\operatorname{Hom}(f,Q))$.

  Conversely, let $v \in \ker(\operatorname{Hom}_A(f,Q))$, i. e. $v \circ f = 0$. By exactness in N, we have $g \circ f = 0$. By the universal property of cokernels, there exists a unique A-linear map $u \in \operatorname{Hom}_A(P,Q)$ such that



  commutes. In particular, $v = u \circ g$, thus $v \in \operatorname{im}(\operatorname{Hom}(g,Q))$. □

Solution.

(i) Since M is finitely presented, let $A^{\oplus m} \to A^{\oplus n} \to M \to 0$ be exact for some $m, n \geq 0$. By Proposition 8.33 and exactness of localisations (Proposition 4.51), the sequence

$$0 \longrightarrow S^{-1}\operatorname{Hom}_A(M,N) \longrightarrow S^{-1}\operatorname{Hom}_A(A^{\oplus n},N) \longrightarrow S^{-1}\operatorname{Hom}_A(A^{\oplus m},N)$$

is exact. Similarly,

$$0 \longrightarrow \operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) \longrightarrow \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus n},S^{-1}N) \longrightarrow \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus m},S^{-1}N)$$

is exact. Furthermore, by the universal property of localisations of modules 4.55, the vertical arrows in the following diagram exist:

$$\begin{array}{ccccccc}
0 & \longrightarrow & S^{-1}\operatorname{Hom}_A(M,N) & \longrightarrow & S^{-1}\operatorname{Hom}_A(A^{\oplus n},N) & \longrightarrow & S^{-1}\operatorname{Hom}_A(A^{\oplus m},N) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus n},S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus m},S^{-1}N)
\end{array}$$

(Namely, by functoriality of S^{-1}, every $f \in \operatorname{Hom}_A(M,N)$ induces $S^{-1}f \in \operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$. With the universal map $\operatorname{Hom}_A(M,N) \to S^{-1}\operatorname{Hom}_A(M,N)$, we obtain the vertical arrow.) Each square in the above diagram commutes, for example the left square with $f\colon A^{\oplus n} \to M$:

$$\begin{array}{ccc}
\varphi/s & \longmapsto & \varphi \circ f/s \\
\downarrow & & \downarrow \\
(m/t \mapsto \varphi(m)/(st)) & \longmapsto & (v/t \mapsto (\varphi\circ f)(v)/(st))
\end{array}$$

We check that the two maps

$$S^{-1}\operatorname{Hom}_A(A^{\oplus n},N) \cong \operatorname{Hom}_{S^{-1}A}(S^{-1}A^{\oplus n},S^{-1}N), \quad \frac{\varphi}{s} \mapsto \left(\frac{v}{t} \mapsto \frac{\varphi(v)}{st}\right), \quad \left(v \mapsto \psi\left(\frac{v}{1}\right)\right) \mapsfrom \psi$$

are mutually inverse. A similar statement holds for m instead of n. Extending each row of the big diagram to the right by 0s, there are four vertical isomorphisms. The five lemma 8.35 implies that the dashed vertical arrow is an isomorphism.

(ii) Let $A = k[T, X_1, X_2, \dots]$ and $S = \overline{\{T\}}$. Consider $M = A/(X_1, X_2, \dots)$ and $N = A/(X_iT^i \mid i \geq 1)$.

Let $\varphi \in \operatorname{Hom}_A(M,N)$, and let $\bar{f} := \varphi(\bar{1})$ for some $f \in A$. Then $0 = \varphi(\bar{X}_i) = X_i\varphi(\bar{1}) \in N$ for all $i \geq 1$. It follows that $T^i \mid f$ for all $i \geq 1$. Because the degree of f in T cannot be ∞, we must have $f = 0$, hence $\varphi = 0$. Thus $S^{-1}\operatorname{Hom}_A(M,N) = S^{-1}0 = 0$ is trivial.

On the other hand, $S^{-1}M \cong S^{-1}k[T] \cong k[T,T^{-1}] \cong S^{-1}N$. This means that $\operatorname{Hom}_{S^{-1}A}(S^{-1}M,S^{-1}N)$ contains some non-trivial map. Thus the two Hom-modules cannot be isomorphic.

Alternative: Let $A = k[X_i, T_i \mid i \geq 1]$ and $S = \overline{\{T_1, T_2, \dots\}}$. Consider $M = A/(X_1, X_2, \dots)$ and $N = A/(X_iT_i \mid i \geq 1)$.

Let $\varphi \in \operatorname{Hom}_A(M,N)$, and let $\bar{f} = \varphi(\bar{1})$. Then $0 = \varphi(\bar{X}_i) = X_i\bar{f}$, hence $T_i \mid f$ for all $i \geq 1$. By the same reasoning as above, it follows that $f = 0$ and $\varphi = 0$, thus $\operatorname{Hom}_A(M,N) = 0$.

We claim that $S^{-1}M \cong S^{-1}N \neq 0$. $S^{-1}M \neq 0$ is clear since no element of S annihilates an element of M. Consider $f\colon A \to S^{-1}N$, $1 \mapsto \bar{1}$. Observe that $f(X_i) = \bar{X}_i = \bar{X}_i\bar{T}_i/T_i = 0$, so $(X_1, X_2, \dots) \subseteq \ker(f)$, and by the universal property of quotients, $\bar{f}\colon M \to S^{-1}N$ exists. By the universal property of localisations of modules 4.55, we obtain a map $S^{-1}M \to S^{-1}N$. Similarly, we obtain a map $S^{-1}N \to S^{-1}M$. They are both inverses to each other since they map $\bar{1} \mapsto \bar{1}$.

Exercise 8.34 (07.4)**.** Let A be a principal ideal domain, and let $0 \neq f \in A \setminus A^\times$. Show that the $A[T]$-module $(f,T) \subseteq A[T]$ is not flat.

Solution. Consider the inclusion $(f,T) \hookrightarrow A[T]$ of $A[T]$-modules. We want to show that $(f,T) \otimes_{A[T]} (f,T) \to A[T] \otimes_{A[T]} (f,T)$ is not injective. Observe that $f \otimes T - T \otimes f \mapsto 1 \otimes fT - 1 \otimes fT = 0$. It remains to show that the kernel element is non-zero, so that the kernel of the map in question is not trivial.

Suppose that $f \otimes T - T \otimes f = 0$. We consider the following commutative diagram with, under this assumption, exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[T] & \xrightarrow{\binom{T}{-f}} & A[T]^{\oplus 2} & \xrightarrow{(f\ T)} & (f,T) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \psi} & & \\ & & (f,T) & \xrightarrow{\binom{T}{-f}} & (f,T)^{\oplus 2} & \xrightarrow{\phi} & (f,T) \otimes_{A[T]} (f,T) & & \end{array}$$

Here, $\psi(\binom{a}{b}) = f \otimes a + T \otimes b$ and $\psi(a \otimes b) = ab$. By assumption, $(T, -f) \in \ker(\phi)$, so there exists a preimage $x \in (f,T)$ of $(T,-f)$ by exactness of $(f,T)^{\oplus 2}$. Lifting up to $A[T]$, the only preimage of $(T,-f) \in A[T]^{\oplus 2}$ is $1 \in A[T]$ by injectivity of $\binom{T}{-f}$. Since the left square commutes, the inclusion $(f,T) \hookrightarrow A[T]$ necessarily maps $x \mapsto 1$. But this implies $1 \in (f,T)$, contradicting that (f,T) contains no units.

Exercise 8.35 (**five lemma**, 08.4)**.** Let A be a ring, and let

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array}$$

be a commutative diagram of A-modules with exact rows and isomorphisms α_2 and α_4.

(i) Assume that α_1 is surjective. Show that α_3 is injective.

(ii) Assume that α_5 is injective. Show that α_3 is surjective.

Remark (from me): The first statement only uses that α_2 and α_4 are injective, and the second statement only uses that α_2 and α_4 are surjective.

Solution.

(i) Let $a \in \ker(\alpha_3)$. Since the inner right square commutes and $g_3(\alpha_3(a)) = g_3(0) = 0$, we also have $\alpha_4(f_3(a)) = 0$. α_4 is an isomorphism, so $f_3(a) = 0$, i. e. $a \in \ker(f_3)$. By exactness in M_3, there exists a $b \in M_2$ such that $f_2(b) = a$. Since the inner left square commutes, we must have $g_2(\alpha_2(b)) = \alpha_3(f_2(b)) = \alpha_3(a) = 0$. Thus $\alpha_2(b) \in \ker(g_2)$. By exactness in N_2, there is a $c \in N_1$ such that $g_1(c) = \alpha_2(b)$. By assumption, α_1 is surjective, so there exists some $d \in M_1$ such that $\alpha_1(d) = c$. Since the outer left square commutes, we have $\alpha_2(f_1(d)) = g_1(\alpha_1(d)) = \alpha_2(b)$. But α_2 is an isomorphism, so $f_1(d) = b$, i. e. $b \in \operatorname{im}(f_1)$. By exactness in M_2, we have $b \in \ker(f_1)$, i. e. $f_2(b) = a = 0$. This shows that α_3 is injective.

(ii) Let $a \in N_3$. Since α_4 is an isomorphism, there is some $b \in M_4$ such that $\alpha_4(b) = g_3(a)$. Since the outer right square commutes, we have $g_4(\alpha_4(b)) = \alpha_5(f_4(b))$. By exactness in N_4, we have $g_4(g_3(a)) = 0$ Plugging everything in yields $\alpha_5(f_4(b)) = 0$. By assumption, α_5 is injective, so $f_4(b) = 0$, i. e. $b \in \ker(f_4)$. By exactness in M_4, there exists a $c \in M_3$ such that $f_3(c) = b$. Since the inner right square commutes, we have $g_3(\alpha_3(c)) = \alpha_4(f_3(c)) = \alpha_4(b) = g_3(a)$, i. e. $g_3(a - \alpha_3(c)) = 0$. Thus $a - \alpha_3(c) \in \ker(g_3)$. By exactness in N_3, there is a $d \in N_2$ such that $g_2(d) = a - \alpha_3(c)$. Since α_2 is an isomorphism, there exists some $e \in M_2$ such that $\alpha_2(e) = d$. Since the inner left square commutes, we must have $\alpha_3(f_2(e)) = g_2(\alpha_2(e)) = a - \alpha_3(c)$, i. e. $\alpha_3(f_2(e) + c) = a$. This shows that α_3 is injective.

Exercise 8.36 (09.4)**.** Let A be a ring, and let M be a finitely presented A-module. Let $n \geq 1$, and let $f\colon A^n \to M$ be an A-linear surjection. Show that $K \coloneqq \ker(f)$ is finitely generated.

Hint: Let $0 \to Q \to A^m \to 0$ be a short exact sequence of A-modules with Q finitely generated. Construct a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \longrightarrow & A^m & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}_m} & & \\ 0 & \longrightarrow & K & \longrightarrow & A^n & \xrightarrow{f} & M & \longrightarrow & 0 \end{array}$$

and use the snake lemma 4.83.

Before we solve this, a quick useful statement.

Lemma 8.37. *Let M be an A-module, and let $N \subseteq M$ be a submodule. If M/N and N are finitely generated, then so is M.*

Proof. The proof is similar to Proposition 3.24. Suppose that $M/N = (\bar{x}_1, \dots, \bar{x}_n)$ and that $N = (y_1, \dots, y_m)$. We claim that $M = (x_1, \dots, x_n, y_1, \dots, y_m)$.

Let $z \in M$. Then $\bar{z} = \sum_{i=1}^n a_i \bar{x}_i$ for some $a_i \in A$. Set $z' \coloneqq z - \sum_{i=1}^n a_i x_i$, which is in N since $\bar{z}' = 0$ in M/N. Then $z' = \sum_{j=1}^m b_j y_j$ for some $b_j \in A$, and thus $z = \sum_{i=1}^n a_i x_i + \sum_{j=1}^m b_j y_j$. □

Solution. We carefully construct the diagram from the hint with short exact rows.

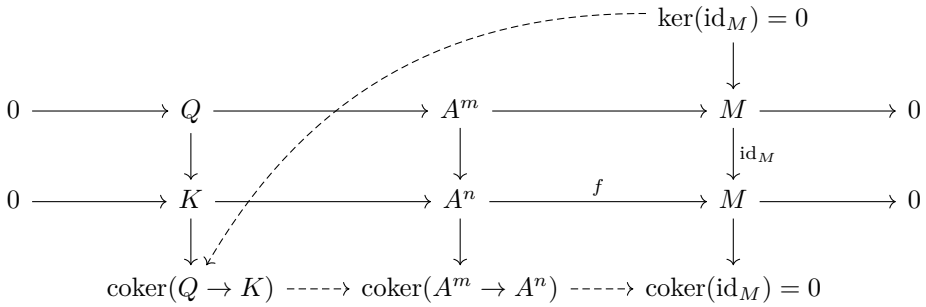
Let $A^k \to A^m \to M \to 0$ be a finite presentation of M. By exactness in A^m, $\ker(A^m \to M)$ is finitely generated. So we can pick any A-module $Q \cong \ker(A^m \to M)$ to obtain the short exact sequence $0 \to Q \to A^m \to M \to 0$. Furthermore, the bottom row $0 \to K \to A^n \to M \to 0$ is also short exact.

We construct the map $A^m \to A^n$. Since A^m is free, the map is well-defined by the images of the basis elements $b \in A^m$. For each image of b under $A^m \to M$, pick any lift to A^n under f (f is surjective). Then $A^m \to A^n$ maps b to this lift. By this construction, the right square commutes.

We construct the map $Q \to K$. As the right square commutes, $A^m \to A^n$ induces a map on kernels: Let $a \in \ker(A^m \to M)$ and let $b \in A^n$ be the image of a. Since the right square commutes and $a \mapsto 0 \mapsto 0$ via M, we must have $a \mapsto b \mapsto 0$ via A^n. Hence $b \in \ker(A^n \to M)$.

So let $a \in Q$, let $b \in A^m$ be the image of a, and let $c \in A^n$ be the image of b. By exactness in A^m, we have $b \in \ker(A^m \to M)$, thus $c \in \ker(A^n \to M)$. By exactness in A^n, we also have $c \in \operatorname{im}(K \to A^n)$. Therefore, $Q \to K$ maps a to the *unique* preimage of c in K ($K \to A^n$ is injective). Note that through this construction, $Q \to K$ is a well-defined A-linear map and the left square commutes.

Now by the snake lemma 4.83, we obtain the following dashed exact sequence:



$\operatorname{coker}(A^m \to A^n)$ is a quotient module of the finitely generated A^m, so it is finitely generated as well. The dashed exact sequence implies that $\operatorname{coker}(Q \to K) \cong \operatorname{coker}(A^m \to A^n)$, hence $\operatorname{coker}(Q \to K)$ is finitely generated. Q is finitely generated, and as the restriction $Q \to \operatorname{im}(Q \to K)$ is surjective, $\operatorname{im}(Q \to K)$ is finitely generated too. By Lemma 8.37, K must be finitely generated.

Exercise 8.38 (10.4)**.** Let A be a local ring, and let M be a finitely presented flat A-module. Show that M is free.

Hint: Let $\mathfrak{m} \subset A$ be the maximal ideal. Use Exercise 8.36 to construct a short exact sequence $0 \to K \to A^n \to M \to 0$ with K finitely generated and $(A/\mathfrak{m})^n \to M/\mathfrak{m}M$ an isomorphism. Now use flatness of M and the snake lemma 4.83 to check that $0 \to K/\mathfrak{m}K \to (A/\mathfrak{m})^n \to M/\mathfrak{m}M \to 0$ is again short exact.

For this exercise, we need a few more versions of Nakayama's lemma Corollary 4.63.

Corollary 8.39 (**Nakayama's lemma**)**.** *Let $(A, \mathfrak{m})$ be a local ring, and let M be a finitely generated A-module.*

(i) *Let $N \subseteq M$ be a submodule. If $M = \mathfrak{m}M + N$, then $M = N$.*

(ii) *Let $\{x_1, \dots, x_n\} \subseteq M$ be a subset such that $\{\bar{x}_1, \dots, \bar{x}_n\}$ is a basis of the $A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$. Then $\{x_1, \dots, x_n\}$ generates M.*

Proof. (From [AtMac, Cor. 2.7, Prop. 2.8].)

(i) Observe that $\mathfrak{m}(M/N) = (\mathfrak{m}M)/N = (\mathfrak{m}M + N)/N = M/N$. Now apply Nakayama's lemma 4.63 on $(M/N)/(\mathfrak{m}(M/N))$ to obtain $M/N = 0$, i. e. $M = N$.

(ii) Let $N := (x_1, \dots, x_n) \subseteq M$. Then the composition $N \to M \to M/\mathfrak{m}M$ is surjective, hence $M = N + \mathfrak{m}M$. By (i), we have $M = N = (x_1, \dots, x_n)$. □

Solution. By Corollary 8.39, we may pick any $A/\mathfrak{m}$-basis of $M/\mathfrak{m}M$ and lift that to a generating set of M. Doing so, we obtain an A-linear surjection $A^{\oplus n} \twoheadrightarrow M$ such that $(A/\mathfrak{m})^{\oplus n} \cong M/\mathfrak{m}M$. By Exercise 8.36, there is a short exact sequence $0 \to K \to A^{\oplus n} \to M \to 0$ with K finitely generated. Tensoring this sequence with $\mathfrak{m}$ yields the exact sequence $\mathfrak{m} \otimes_A K \to \mathfrak{m} \otimes_A A^{\oplus n} \to \mathfrak{m} \otimes_A M \to 0$.

Thus we obtain the following commutative diagram with two exact middle rows:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & \mathfrak{m} \otimes_A K & \longrightarrow & \mathfrak{m} \otimes_A A^{\oplus n} & \longrightarrow & \mathfrak{m} \otimes_A M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & A^{\oplus n} & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K/\mathfrak{m}K & \dashrightarrow & (A/\mathfrak{m})^{\oplus n} & \dashrightarrow & M/\mathfrak{m}M & \dashrightarrow & 0
\end{array}$$

Here, the vertical maps are described by $\mathfrak{m} \otimes_A K \to K$, $m \otimes k \mapsto mk$, and similarly for $A^{\oplus n}$ and M. Hence the image of the vertical maps are precisely $\mathfrak{m}K$, $\mathfrak{m}A^{\oplus n}$ and $\mathfrak{m}M$, resp., thus the cokernels in the dashed row. Furthermore, since M is flat, tensoring $\mathfrak{m} \hookrightarrow A$ with M yields that $\mathfrak{m} \otimes_A M \hookrightarrow M$ is injective, i. e. its kernel is 0. By the snake lemma 4.83, we obtain the short exact sequence

$$0 \to K/\mathfrak{m}K \to A^{\oplus n}/\mathfrak{m}^{\oplus n} \cong (A/\mathfrak{m})^{\oplus n} \to M/\mathfrak{m}M \to 0.$$

This implies $K/\mathfrak{m}K = 0$ since $(A/\mathfrak{m})^{\oplus n} \to M/\mathfrak{m}M$ is an isomorphism. By Nakayama's lemma 4.63, $K = 0$ (notice that K is finitely generated). So the exact sequence becomes $0 \to 0 \to A^{\oplus n} \to M \to 0$, and $M \cong A^{\oplus n}$ is free.

Remark 8.40. Note that in general, $\mathfrak{a} \otimes_A M \cong \mathfrak{a}M$ only for flat A-modules M. Consider for example $A = \mathbb{Z}/4$ and $\mathfrak{a} = M = (2)$. Then $\mathfrak{a}M = (4) = 0$. On the other hand, $\mathfrak{a} \otimes_A M = (2) \otimes_A (2) \neq 0$ since $(2) \times (2) \to \mathbb{Z}/4$, $(2a, 2b) \mapsto 2ab$ is A-bilinear and non-zero, hence $(2) \otimes_A (2) \to \mathbb{Z}/4$ is non-zero.

8.6 Integral Dependence

Exercise 8.41 (08.1)**.** Let A be a ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Show that $A/\mathfrak{a}$ is a finitely presented A-algebra if and only if $\mathfrak{a}$ is a finitely generated ideal.

Solution. If $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = (f_1, \dots, f_m)$ as an A-module, then $A/\mathfrak{a} = A/(f_1, \dots, f_m)$ is finitely presented.

Conversely, assume that $A/\mathfrak{a} \cong A[T_1, \dots, T_n]/(f_1, \dots, f_m)$ is finitely presented. Write $B := A[T_1, \dots, T_n]$. Then we have the following commutative diagram of B-modules with short exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (f_1, \dots, f_m) & \longrightarrow & B & \longrightarrow & B/(f_1, \dots, f_m) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \cong\downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & \mathfrak{a} & \longrightarrow & A & \longrightarrow & A/\mathfrak{a} & \longrightarrow & 0
\end{array}$$

Here, the vertical arrows are given by the evaluation $T_i \mapsto 0$ for all $i = 1, \dots, n$. The terms in the bottom row can be viewed as B-modules via $(\sum_{(i_1,\dots,i_n) \in \mathbb{N}_0^n} a_{(i_1,\dots,i_n)} T_1^{i_1} \cdots T_n^{i_n})x = a_{(0,\dots,0)}x$ for all module elements x. Note that α is well-defined since $\gamma(\bar{f}_i) = 0$, and thus $\alpha(f_i) \in \mathfrak{a}$.

γ is injective and β is surjective, thus $\ker(\gamma) = 0$ and $\operatorname{coker}(\beta) = 0$. By the snake lemma 4.83, we must have $\operatorname{coker}(\alpha) = 0$, i. e. α is surjective. We obtain an B-linear surjection $B^{\oplus m} \twoheadrightarrow (f_1, \dots, f_m) \to \mathfrak{a}$. Tensoring with A yields the B-linear surjection $A^{\oplus m} \cong B^{\oplus m} \otimes_B A \twoheadrightarrow \mathfrak{a} \otimes_B A$, which induces an A-linear surjection $A^{\oplus m} \twoheadrightarrow \mathfrak{a} \otimes_A A \cong \mathfrak{a}$. Thus $\mathfrak{a}$ is a finitely generated A-module or ideal.

Exercise 8.42 (08.2)**.** Let k be a field. Show that the ring extensions $k[X + Y] \to k[X, Y]/(XY)$ and $k[X^2 - 1] \to K[X]$ are integral.

Solution. According to Corollary 5.8, integrality is stable under addition and multiplication, so it suffices to show that the generators are integral.

For the first map, consider $f(T) \coloneqq T^2 - (X+Y)T \in k[X+Y][T]$, which is monic. Then $f(\bar{X}) = \bar{X}^2 - \bar{X}^2 - \bar{X}\bar{Y} = 0 = \cdots = f(\bar{Y})$.

For the second map, consider $f(T) \coloneqq T^2 - 1 - (X^2-1) \in k[X^2-1][T]$, which is monic. Then $f(X) = X^2 - 1 - (X^2-1) = 0$.

Exercise 8.43 (08.3)**.** Let $A \to B$ be a finite ring map, i. e. B is an A-algebra such that it is finite as an A-module. Show that the induced map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ on spectra has finite fibres.

Remark: The ring map $\mathbb{Z} \to \mathbb{Q}$ shows that the converse is not true ($\operatorname{Spec}(\mathbb{Q}) = \{(0)\}$ but $\mathbb{Q} = (\frac{1}{n} \mid n \in \mathbb{Z}_{>0})$ as a $\mathbb{Z}$-module).

Solution. Let $\mathfrak{p} \in \operatorname{Spec}(A)$ be arbitrary. Combine Observation 2.68 and Remark 4.45 to get $\operatorname{Spec}(\phi)^{-1}(\mathfrak{p}) \cong \operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$.

Since B is a finitely generated A-module, we have $A^{\oplus n} \twoheadrightarrow B$ as A-modules for some $n \geq 0$. Since tensoring is right-exact, we obtain $A^{\oplus n} \otimes_A \kappa(\mathfrak{p}) \twoheadrightarrow B \otimes_A \kappa(\mathfrak{p})$. If we consider the tensor products as a scalar extension to the field $\kappa(\mathfrak{p})$, then $B \otimes_A \kappa(\mathfrak{p})$ is a ring as well as a finite-dimensional $\kappa(\mathfrak{p})$-vector space (with dimension at most n). We have seen in the proof of Exercise 8.7 that $B \otimes_A \kappa(\mathfrak{p})$ has at most n different prime ideals. Thus $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ and $\operatorname{Spec}(\phi)^{-1}(\mathfrak{p})$ are finite.

Exercise 8.44 (09.1)**.** Assume that $d \in \mathbb{Z}$ is not a square. Determine all $x, y, z \in \mathbb{Z}$ with $\gcd(x,y,z) = 1$ and $x^2 - dy^2 = z^2$.

Hint: Follow the arguments in sec. 5.4, and consider lines through the point $(-1, 0) \in \mathbb{Q}^2$.

Solution.

(i) Let $X(\mathbb{Q}) \coloneqq \{(a,b) \in \mathbb{Q}^2 \mid a^2 - db^2 = 1\}$ be the unit conic section parametrised by d, and let $P \coloneqq (-1,0) \in X(\mathbb{Q})$. We call a solution $(x,y,z) \in \mathbb{Z}^3$ with $\gcd(x,y,z) = 1$ *and* $z > 0$ of $x^2 - dy^2 = z^2$ *primitive*.

Each primitive solution (x,y,z) gives exactly two solutions, namely (x,y,z) and $(-x,-y,-z)$ (note that $z \neq 0$ always holds, as otherwise either $y = 1$ and d would be a square, or $x = y = 0$ and $\gcd(x,y,z) = \gcd(0,0,0)$ is not defined).

(ii) Then we have a bijection between primitive solutions and $X(\mathbb{Q})$.

We will construct mutually inverse maps: The first map is $(x,y,z) \mapsto (\frac{x}{z}, \frac{y}{z}) \in X(\mathbb{Q})$, simply by dividing the defining relation $x^2 - dy^2 = z^2$ through z^2.

The inverse is constructed as follows: Let $(a,b) \in X(\mathbb{Q})$. Then we can write $a = \frac{x}{z}$ and $b = \frac{y}{z}$ with $\gcd(x,y,z) = 1$ and $z > 0$, Now map $(a,b) \mapsto (x,y,z)$, where (x,y,z) is indeed a primitive solution.

(iii) Next we have a bijection $\mathbb{Q} \to X(\mathbb{Q}) \setminus \{P\}$.

For each $q \in \mathbb{Q}$, we construct a line L_q through P with slope q, i. e. the solutions of $qa + q = b$. We claim that L_q intersects $X(\mathbb{Q})$ in another point except P. To show this, we solve the system of equations $a^2 - db^2 = 1$ and $qa + q = b$. Substituting b into the first equation yields

$$0 = a^2 - d(qa+q)^2 - 1 = (1 - dq^2)a^2 - 2dq^2 a - (1 + dq^2).$$

Note that $d \in \mathbb{Z}$ is not a square, so $dq^2 \notin \mathbb{Z}_{>0}$ and, in particular, $dq^2 \neq 1$, i. e. we may safely divide by $1 - dq^2$. Since $P \in L_q \cap X(\mathbb{Q})$, we know that one solution of this equation is $a = -1$. Vieta's formulas give the *unique* other solution

$$a = \frac{1+dq^2}{1-dq^2} \implies b = q\frac{1+dq^2}{1-dq^2} + q = \frac{q + dq^3 + q - dq^3}{1-dq^2} = \frac{2q}{1-dq^2}.$$

This point (a,b) is indeed rational, and hence $(a,b) \in X(\mathbb{Q}) \setminus \{P\}$.

Conversely, every point $(a,b) \in X(\mathbb{Q}) \setminus \{P\}$ defines a line through P and (a,b). This line has slope

$$q = \frac{b}{1+a},$$

which is indeed rational. Note that $a \neq -1$ since $(a,b) \neq P$, and $P \in X(\mathbb{Q})$ is the only point with a-coordinate -1 (if $(-1)^2 - db^2 = 1$, then $b = 0$ since $d \neq 0$). One can easily verify that the maps

$$q \mapsto \left(\frac{1+dq^2}{1-dq^2}, \frac{2q}{1-dq^2}\right), \qquad \frac{b}{1+a} \mapsfrom (a,b)$$

are mutual inverses.

(iv) Now we combine everything. Observe that $P \in X(\mathbb{Q})$ corresponds to the primitive solution $(-1,0,1)$. Writing $q = \frac{u}{v} \in \mathbb{Q}$ with $u, v \in \mathbb{Z}$, $\gcd(u,v) = 1$ and $v > 0$, we have the following bijection between $\mathbb{Q}$ and primitive solutions except $(-1,0,1)$:

$$q \mapsto \left(\frac{1+dq^2}{1-dq^2}, \frac{2q}{1-dq^2}\right) = \left(\frac{v^2+du^2}{v^2-du^2}, \frac{2uv}{v^2-du^2}\right) \mapsto \left(\frac{v^2+du^2}{g}, \frac{2uv}{g}, \frac{v^2-du^2}{g}\right),$$

where $g \coloneqq \pm\gcd(v^2+du^2, 2uv, v^2-du^2)$. The sign of g is chosen in such a way that $(v^2-du^2)/g > 0$. In fact, $(-1,0,1)$ is also of this form with $u = 1$ and $v = 0$.

Let us inspect g a bit further. Let $p \in \mathbb{Z}$ be a prime factor of g, i. e. $p \mid 2uv, v^2 \pm du^2$. We exhaust the fact that $p \mid 2uv$.

- We have $p = 2$ if and only if $v^2 \equiv du^2 \mod 2$. As $\gcd(u,v) = 1$, this is equivalent to $v^2 \equiv d \mod 2$, i. e. v and d are both even/odd.
- Suppose that $p \mid u$. Then $p \mid v^2$, which is impossible since $\gcd(u,v) = 1$.
- We have $p \mid v$ if and only if $p \mid du^2$. As $\gcd(u,v) = 1$, this is equivalent to $p \mid d$.

To summarise, the (not necessarily primitive) solutions are

$$\begin{cases} \left(\frac{v^2+du^2}{\pm 2g}, \frac{uv}{\pm g}, \frac{v^2-du^2}{\pm 2g}\right), & \text{if } v \text{ and } d \text{ are odd,} \\ \left(\frac{v^2+du^2}{\pm g}, \frac{2uv}{\pm g}, \frac{v^2-du^2}{\pm g}\right), & \text{otherwise,} \end{cases}$$

with $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{\geq 0}$, $\gcd(u,v) = 1$ and $g \coloneqq \gcd(v,d)$.

Exercise 8.45 (09.2)**.** Let k be an algebraically closed field, and let $f(X) \in k[X]$ be a polynomial. Determine the set $\operatorname{Spec}(k[X,Y]/(Y^2 - f(X)))$ and the cardinality of all fibres of the map

$$\operatorname{Spec}(\phi)\colon \operatorname{Spec}(k[X,Y]/(Y^2 - f(X))) \to \operatorname{Spec}(k[X])$$

that is induced by the k-algebra homomorphism $\phi\colon k[X] \to k[X,Y]/(Y^2 - f(X))$, $X \mapsto X$.

Solution. We first examine when $Y^2 - f$ factors. Suppose that $Y^2 - f(X) = pq$ with $0 \neq p, q \in k[X,Y]$ Considering the degree in terms of Y, we have $2 = \deg_Y(Y^2 - f) = \deg_Y(p) + \deg_Y(q)$. Thus we distinguish two cases:

(i) Assume that w. l. o. g. $p = g(X)$ and $q = Y^2 h_2(X) + Y h_1(X) + h_0(X)$ with $g, h_1, h_2, h_3 \in k[X]$. Comparing the coefficient of Y^2, we obtain $gh_2 = 1$, so $g \in k[X]^\times = k^\times$. This shows that $Y^2 - f$ is irreducible and thus a prime element in $k[X,Y]$ (recall that due to Gauss's lemma, $k[X,Y]$ is a unique factorisation domain).

(ii) Assume that $p = g_1(X)Y + g_0(X)$ and $q = h_1(X)Y + h_0(X)$ with $g_1, g_2, h_1, h_2 \in k[X]$. Comparing the coefficient of Y^2 again, we obtain $g_1 h_1 = 1$, so $g_1, h_1 \in k^\times$, and we may assume w. l. o. g. that $g_1 = h_1 = 1$. Furthermore, comparing the coefficient of Y, we must have $g_0 h_1 + g_1 h_0 = g_0 + h_0 = 0$. Hence $p = Y + g_0(X)$ and $q = Y - g_0(X)$, i. e. f is a square in $k[X]$.

Back to our main problem. Recall that since k is algebraically closed

$$\operatorname{Spec}(k[X,Y]) = \{(0)\} \sqcup \{(h) \mid h \in k[X,Y] \text{ irreducible}\} \sqcup \{(X-x, Y-y) \mid x, y \in k\}$$
$$\operatorname{Spec}(k[X]) = \{(0)\} \sqcup \{(X-x) \mid x \in k\}$$

(cf. Example 2.59), and that $\operatorname{Spec}(k[X,Y]/(Y^2 - f(X)))$ consist of all prime ideals of $k[X,Y]$ containing $Y^2 - f(X)$ (Example 2.14). The ideal (0) is obviously out of question.

(i) Assume that $Y^2 - f(X)$ is prime. Thus the only prime ideal in $k[X,Y]$ of the form (h) that contains $Y^2 - f(X)$ is $(Y^2 - f(X))$.

For prime ideals of the form $(X-x, Y-y)$, suppose that $Y^2 - f(X) \in (X-x, Y-y)$. Then (x,y) must be a solution of $Y^2 - f(X)$, i. e. $y = \pm\sqrt{f(x)}$ (the square root exists since k is algebraically closed). This condition is sufficient because $Y^2 - f(X) = (Y + \sqrt{f(x)})(Y - \sqrt{f(x)}) + (f(x) - f(X))$ and $X - x \mid f(x) - f(X)$. Therefore we obtain

$$\operatorname{Spec}(k[X,Y]/(Y^2 - f(X))) = \{(Y^2 - f(X))\} \sqcup \{(X-x, Y \pm \sqrt{f(x)}) \mid x \in k\}.$$

(ii) Assume that $Y^2 - f(X) = (Y + g(X))(Y - g(X))$ for some $g \in k[X]$. Note that $Y \pm g(X)$ are irreducible in $k[X,Y]$, so the only prime ideals of the form (h) that contain $Y^2 - f(X)$ are $(Y \pm g(X))$. For prime ideals of the form $(X-x, Y-y)$, we have the same argument as before. Thus

$$\operatorname{Spec}(k[X,Y]/(Y^2 - f(X))) = \{(Y \pm g(X))\} \sqcup \{(X-x, Y \pm \sqrt{f(x)}) \mid x \in k\}.$$

For the fibres, observe that ϕ is injective, so we may interpret ϕ as $k[X] \subseteq k[X,Y]/(Y^2 - f(X))$. We use Observation 2.68.

(i) For $(0) \in \operatorname{Spec}(k[X])$, we have

$$\phi(k[X] \setminus (0)) \cap (Y^2 - f(X)) = \varnothing, \qquad \phi(k[X] \setminus (0)) \cap (X-x, Y \pm \sqrt{f(x)}) = (X-x) \cdot k[X] \neq \varnothing.$$

For $(X-x) \in \operatorname{Spec}(k[X])$, we have

$$\phi((X-x)) \nsubseteq (Y^2 - f(X)), \qquad \phi((X-x)) \subseteq (X-x, Y \pm \sqrt{f(x)}),$$
$$\phi(k[X] \setminus (X-x)) \cap (X-x, Y \pm \sqrt{f(x)}) = \varnothing$$

Therefore

$$\operatorname{Spec}(\phi)^{-1}((0)) = \{(Y^2 - f(X))\}, \qquad \operatorname{Spec}(\phi)^{-1}((X-x)) = \{(X-x, Y \pm \sqrt{f(x)})\}$$

with cardinalities 1 and 2, resp.

(ii) This case is similar to the above. What changes is that

$$\phi(k[X] \setminus (0)) \cap (Y \pm g(X)) = \varnothing, \qquad \phi((X-x)) \nsubseteq (Y \pm g(X)).$$

Therefore

$$\operatorname{Spec}(\phi)^{-1}((0)) = \{(Y \pm g(X))\}, \qquad \operatorname{Spec}(\phi)^{-1}((X-x)) = \{(X-x, Y \pm \sqrt{f(x)})\}$$

with cardinalities 2 and 2, resp.

Exercise 8.46 (09.3)**.** Let $m, n \geq 1$, and let $\zeta_m = \mathrm{e}^{2\pi\mathrm{i}/m} \in \mathbb{C}$ be a primitive mth root of unity. Set $G \coloneqq \langle \zeta_m \rangle \subseteq \mathbb{C}^\times$. We let G act on $A \coloneqq \mathbb{C}[T_1, \ldots, T_n]$ via $(g, f(T_1, \ldots, T_n)) \mapsto g \cdot f \coloneqq f(gT_1, \ldots, gT_n)$.

(i) Determine the ring of invariants $A^G \coloneqq \{f \in A \mid g \cdot f = f \text{ for all } g \in G\}$.

(ii) Set $m = n = 2$. Find a presentation $A^G \cong \mathbb{C}[X_1, \ldots, X_k]/(h_1, \ldots, h_l)$.

Solution.

(i) Observe that this group action is $\mathbb{C}$-linear, i. e. $g(f+h) = gf + gh$ and $g(af) = cg(f)$ for all $f, h \in A$ and $c \in \mathbb{C}$. So it suffices to consider monic monomials $T_1^{e_1} \cdots T_n^{e_n}$ for $e_i \in \mathbb{Z}_{\geq 0}$.

Let $T_1^{e_1} \cdots T_n^{e_n} \in A^G$. Then for all $g = \zeta_m^k \in A^G$ with $0 \leq k < m$, we have $g \cdot (T_1^{e_1} \cdots T_n^{e_n}) = g^{e_1 + \cdots + e_n} T_1^{e_1} \cdots T_n^{e_n} = T_1^{e_1} \cdots T_n^{e_n}$ if and only if $g^{e_1 + \cdots + e_n} = \zeta_m^{k(e_1 + \cdots + e_n)} = 1$, that is $m \mid k(e_1 + \cdots + e_n)$. A sufficient and necessary condition is $m \mid (e_1 + \cdots + e_n)$. Hence $A^G = \mathbb{C}[T_1^{e_1} \cdots T_n^{e_n} \mid e_1 + \cdots + e_n = m]$.

(ii) In this case, $A^G = \mathbb{C}[T_1^2, T_1T_2, T_2^2]$. Define the $\mathbb{C}$-algebra map

$$\phi\colon \mathbb{C}[X_1, X_2, X_3] \twoheadrightarrow A^G, \qquad X_1 \mapsto T_1^2, \quad X_2 \mapsto T_1T_2, \quad X_3 \mapsto T_2^2.$$

We claim that $\ker(\phi) = (X_1X_3 - X_2^2)$. On the one hand, $\phi(X_1X_3 - X_2^2) = T_1^2T_2^2 - (T_1T_2)^2 = 0$. On the other hand, let $f \in \ker(\phi)$. Consider $\bar{f} \in \ker(\bar{\phi}) \subseteq A/(X_1X_3 - X_2^2)$, where $\bar{\phi}$ is the induced map by the universal property of quotients. We can write $\bar{f} = h_1X_2 + h_2$ for $h_1, h_2 \in \mathbb{C}[X_1, X_3]$, which yields $\bar{\phi}(\bar{f}) = \bar{\phi}(h_1)T_1T_2 + \bar{\phi}(h_2) = 0$. Observe that each monomial in $\bar{\phi}(h_1), \bar{\phi}(h_2) \in \mathbb{C}[T_1^2, T_2^2]$ has even total degree, so the monomials in $\bar{\phi}(h_1)T_1T_2$ and $\bar{\phi}(h_2)$ do not kill each other. Hence $\bar{\phi}(h_1) = \bar{\phi}(h_2) = 0$, thus $h_1 = h_2 = 0$ and $\bar{f} = 0$. Finally, $\ker(\bar{\phi}) = \ker(\phi)/(X_1X_3 - X_2^2) = 0$ shows the claim.

In conclusion, we have $A^G \cong \mathbb{C}[X_1, X_2, X_3]/(X_1X_3 - X_2^2)$ by the homomorphism theorem.

Alternative: Another way to see that $\ker(\phi) \subseteq (X_1X_3 - X_2^2)$. We have a chain of prime ideals $(0) \subset (T_1^2, T_1T_2) \subset (T_1^2, T_1T_2, T_2^2)$ (notice that the quotients by these ideals are the integral domains A^G, $\mathbb{C}[T_2^2]$ and $\mathbb{C}$, resp.). Thus $\dim(\mathbb{C}[X_1, X_2, X_3]/\ker(\phi)) = \dim(A^G) \geq 2$. By Theorem 6.33, we know that $\dim(\mathbb{C}[X_1, X_2, X_3]) = 3$, and Krull's principal ideal theorem 6.57 implies that $\dim(\mathbb{C}[X_1, X_2, X_3]/(X_1X_3 - X_2^2)) = 2$ already. Would the kernel be bigger than $(X_1X_3 - X_2^2)$, then the Krull dimension of the quotient ring would decrease. Hence $\ker(\phi) = (X_1X_3 - X_2^2)$.

8.7 Basics in Algebraic Geometry

Exercise 8.47 (10.1)**.** Let k be a field, and let $f\colon A \to B$ be a k-algebra map with B finitely generated. Let $\mathfrak{m} \subset B$ be a maximal ideal. Show that $f^{-1}(\mathfrak{m}) \subset A$ is a maximal ideal.

Solution. Write $\mathfrak{p} \coloneqq f^{-1}(\mathfrak{m}) \subset A$, which is prime. By Hilbert's Nullstellensatz 6.8, $B/\mathfrak{m}$ is a finite field extension over k. f induces a ring map $A/\mathfrak{p} \to B/\mathfrak{m}$. As $B/\mathfrak{m}$ is a field, this map must be injective, hence $A/\mathfrak{p}$ is finite over k as well (think of $B/\mathfrak{m}$ as a finite-dimensional k-vector space). Since $A/\mathfrak{p}$ is an integral domain, by Exercise 8.7, $A/\mathfrak{p}$ is a field. Therefore $\mathfrak{p}$ is maximal.

Exercise 8.48 (10.2)**.** Let $Z \subseteq k^n$ be an algebraic subset with $n \geq 0$. Show that $I(Z)$ is a prime ideal if and only if Z is irreducible.

Solution. Suppose that Z is irreducible. Let $fg \in I(Z)$. By Remark 6.21, we obtain $Z \subseteq Z(I(Z)) \subseteq Z(fg)$. From Observation 6.15 we know that $Z(fg) = Z(f) \cup Z(g)$, implying $Z = (Z(f) \cap Z) \cup (Z(g) \cap Z)$. By irreducibility, $Z \subseteq Z(f)$ or $Z \subseteq Z(g)$. Again by Remark 6.21, $f \in I(Z(f)) \subseteq I(Z)$ or $g \in I(Z(g)) \subseteq I(Z)$, so $I(Z)$ is prime.

Conversely, suppose that Z is not irreducible, say $Z = Z(\mathfrak{a}_1) \cup Z(\mathfrak{a}_2) = Z(\mathfrak{a}_1\mathfrak{a}_2)$ with $Z(\mathfrak{a}_1), Z(\mathfrak{a}_2) \neq Z$ and ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ (we used Observation 6.15 here). Note that $\mathfrak{a}_1, \mathfrak{a}_2 \neq I(Z)$, as otherwise $Z(\mathfrak{a}_i) = Z(I(Z)) = Z$ for some $i \in \{1, 2\}$ by Hilbert's Nullstellensatz 6.23. Therefore we can pick $f_i \in \mathfrak{a}_i \setminus I(Z)$ for $i = 1, 2$, which implies $f_1f_2 \in \mathfrak{a}_1\mathfrak{a}_2 \subseteq \sqrt{\mathfrak{a}_1\mathfrak{a}_2} = I(Z)$ by Hilbert's Nullstellensatz 6.23.

Exercise 8.49 (10.3)**.** By Remark 6.27, a ring is Jacobson if each prime ideal is the intersection of all maximal ideals containing it.

(i) Show that a ring A is Jacobson if and only if for all prime ideals $\mathfrak{p} \subset A$ and for all $a \notin \mathfrak{p}$, there exists a maximal ideal $\mathfrak{m} \subset A$ such that $a \notin \mathfrak{m}$ and $\mathfrak{p} \subseteq \mathfrak{m}$.

(ii) Let $f\colon A \to B$ be an injective integral ring map, and assume that B is Jacobson. Show that A is Jacobson. Deduce from the given proof for Theorem 6.25 that for each field k and $n \geq 0$, the ring $k[X_1, \ldots, X_n]$ is Jacobson.

Solution.

(i) By Remark 6.27, A is Jacobson if and only if $\mathfrak{p} = \bigcap_{\mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m}$ for all prime ideals $\mathfrak{p}$. This is set-theoretically equivalent to the following condition: If $a \notin \mathfrak{p}$, then there must be one $\mathfrak{m}$ among the maximal ideals in the intersection such that $a \notin \mathfrak{m}$.

(ii) f induces a surjection $\operatorname{Spec}(f)\colon \operatorname{Spec}(B) \twoheadrightarrow \operatorname{Spec}(A)$ by Corollary 5.15. Let $\mathfrak{p} \in \operatorname{Spec}(A)$ be arbitrary. Then there exists some $\mathfrak{q} \in \operatorname{Spec}(B)$ with $f^{-1}(\mathfrak{q}) = \mathfrak{p}$. By the definition of Jacobson rings, $\mathfrak{q} = \bigcap_{\mathfrak{q} \subseteq \mathfrak{m}} \mathfrak{m}$, so $\mathfrak{p} = \bigcap_{\mathfrak{q} \subseteq \mathfrak{m}} f^{-1}(\mathfrak{m})$. By Corollary 5.13, each $f^{-1}(\mathfrak{m})$ must be maximal as well. Since $\operatorname{Spec}(f)$ is

surjective, each maximal ideal in A containing $\mathfrak{p}$ appears in the intersection $\mathfrak{p} = \bigcap_{\mathfrak{q}\subseteq\mathfrak{m}} f^{-1}(\mathfrak{m})$. Therefore $\mathfrak{p} = \bigcap_{\mathfrak{q}\subseteq\mathfrak{m}} f^{-1}(\mathfrak{m}) = \bigcap_{\mathfrak{p}\subseteq\mathfrak{n}\in\operatorname{MaxSpec}(A)} \mathfrak{n}$, and we are done.

By definition, $\overline{k}/k$ is an algebraic field extension, so $k \hookrightarrow \overline{k}$ is integral. Hence $k[X_1,\dots,X_n] \hookrightarrow \overline{k}[X_1,\dots,X_n]$ is integral as well: From Corollary 5.8, we know that integrality is closed under addition and multiplication. $\overline{k}$ is integral over $k \subseteq k[X_1,\dots,X_n]$, and each X_i is obviously integral over $k[X_1,\dots,X_n]$. Now we know from Theorem 6.25 that $\overline{k}[X_1,\dots,X_n]$ is Jacobson. Apply the above result, and we win.

Exercise 8.50 (11.1)**.** Let k be a field, and let A and B be two finitely generated k-algebras. Show that $\dim(A \otimes_k B) = \dim(A) + \dim(B)$.

Solution. Noether normalisation 6.5 and Corollary 6.34 give finite injective ring maps $k[X_1,\dots,X_{\dim(A)}] \hookrightarrow A$ and $k[Y_1,\dots,Y_{\dim(B)}] \hookrightarrow B$, which are also k-linear. We want to show that $k[X_i,Y_j] \hookrightarrow A \otimes_k B$ is again a finite injective ring map. Then $\dim(A)+\dim(B) = \dim(k[X_i,Y_j]) = \dim(A\otimes_k B)$ by Corollary 6.34, as desired.

$k[X_i]$ and B are k-vector spaces, so they are free and hence flat. This gives the injections $k[X_i,Y_j] \cong k[X_i]\otimes_k k[Y_j] \hookrightarrow k[X_i]\otimes_k B$ (we used Remark 4.38 here) and $k[X_i]\otimes_k B \hookrightarrow A\otimes_k B$. So their composition is again an injection.

For finiteness, we are given k-linear surjections $k[X_i]^{\oplus s} \twoheadrightarrow A$ and $k[Y_j]^{\oplus t} \twoheadrightarrow B$. Since tensoring is right-exact, we obtain the surjections $k[X_i,Y_j]^{\oplus st} \cong k[X_i]^{\oplus s}\otimes_k k[Y_j]^{\oplus t} \twoheadrightarrow k[X_i]^{\oplus s}\otimes_k B$ (we used Proposition 4.25 here) and $k[X_i]^{\oplus s}\otimes_k B \twoheadrightarrow A\otimes_k B$. Their composition is again a surjection, so $A\otimes_k B$ is a finite $k[X_i,Y_j]$-module.

Alternative: Actually for Corollary 6.34, integrality of $k[X_i,Y_j] \hookrightarrow A\otimes_k B$ suffices.

We generalise Proposition 5.10: Let $A \to B$ be an integral map of R-algebras, and let C be R-algebra. Then $C\otimes_R A \to C\otimes_k B$ is again integral. The proof is identical to the one given in Proposition 5.10, but we spare the step '$C\otimes_A A \cong C$'.

This shows that $k[X_i,Y_j] \hookrightarrow k[X_i]\otimes_k B$ and $k[X_i]\otimes_k B \hookrightarrow A\otimes_k B$ are integral. By Corollary 5.9, their composition is also integral.

Exercise 8.51 (11.2)**.** Let k be a field, and consider the k-algebra map

$$\varphi\colon k[x,y]/(y^2-x^3) \to k[t], \qquad x\mapsto t^2, \quad y\mapsto t^3.$$

Show that φ is finite, induces a bijection on spectra and is not an isomorphism.

Solution. Henceforth $A := k[x,y]/(y^2-x^3)$.

φ is finite: Observe that $t^2, t^3, \dots \in \operatorname{im}(\varphi)$. Hence $k[t] = \operatorname{im}(\varphi)[t]$, and according to Proposition 5.7, it suffices to show that t is integral over A. This is indeed the case, e. g. via $T^2 - x \in A[T]$.

φ is not an isomorphism: We show that φ fails to be surjective, namely, φ does not target t. Suppose that there exists some $f\in A$ such that $\varphi(f) = t$. Since we can write $f = g(x) + yh(x)$ for suitable $g(x),h(x)\in k[x]$, we obtain $\varphi(f) = \varphi(g) + t^3\varphi(h)$. Observe that all terms of $\varphi(g)$ and $\varphi(h)$ have even degree, so the terms of $\varphi(g)$ and of $t^3\varphi(h)$ do not cancel each other. In order for $\varphi(f) = t$ to hold, we must have $\varphi(g) = 0$ and $t^3\varphi(h) = t$, which is impossible.

φ induces a bijection on spectra: We show that φ is injective. Suppose that $\bar{f} = g(x) + yh(x) \in \ker(\varphi)$ as above. With the same arguments, we conclude that $\varphi(g) = 0 = \varphi(h)$, hence $g = 0 = h$, hence $\bar{f} = 0$.

The above should give a hint that t is the sole obstacle to make φ into an isomorphism. Observe that if we could invert x, then $y/x \mapsto t^3/t^2 = t$. So let us do exactly that. Localising the injection $A \hookrightarrow k[t]$ of A-modules at $x\in A$, we obtain the injection $\tilde{\varphi}\colon k[x,x^{-1},y]/(y^2-x^3) = A[x^{-1}] \hookrightarrow k[t,t^{-2}]$ of $A[x^{-1}]$-modules. Now, $\tilde{\varphi}$ is surjective since $\tilde{\varphi}(y/x) = t$ and $\tilde{\varphi}(x^{-1}) = t^{-2}$, which are the k-algebra generators of the codomain of $\tilde{\varphi}$.

$\tilde{\varphi}$ is thus an isomorphism and induces a bijection $\operatorname{Spec}(\tilde{\varphi})\colon \operatorname{Spec}(k[t,t^{-2}]) \to \operatorname{Spec}(A[x^{-1}])$. Reconstructing $\operatorname{Spec}(\varphi)$, we know that

$$\operatorname{Spec}(k[t]) = \operatorname{Spec}(k[t,t^{-2}]) \sqcup \operatorname{Spec}(k[t]/(t^2)), \qquad \operatorname{Spec}(A) = \operatorname{Spec}(A[x^{-1}]) \sqcup \operatorname{Spec}(A/(x)).$$

Since $k[t]$ is a unique factorisation domain, we have $\operatorname{Spec}(k[t]/(t^2)) = \{(t)\}$. Furthermore,

$$\operatorname{Spec}(A/(x)) = \{\mathfrak{p}\in\operatorname{Spec}(k[x,y]) \mid (x)+(y^2-x^3) = (x,y^2)\subseteq\mathfrak{p}\} = \{(x,y)\}.$$

Indeed, $(x,y)\subset A$ is prime since $A/(x,y)\cong k$, but $(x,y^2)\subset A$ is not since $A/(x,y^2)\cong k[y]/(y^2)$ is not an integral domain. Finally, we just have to check that $\operatorname{Spec}(\varphi)((t)) = \varphi^{-1}((t)) = (x,y)$. But this is true since $\varphi(x) = t^2$, $\varphi(y) = t^3$ and $\varphi(1) = 1$. Hence $\bar{\varphi}\colon A/(x) \to k[t]/(t^2)$ induces a bijection $\operatorname{Spec}(\bar{\varphi})$, so $\operatorname{Spec}(\varphi)$ is in total bijective.

Exercise 8.52 (11.3)**.** In this exercise, we denote by $\mathrm{MinSpec}(A)$ the set of minimal prime ideals of a ring A.

(i) Let $A_1, \dots, A_n$ be rings, and let B be their product. Show that

$$\mathrm{MinSpec}(B) \cong \coprod_{i=1}^{n} \mathrm{MinSpec}(A_i).$$

(ii) Let $f\colon A \to B$ be an injective integral ring map. Show the inclusion

$$\mathrm{MinSpec}(A) \subseteq \mathrm{Spec}(f)(\mathrm{MinSpec}(B)),$$

and give an example where the inclusion is strict.

Solution.

(i) We first determine $\mathrm{Spec}(B)$. Let $\mathfrak{q} \in \mathrm{Spec}(B)$, and denote by $e_i := (0, \dots, 0, 1, 0, \dots, 0) \in B$ the ith unit vector. Since $B = (e_1, \dots, e_n)$ and $\mathfrak{q} \neq B$, there must be some $1 \leq i \leq n$ such that $e_i \notin \mathfrak{q}$. Then $e_i e_j = 0 \in \mathfrak{q}$ for all $j \neq i$, so $e_j \in \mathfrak{q}$ for all $j \neq i$, hence $(e_j \mid j \neq i) \subseteq B$. Now consider $a, b \in A_i$, and let $\pi_i\colon B \twoheadrightarrow A_i$ be the canonical projection. Then $abe_i \in \mathfrak{q}$ (this is abuse of notation; what we mean is $(0, \dots, ab, \dots, 0)$) if and only if $ae_i \in \mathfrak{q}$ or $be_i \in \mathfrak{q}$ if and only if $a \in \pi(\mathfrak{q})$ or $b \in \pi(\mathfrak{q})$ if and only if $ab \in \pi(\mathfrak{q})$. This shows that $\pi(\mathfrak{q}) =: \mathfrak{p}_i$ is a prime ideal in A_i. We obtain $\mathfrak{q} = A_1 \times \cdots \times \mathfrak{p}_i \times \cdots \times A_n$, which is indeed a prime ideal.

This readily implies that $\mathfrak{q} \in \mathrm{MinSpec}(B)$ with $\pi_i(\mathfrak{q}) \neq A_i$ if and only if $\pi_i(\mathfrak{q}) \in \mathrm{MinSpec}(A_i)$. Thus the to be proven statement follows.

(ii) We know from Corollary 5.15 that $\mathrm{Spec}(f)$ is surjective. Hence for each $\mathfrak{p} \in \mathrm{MinSpec}(A)$, there is some $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathrm{Spec}(f)(\mathfrak{q}) = \mathfrak{p}$. Moreover, there exists some $\mathfrak{q}' \in \mathrm{MinSpec}(B)$ such that $\mathfrak{q}' \subseteq \mathfrak{q}$ (this follows from applying the proof of Exercise 8.12 to the set of all prime ideals below $\mathfrak{q}$). Then $\mathrm{Spec}(f)(\mathfrak{q}') \subseteq \mathfrak{p}$, but by minimality of $\mathfrak{p}$, we have equality.

Remark: In fact, we have $\mathfrak{q}' = \mathfrak{q}$ by Corollary 5.14.

For the example, consider $A = \mathbb{Z}$ and $B = \mathbb{Z} \times \mathbb{Z}/2$. The canonical map $f\colon A \to B$, $1 \mapsto (1, 1)$ is injective since $\pi_1 \circ f = \mathrm{id}_{\mathbb{Z}}$, where $\pi_1\colon B \to \mathbb{Z}$ is the canonical projection in the first component. Moreover, the generators $(1, 0)$ and $(0, 1)$ of B are integral over $f(A)[T]$ via the monic polynomial $T^2 - T \in f(A)[T]$. Thus by Corollary 5.8, f itself is integral.

We have $\mathrm{MinSpec}(A) = \{(0)\}$, but $\mathbb{Z} \times (0) \in \mathrm{MinSpec}(B)$ and $f^{-1}(\mathbb{Z} \times (0)) = (2)$.

Exercise 8.53 (11.4)**.** Let k be an algebraically closed field, and let $Z = Z(xz, yz, xw, yw) \subseteq k^4$ be the vanishing set of $(xz, yz, xw, yw) \subseteq k[x, y, z, w]$. Determine the irreducible components of Z and their intersections.

Hint: Construct an injective ring map $k[x, y, z, w]/(xz, yz, xw, yw) \hookrightarrow k[r, s] \times k[u, v]$ and use Exercise 8.52 to determine the irreducible components.

Solution. Let f be the map in the hint, and let $A := k[x, y, z, w]/(xz, yz, xw, yw)$ and $B := k[r, s] \times k[u, v]$. We define $f\colon x \mapsto (r, 0), y \mapsto (s, 0), z \mapsto (0, u), w \mapsto (0, v)$ with $f(a) = (a, a)$ for all $a \in k$. This is injective since $A \cong k \oplus \bigoplus_{i+j \geq 1} kx^i y^j \oplus \bigoplus_{n+m \geq 1} kz^n w^m$ as a k-module and thus $\ker(f) = 0$. f is also integral since $(1, 0), (0, 1) \in B$ are integral over $f(A)$ via $T^2 - T$.

By the proof of Corollary 6.51, the irreducible components of Z correspond to the minimal prime ideals in A, given through $Z(\mathfrak{p}) \leftrightarrow \mathfrak{p}$. Exercise 8.52 implies that

$$\mathrm{MinSpec}(B) = \{k[r, s] \times (0), (0) \times k[u, v]\},$$
$$\mathrm{MinSpec}(A) \subseteq \{f^{-1}(k[r, s] \times (0)) = (x, y), f^{-1}((0) \times k[u, v]) = (z, w)\}.$$

Now we see that (x, y) and (z, w) are indeed minimal in A: Let $\bar{\mathfrak{p}} \in \mathrm{Spec}(A)$, i. e. $(xz, yz, xw, yw) \subseteq \mathfrak{p}$. If $x \notin \mathfrak{p}$, then $xz, xw \in \mathfrak{p}$ implies $z, w \in \mathfrak{p}$, so $(z, w) \subseteq \mathfrak{p}$; same spiel for $y \notin \mathfrak{p}$, $z \notin \mathfrak{p}$ or $w \notin \mathfrak{p}$ (in the two latter cases, we have $(x, y) \subseteq \mathfrak{p}$).

Thus the irreducible components of Z are $Z(x, y)$ and $Z(z, w)$. Their intersection is $Z(x, y) \cap Z(z, w) = Z(x, y, z, w)$ by Observation 6.15.

Alternative: We could circumvent the construction of f and the usage of the Exercise 8.52 by arguing more directly.

As above, the irreducible components correspond to the minimal prime ideals in A, i. e. the minimal prime ideals $\mathfrak{p} \subset k[x,y,z,w]$ such that $(xz, yz, xw, yw) \subseteq \mathfrak{p}$. Also as above, we have $(x,y) \subseteq \mathfrak{p}$ or $(z,w) \subseteq \mathfrak{p}$. Now (x,y) and (z,w) are prime ideals since $k[x,y,z,w]/(x,y) \cong k[z,w]$ and $k[x,y,z,w]/(z,w) \cong k[x,y]$ are integral domains. Thus we must have either $\mathfrak{p} = (x,y)$ or $\mathfrak{p} = (z,w)$.

Here a criterion for irreducible components, which makes determining decompositions very easy.

Proposition 8.54. *Let $Z = Z(\mathfrak{p}_1) \cup \cdots \cup Z(\mathfrak{p}_r)$ be an algebraic subset with prime ideals $\mathfrak{p}_i \subset k[X_1, \ldots, X_n]$ and $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ for all $i \neq j$. Then this is precisely the decomposition into irreducible components.*

Proof. Let $\mathfrak{q} \coloneqq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. Then $Z = Z(\mathfrak{q})$ by Observation 6.15, and by Hilbert's Nullstellensatz 6.23, $\sqrt{\mathfrak{q}} = I(Z(\mathfrak{q})) = \bigcap_{i=1}^r I(Z(\mathfrak{p}_i)) = \bigcap_{i=1}^r \mathfrak{p}_i = \mathfrak{q}$ since prime ideals are radical.

Let $\mathfrak{p}$ be a minimal prime ideal above $\mathfrak{q}$. We claim that there is some i such that $\mathfrak{p} = \mathfrak{p}_i$. Suppose that we have $\mathfrak{p}_i \nsubseteq \mathfrak{p}$ for all i, meaning for each i, there exists $r_i \in \mathfrak{p}_i \setminus \mathfrak{p}$. Then $r_1 \cdots r_s \in \mathfrak{q} \setminus \mathfrak{p}$, contradicting $\mathfrak{q} \subseteq \mathfrak{p}$. Hence $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i, and by minimality, $\mathfrak{p}_i = \mathfrak{p}$.

Thus each minimal prime ideal above $\mathfrak{q}$ appears as one of the $\mathfrak{p}_i$. If there would be a $\mathfrak{p}_i$ which is not minimal, then there exists a minimal $\mathfrak{p}_j$ with $\mathfrak{p}_j \subset \mathfrak{p}_i$, a contradiction to our assumption. Hence as in Corollary 6.51, there is a bijection between minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ above the radical ideal $\mathfrak{q}$ and the irreducible components $Z(\mathfrak{p}_1), \ldots, Z(\mathfrak{p}_r)$ of $Z = Z(I(Z)) = Z(\mathfrak{q})$. □

This solves the previous problem immediately, namely $Z(xz, yz, xw, yw) = Z((x,y)(z,w)) = Z(x,y) \cup Z(z,w)$.

Exercise 8.55. Determine the irreducible components of $Z(x(y+1), x(y+x^2)) \subseteq k^2$.

Solution. In combination with Observation 6.15, we have

$$\begin{aligned} Z(x(y+1), x(y+x^2)) &= Z(x(y+1, y+x^2)) = Z(x) \cup Z(y+1, y+x^2) = Z(x) \cup Z(y+1, x^2-1) \\ &= Z(x) \cup (Z(y+1) \cap Z(x^2-1)) = Z(x) \cup (Z(y+1) \cap (Z(x+1) \cup Z(x-1))) \\ &= Z(x) \cup Z(y+1, x+1) \cup Z(y+1, x-1). \end{aligned}$$

8.8 Basics in Algebraic Number Theory

Exercise 8.56 (12.1)**.** Let A be a ring, and let G be a finite group acting on A by ring automorphisms.

(i) Show that A is integral over A^G.

Hint: For $a \in A$, consider the polynomial $\prod_{g \in G}(T - g(a))$.

(ii) Assume that A is an integral domain. Show that $\mathrm{Quot}(A)^G = \mathrm{Quot}(A^G)$.

We have actually seen the hint in the introduction to algebra already, specifically [Sch, Lem. 7.4].

Solution.

(i) Let $a \in A$ be arbitrary, and let $f(T) \coloneqq \prod_{g \in G}(T - g(a)) \in A[T]$, which is monic. Let $\sigma \in G$ be arbitrary. Observe that left-multiplication with $\sigma \colon G \to G$ defines a group isomorphism, since σ is invertible. Hence $\sigma(f(T)) = \prod_{g \in G}(T - \sigma(g(a))) = \prod_{g' \in G}(T - g'(a)) = f(T)$. This shows that, after expanding f, we have $f(T) \in A^G[T]$. Since $1 \in G$, f contains a factor $T - a$, so $f(a) = 0$. Thus a is integral over A^G.

(ii) Set $K \coloneqq \mathrm{Quot}(A)$. Let $x/y \in \mathrm{Quot}(A^G)$ with $x \in A^G$ and $0 \neq y \in A^G$. Then $\sigma(x/y) = \sigma(x)/\sigma(y) = x/y$ for all $\sigma \in G$, hence $x/y \in K^G$.

Conversely, let $x/y \in K^G$ with $x \in A$ and $0 \neq y \in A$. Write $x' \coloneqq x \prod_{1 \neq g \in G} g(y) \in A$ and $y' \coloneqq \prod_{g \in G} g(y) \in A$. Then $x/y = x'/y'$. As we have seen before, $\sigma(y') = y'$ holds for all $\sigma \in G$, implying $y' \in A^G \subseteq K^G$. This gives $x' = (x/y)y' \in K^G$, hence $x' \in K^G \cap A = A^G$. In the end, $x/y = x'/y' \in \mathrm{Quot}(A^G)$.

Exercise 8.57 (12.2)**.** Let A be a normal integral domain, and let G be a finite group acting on A by ring automorphisms.

(i) Show that A^G is normal.

(ii) Let k be a field with $\operatorname{char}(k) \neq 2$. Show that $k[x,y,z]/(z^2 - xy)$ is normal.

Hint: Exercise 8.46.

Solution.

(i) Let $x \in \operatorname{Quot}(A^G)$ be integral over A^G. We have to show that $x \in A^G$. By Exercise 8.56, $x \in \operatorname{Quot}(A)^G \subseteq \operatorname{Quot}(A)$. Since x is integral over A^G, it is also integral over A. A is normal by assumption, so $x \in A$. Thus $x \in A \cap \operatorname{Quot}(A)^G = A^G$.

(ii) Consider $A = k[u,v]$. As a unique factorisation domain, it is normal according to Proposition 7.4. Consider the action of $G = \{1, \sigma\} \cong \mathbb{Z}/2$ via $\sigma(f(u,v)) = f(-u,-v)$ for all $f(u,v) \in A$. Keeping $\operatorname{char}(k) \neq 2$ in mind, we can reason completely analogous to Exercise 8.46 in order to see that $A^G = k[u^2, uv, v^2]$. Exercise 8.46 further shows that A^G admits the presentation $\cong k[u^2, uv, v^2] \cong k[x,y,z]/(z^2 - xy)$. Thus by (i), $k[x,y,z]/(z^2 - xy)$ is normal.

Exercise 8.58 (12.3)**.** Let L/K be a finite Galois extension of number fields with Galois group $G \coloneqq \operatorname{Gal}(L/K)$. Show that $\mathcal{O}_L$ is stable under the action of G on L, and that $\mathcal{O}_L^G = \mathcal{O}_K$.

Solution. Let $x \in \mathcal{O}_L$. Since x is integral over $\mathbb{Z}$, it admits a monic polynomial $f(T) \in \mathbb{Z}[T]$ such that $f(x) = 0$. By definition of Galois groups, observe that $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K = L^G$. Hence $f(\sigma(x)) = \sigma(f(x)) = g(0) = 0$, thus $\sigma(x) \in \mathcal{O}_L$ for all $\sigma \in G$, and $\mathcal{O}_L$ is stable under G.

For the second claim, we argue that $\mathcal{O}_L^G = \mathcal{O}_L \cap L^G = \mathcal{O}_L \cap K = \mathcal{O}_K$. The first equality follows from the definition of G-invariants and the fact that $\mathcal{O}_L$ is stable under G. The second equality follows from $L^G = K$ for finite Galois groups G. The third equality follows since $\mathcal{O}_L = \overline{\mathbb{Z}}^L$ and $\mathcal{O}_K = \overline{\mathbb{Z}}^K$.

Exercise 8.59 (12.4)**.** Let k be a field, and let $A \coloneqq k[x,y]/(y^2 - x^3 - x^2)$.

(i) Show that A is an integral domain.

(ii) Show that $t \coloneqq y/x \in \operatorname{Quot}(A)$ does not lie in A.

(iii) Show that t is integral over A.

(iv) Show that $\operatorname{Quot}(A) = k(t)$, and that $k[t] \subseteq \operatorname{Quot}(A)$ is the normalisation of A.

Solution.

(i) It suffices to show that $(y^2 - x^3 - x^2) \subseteq k[x,y]$ is prime, i. e. $f(x,y) = y^2 - x^3 - x^2$ is irreducible. Suppose that f is not irreducible. Considering the degree in y, there is a factorisation of f of the form $(y - g(x))(y - h(x))$ with $g(x), h(x) \in k[x]$. Expanding and comparing with coefficients of f, we see that $g(x) + h(x) = 0$ and $g(x)y(x) = -x^3 - x^2$, implying $g(x)^2 = x^3 - x^2$. But $x^3 - x^2$ can impossibly be factored as a square.

Alternative: If we consider the whole exercise, $t = y/x$ will play a big role. Since $y^2 = x^2(x+1)$ in A, we have $t^2 = y^2/x^2 = x + 1$ in $\operatorname{Quot}(A)$. Furthermore, we have $y = tx$ in $\operatorname{Quot}(A)$.

This gives the idea to consider the k-algebra map $\phi\colon k[x,y] \to k[t]$, $x \mapsto t^2 - 1$, $y \mapsto t^3 - t$. This map is constructed in such a way that $\ker(\phi) = (y^2 - x^3 - x^2)$. Indeed, we have $\phi(y^2 - x^3 - x^2) = 0$, so we may consider $\bar{\phi}\colon A \to k[s]$. Our goal is to show that $\ker(\bar{\phi}) = 0$.

Consider $\bar{f} \in \ker(\bar{\phi})$, which is of the form $\bar{f} = g(x) + yh(x)$ with $g(x), h(x) \in k[x]$. Then $\bar{\phi}(\bar{f}) = g(t^2-1) + t(t^2-1)h(t^2-1) = 0$. Observe that the left and right summand have even and odd degree, resp., hence they do not cancel each other. This shows that necessarily $g(x) = 0 = h(x)$, i. e. $\bar{f} = 0$.

Thus $\ker(\bar{\phi}) = 0$, and $\bar{\phi}$ is an injection of A into an integral domain $k[t]$.

(ii) Suppose that $t \in A$, i. e. there exists some $f(x,y) \in k[x,y]$ such that $f(x,y) \equiv y/x \mod (y^2 - x^3 - x^2)$. This implies $y - xf(x,y) \in (y^2 - x^3 - x^2)$, hence there exists some $g(x,y) \in k[x,y]$ such that $y - xf(x,y) = (y^2 - x^3 - x^2)g(x,y)$ in $k[x,y]$. If we evaluate at $x = 0$, we obtain $y = y^2 g(0,y)$, a contradiction since $y^2 \nmid y$. Thus $t \notin A$.

Alternative: Using the same $\bar{\phi}$ as above, suppose that $t \in \operatorname{im}(\bar{\phi})$, i. e. $\bar{\phi}(\bar{f}) = g(t^2-1) + t(t^2-1)h(t^2-1) = t$ with $g(x), h(x) \in k[x]$. Since the two summands do not interfere with each other and $\deg(t) = 1$, we must have $g(x) = 0$. This leaves $\deg(t(t^2-1)h(t^2-1)) = \deg(t) + \deg(t^2-1) + \deg(h(t^2-1)) \geq 2$. Thus such an $\bar{f}$ cannot exist, and $t \notin \operatorname{im}(\bar{\phi})$.

Observe that if we localise at x, we obtain the induced injective k-algebra map $A[x^{-1}] \hookrightarrow k[t, (t^2-1)^{-1}]$. Under this map, $y/x \mapsto t$. Restricting back to $\bar{\phi}$ again shows that $y/x \notin A$.

(iii) $t = y/x$ is a root of the monic $T^2 - (x+1) \in A[T]$ because $t^2 = y^2/x^2 = (x^3 + x^2)/x^2 = x + 1$.

(iv) Since $t \in \mathrm{Quot}(A)$, we already have $k(t) \subseteq \mathrm{Quot}(A)$. Conversely, observe that $A \subseteq k[t]$ since $x = t^2 - 1 \in k[t]$ and $y = t^3 - t^2 \in k[t]$ for the k-algebra generators of A. Hence $\mathrm{Quot}(A) \subseteq \mathrm{Quot}(k[t]) = k(t)$.

Notice that the normalisation of A is nothing other then $\overline{A}^{\mathrm{Quot}(A)}$. By (iii), we have $k[t] \subseteq \overline{A}^{\mathrm{Quot}(A)}$. Conversely, we know that $k[t]$ is normal by Proposition 7.4. Because of $A \subseteq k[t]$ and $\mathrm{Quot}(A) = k(t)$, we have $\overline{A}^{\mathrm{Quot}(A)} \subseteq k[t]$.

8.9 Review

Exercise 8.60. True or false?

(i) If A is a unique factorisation domain, then A is noetherian.

(ii) If A is a principal ideal domain, then A is noetherian.

(iii) If $A \subseteq B$ is a finite ring extension, then it is also integral.

(iv) A ring A is a principal ideal domain if and only if all free modules are free.

(v) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of A-modules, then $\mathrm{Hom}(M', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M'', N) \to 0$ is also exact.

(vi) If A is a local ring, then $A[X]/(X^n)$ is local again for all $n \geq 1$.

(vii) If $f \colon A \to B$ is a surjective ring map, and if A is local and $B \neq 0$, then B is also local.

(viii) $Z(y, x^2 - y - 1) \in k^2$ is irreducible.

(ix) If k is an algebraically closed field, then k (with the Zariski topology) is Hausdorff.

(x) An A-module M is free if and only if $M_{\mathfrak{p}}$ is free as an $A_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \mathrm{Spec}(A)$.

(xi) If A is a euclidean ring, and if M is a torsion-free A-module, then M is free.

(xii) There is a bijection between radical ideals in $k[x_1, \dots, x_n]$ and algebraic subsets of k^n for any field k.

(xiii) Let A be a finitely generated k-algebra that is also an integral domain. Let $0 \notin S \subseteq A$ be a multiplicative subset. Then $\dim(S^{-1}A) = \dim(A)$.

(xiv) $(7) \subseteq \mathcal{O}_{\sqrt{37}}$ is divided by three different prime ideals.

(xv) $(5) \subseteq \mathcal{O}_{\sqrt{-1}}$ is divided by two different prime ideals.

Solution.

(i) False: Consider $(X_1, X_2, \dots) \subseteq A \coloneqq k[X_1, X_2, \dots]$, which is not finitely generated. A is indeed a unique factorisation domain, since any $f \in A$ consists of finitely many terms, and we have $A = \bigcup_{n \geq 0} k[X_1, \dots, X_n]$. Hence we finde some $m \geq 0$ such that $f \in k[X_1, \dots, X_m]$, so f admits a prime factorisation.

(ii) True: Every ideal is generated by one element.

(iii) True: Corollary 5.8.

(iv) True: For the 'if' direction, note that, by assumption, each ideal $\mathfrak{a} \subseteq A$ as a A-module is free. Let $\{a_1, \dots, a_n\}$ be an A-basis of $\mathfrak{a}$. Then $a_1 a_2 - a_2 a_1 = 0$, so we must have $n = 1$.

For the 'only if' direction, if the module is finitely generated, we use the structure theorem 3.52 since any submodule of a torsion-free module is torsion-free as well. The general case follows by transfinite induction over ordinals.

(v) False: The contravariant Hom-functor is left-exact (Proposition 8.33).

(vi) True: The prove is similar to Proposition 1.47, i. e. we show that $\bar{f} \in (A[X]/(X^n))^\times$ if and only if the constant term of $\bar{f}$ is in $A^\times$.

(vii) True: By the homomorphism theorem, we have $A/\ker(f) \cong B$. Since the ideals of $A/\ker(f)$ correspond to the ideals in A containing $\ker(f)$, $A/\ker(f) \cong B$ are local.

(viii) False:

$$\begin{aligned} Z(y, x^2 - y - 1) = Z(y, x^2 - 1) &= Z(y) \cap Z(x^2 - 1) = Z(y) \cap (Z(x-1) \cup Z(x+1)) \\ &= (Z(y) \cap Z(x-1)) \cup (Z(y) \cap Z(x+1)) = Z(y, x+1) \cup Z(y, x-1). \end{aligned}$$

(ix) False: Show that the intersection of two non-empty open sets is again non-empty.

(x) False: Consider the Dedekind ring $A = \mathbb{Z}[\sqrt{-5}]$ and the non-principal ideal $M = (2, 1+\sqrt{-5}) \subseteq A$. Then $M_\mathfrak{p} \subseteq A_\mathfrak{p}$ is locally free for all $\mathfrak{p} \in \operatorname{Spec}(A)$, but M is not free, e. g. $3 \cdot 2 - (1-\sqrt{-5})(1+\sqrt{-5}) = 0$.

(xi) False: $\mathbb{Q}$ as a $\mathbb{Z}$-module is not free (see Exercise 8.1), but $\mathbb{Q}$ is torsion-free since the $\mathbb{Z}$-module structure originates from the multiplication in the field $\mathbb{Q}$.

(xii) False: Consider $k = \mathbb{R}$, which is not algebraically closed. Then $(1) \mapsto \varnothing$ and $(x^2+1) \mapsto \varnothing$. Note that $(x^2+1) \subseteq \mathbb{R}[x]$ is radical since x^2+1 is irreducible over $\mathbb{R}$.

(xiii) False: Consider $A = k[T]$ and $S = A \setminus \{0\}$. Then $\dim(S^{-1}A) = \dim(\operatorname{Quot}(A)) = 0 \neq 1 = \dim(A)$. But cf. Proposition 6.59.

(xiv) False: Recall Example 7.31. The minimal polynomial of $\sqrt{37}$ has at most two factors over $\mathbb{Z}$, so there are at most two prime ideals above (7).

(xv) True: By the Chinese remainder theorem 8.5, we have

$$\begin{aligned} \mathcal{O}_{\sqrt{-1}}/(5) \cong \mathbb{F}_5[T]/(T^2+1) \cong \mathbb{F}_5[T]/(T+2) \times \mathbb{F}_5[T]/(T+3) \cong \mathbb{F}_5 \times \mathbb{F}_5 \\ \implies |\operatorname{Spec}(\mathcal{O}_{\sqrt{-1}}/(5))| = |\operatorname{Spec}(\mathbb{F}_5 \times \mathbb{F}_5)| = 2. \end{aligned}$$

Exercise 8.61. Compute the Noether normalisation of the following rings:

(i) $k[x, x^{-1}]$.

(ii) $k[x, y, z]/(y - z^2, xz - y^2)$.

Solution.

(i) We have $k[x, x^{-1}] \cong k[x, y]/(xy - 1)$. We claim that $k[\bar{x} + \bar{y}] \subseteq k[\bar{x}, \bar{y}]$ is integral. Indeed, $\bar{x}$ is a root of the monic non-zero polynomial $T^2 - (\bar{x} + \bar{y})T + 1 \in k[\bar{x} + \bar{y}][T]$. Similarly for $\bar{y}$.

(ii) We have $k[x, y, z]/(y - z^2, xz - y^2) \cong k[x, z]/(xz - z^4)$. We claim that $k[\bar{x}] \subseteq k[\bar{x}, \bar{z}]$ is integral. Indeed, $\bar{z}$ is a root of the monic non-zero polynomial $T^4 - \bar{x}T \in k[\bar{x}][T]$.

A Appendix

A.1 Donating Computing Power for Number Theory Research

Databases like [LMF] require a lot of computation, and this database in particular was contributed by a handful of people. The data on number fields includes data from John Jones and David Roberts, which in turn include data from the project *NumberFields@home* by Eric D. Driver. This project is remarkable since it is a distributed computing project and runs on home computers of volunteers, and you (yes, you!) can contribute by donating free clock cycles. For more information on the theoretical site, check out the project description.

A.2 Mumford's Treasure Map

I came across very interesting and actually very deep depictions of spectra in algebraic geometry. These are all from Mumford's [Mum], a very influential book back in the days where intuition in algebraic geometry was almost non-existent. You can read a bit of trivia and an explanation of Figure A.5 in the great blog post [Leb].

I decided to just put the Figures A.1 to A.5 here and let you philosophise on them and behold them in awe. If not noted otherwise, all pictures are self-made screenshots.

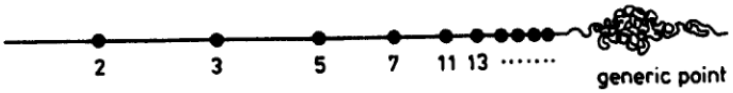


Figure A.1: Spec($\mathbb{Z}$).

Figure A.2: Spec(A) for a discrete valuation ring (A, M).

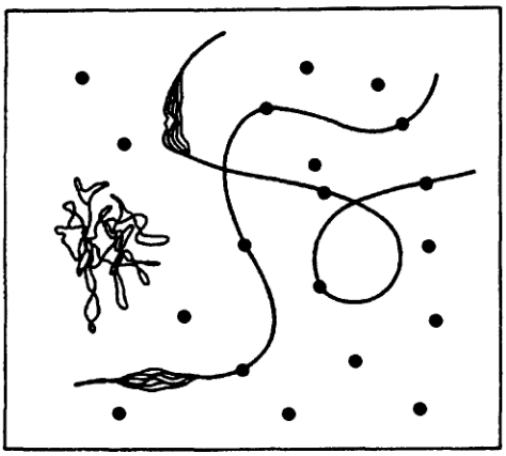


Figure A.3: Spec($k[X, Y]$) for algebraically closed fields k.

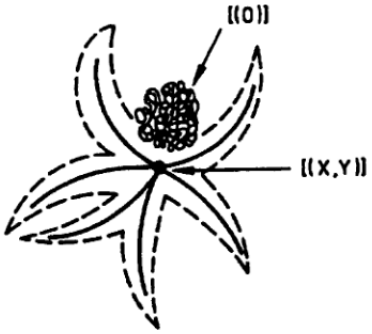


Figure A.4: Spec(Quot($k[X, Y]$)) for algebraically closed fields k.

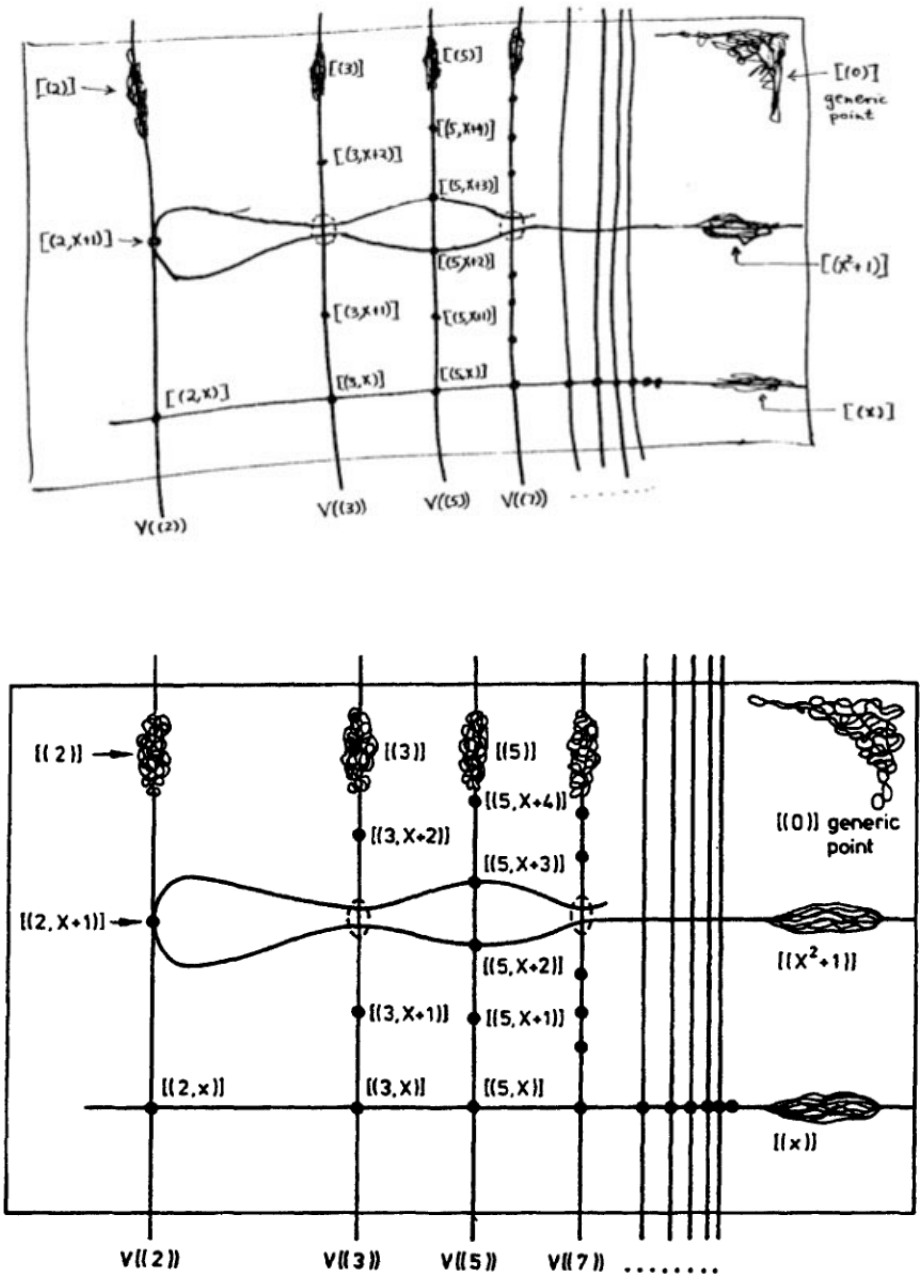


Figure A.5: Spec($\mathbb{Z}[X]$). The first picture is from the urtext (source), the second from the Springer edition. In our notation, $V((p)) \coloneqq Z((p))$.