ALGEBRAIC NUMBER THEORY

SUMMER 2024

Contents

Organization. Here are the coordinates for the lecture:

- Tuesdays, 9:50–11:20 & Fridays, 11:40–13:20 in Room S215 401 and via Zoom (Meeting-ID: 654 2542 5948, Password: Largest six digit number divisible by 3.)
- First lecture: April 16, Last lecture: July 19
- A total of 28 lectures of 90 minutes each.
- Exam either oral or written depending on the number of participants.

Exercises. The exercises will be written in the present manuscript. Also, there will be exercise sessions that provide room for discussing and solving the exercises together other participants of the course. These will take place:

- Wednesdays, 11:40–13:20 in Room S215 401
- First session: April 24, Last session: July 17

Literature. The present lecture is based on handwritten notes by Torsten Wedhorn. The author thanks him heartily for sharing them. Besides, there is a lot of literature on the subject. Here is a selection that the author used (in part) to prepare the lecture:

- The book of Kato–Kurokawa–Saito [KKS00] gives a motivated introduction to elementary number theory with many historical comments. A must read!
- The book of Neukirch [Neu99] belongs to the classics. The content of the lectures (very) roughly correspond to the material in Chapters I & II in Neukirch's book.
- The second book of Kato–Kurokawa–Saito [KKS11] is great as well. The lectures will work towards the contents of the book, but will probably not cover much of it. However, the examples, especially in the beginning of the book, are very instructive.
- Other excellent introductions to the topic include the books of Lang [Lan94], Zagier [Zag81] and Cassels–Fröhlich [CF86] as well as the course notes of Milne [Mil].

Comments. The present manuscript might not cover everything that will be discussed during the lecture and thus relevant for the final exam. However, it will probably contain most of it.

Any comments regarding typos, mistakes, presentation of the material etc. are highly welcome! Please talk to me during the lecture.

1. Introduction

Algebraic number theory, or from the author's perspective, arithmetic algebraic geometry is a branch of mathematics that deals with solution spaces of polynomial equations. Solutions in the integers $\mathbb{Z}$ (or, the rational numbers $\mathbb{Q}$) are of particular interest. Here is a famous problem:

Problem 1.1. Find all $x, y, z \in \mathbb{Z}$ that satisfy the quadratic equation $x^2 + y^2 = z^2$.

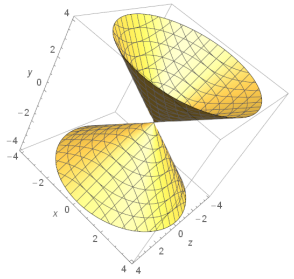
Here are all triples, up to multiples, with $1 \leq x, y, z \leq 100$:

$$\begin{array}{cccc} (3,4,5) & (5,12,13) & (8,15,17) & (7,24,25) \\ (20,21,29) & (12,35,37) & (9,40,41) & (28,45,53) \\ (11,60,61) & (16,63,65) & (33,56,65) & (48,55,73) \\ (13,84,85) & (36,77,85) & (39,80,89) & (65,72,97) \end{array}$$

For example, $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$ and so on. Such triples are called *Pythagorean triples*. Each corresponds to a right triangle with hypothenuse of length z and the two other sides of length x and y respectively. We will see soon that there are infinitely many Pythagorean triples and how to parametrize them.

Geometrically, the problem asks to find all lattice points lying on the yellow conic depicted below. That is, put the standard lattice $\mathbb{Z}^3$ inside $\mathbb{R}^3$ and ask yourself at which points does the yellow conic intersect the lattice points.

Before discussing the solution to Problem 1.1, let us look at another famous problem. Namely, we enlarge the degree of the variables in the former equation:



Picture of $x^2 + y^2 = z^2$ in $\mathbb{R}^3$.

Problem 1.2. Let $n \geq 3$. Find all $x, y, z \in \mathbb{Z}$ that satisfy the equation $x^n + y^n = z^n$.

The outcome is completely different: There are no triples with $xyz \neq 0$. Pierre de Fermat (17th century) wrote in his copy of Diophantus's arithmetica that he had a proof that was, however, too large to fit in the margin. Fermat's notes of the proof were never found. It took more than 350 years and the work of many mathematicians until the proof was finally completed by Andrew Wiles in 1994. That this particular problem, which goes under the name "Fermat's last theorem", is so famous seems rather the result of many failed attempts to come up with solutions but less the importance of this specific equation for number theory. However, by trying to solve Problem 1.2 a lot of beautiful mathematics was developed during the past centuries, some of which we will see during the lectures. Let us now come back to studying quadratic equations in more detail.

Conics. Let $a, b, c \in \mathbb{Z}$. Consider the following equation:

$$ax^2 + by^2 = c \tag{1.1}$$

Such equations are examples of *conics*, and you can go to WolframAlpha, for example, to draw pictures in $\mathbb{R}^2$ for particular choices of a, b and c.

Question 1.3. Are there $x, y \in \mathbb{Z}$ (or, $x, y \in \mathbb{Q}$) such that $ax^2 + bx^2 = c$?

Or, even better: Describe the solution sets $\{(x, y) \mid ax^2 + bx^2 = c\}$ with (x, y) in $\mathbb{Z}^2$ and in $\mathbb{Q}^2$ respectively. We will see that if a solution exists, then it is not hard to describe the solution sets. However, the existence of a solution is more involved as we will see soon. Let us consider the following cases:

(A) Unit circle and other conics with solutions. Assume $a = b = c = 1$. Then, Equation (1.1) takes the form

$$x^2 + y^2 = 1, \tag{1.2}$$

which describes the unit circle in $\mathbb{R}^2$. Solutions in $\mathbb{Z}^2$ are easily determined to be $\{(0, \pm 1), (\pm 1, 0)\}$. Solutions in $\mathbb{Q}^2$ are more interesting:

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1 \iff 3^2 + 4^2 = 5^2$$

Thus, by clearing denominators in $x, y \in \mathbb{Q}$, we see that rational solutions of the unit circle (1.2) correspond to the Pythagorean triples from Problem 1.1. Now, if $(x, y) \in \mathbb{Q}^2$ lies on the unit circle (1.2) and if $(x, y) \neq (-1, 0)$, then the slope of the line joining $(-1, 0)$ and (x, y) is $\frac{y}{x+1}$.

Exercise 1.4. Show that the map $(x, y) \mapsto \frac{y}{x+1}$ induces a bijection

$$\left\{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\right\} \xrightarrow{1:1} \mathbb{Q} \cup \{\infty\}.$$

More generally, assume that $abc \neq 0$ and that $ax^2 + by^2 = c$ *has some* solution $P := (x_0, y_0) \in \mathbb{Q}^2$. Then, one has the following bijection:

$$\begin{aligned} \left\{Q = (x, y) \in \mathbb{Q}^2 \mid ax^2 + by^2 = c\right\} &\xrightarrow{1:1} (\mathbb{Q} \cup \{\infty\}) \backslash \{\text{at most 2 elements}\} \\ Q &\longmapsto \text{slope of line } \overline{PQ} \text{ joining } P \text{ and } Q \end{aligned}$$

Here, for $P = Q$, the line $\overline{PQ}$ is the tangent line to the real conic $\{(x, y) \in \mathbb{R}^2 \mid ax^2 + by^2 = c\}$, and the slope is ∞ if $\overline{PQ}$ is parallel to the y-axis (as is the case for $(x, y) = (-1, 0)$ in Exercise 1.4). The phrase "at most 2 elements" means that we remove $\pm\sqrt{-\frac{a}{b}}$ from $\mathbb{Q} \cup \{\infty\}$ if $-\frac{a}{b}$ is a square of a rational number, otherwise we remove nothing from $\mathbb{Q} \cup \{\infty\}$. The reader is referred to [KKS00, Chapter 2] for more on this subject.

So, we conclude that if a rational solution to (1.1) exists, then there are infinitely many such solution and we can parametrize them explicitly. However, the existence of a rational solution is more subtle as we will see now.

(B) Existence of solutions. Here we will only focus on special cases leaving the rest to the curious reader. In the following, let p be an *odd*[1] prime number.

Proposition 1.5. *There exist $(x, y) \in \mathbb{Z}^2$ satisfying*

(1) the equation $x^2 + y^2 = p$ if and only if $p \equiv 1 \mod 4$,

[1]We leave it to the reader to adjust the statements in the case $p = 2$.

(2) the equation $x^2 + 2y^2 = p$ if and only if $p \equiv 1$ or $3 \mod 8$,
(3) the equation $x^2 + 3y^2 = p$ if and only if $p \equiv 1 \mod 3$, and
(4) the equation $x^2 - 2y^2 = p$ if and only if $p \equiv 1$ or $7 \mod 8$.

In each case, if there is no integral solution, then there is no rational solution as well.

We will focus on Part (1) of the proposition. For a proof of Parts (2), (3) and (4) the reader is referred to [KKS00, Chapter 4]. The conditions on p for the existence of solutions are examples of so-called "reciprocity laws". Arguably, the most complete picture of such laws we have of today is given by a web of theorems and conjectures going under the name of *Langlands program*, named after the Canadian mathematician Robert Langlands (still alive). We refer to Emerton's survey for a great overview [Eme21].

Exercise 1.6. Let $x, y \in \mathbb{Z}$. Show that if x^2+y^2 is an odd integer, then $x^2+y^2 \equiv 1 \mod 4$, i.e., $x^2 + y^2 = 4k + 1$ for some $k \in \mathbb{N}$.

The exercise solves the "only if" direction in Part (1). For the converse direction, we consider the ring $\mathbb{Z}[i] = \{x+iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ where $i \in \mathbb{C}$ is a fixed square root of -1. The ring, named after Carl-Friedrich Gauss, is called *Gaussian integers*. In this ring, we have a factorization

$$x^2 + y^2 = (x + iy)(x - iy)$$

for all $x, y \in \mathbb{Z}$. Fortunately, factorizations in $\mathbb{Z}[i]$ are well-behaved. The following lemma implies that $\mathbb{Z}[i]$ is a principal ideal domain, in particular, an unique factorization domain:

Lemma 1.7. *The ring $\mathbb{Z}[i]$ is euclidean.*

Proof. The ring $\mathbb{Z}[i]$ is a domain as a subring of $\mathbb{C}$. The square of the complex absolute value induces a norm map $N(-) := |-|^2 \colon \mathbb{Z}[i] \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$ that makes $\mathbb{Z}[i]$ into an euclidean ring: for $a, b \in \mathbb{Z}[i]$ with $b \neq 0$ let $q \in \mathbb{Z}[i]$ such that $|\frac{a}{b} - q|$ is minimal. Here we think about $\mathbb{Z}[i] \subset \mathbb{C}$ as defining the vertices of a grid in the complex plane with mesh size 1. Since the mesh size is 1, we have $|\frac{a}{b} - q| \leq \frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$, and so $N(\frac{a}{b} - q) = |\frac{a}{b} - q|^2 \leq \frac{1}{2}$. This implies

$$N(a - qb) \leq \frac{N(b)}{2} < N(b).$$

Hence, we reached the desired division with remainder $a = qb+r$ with $N(r) < N(b)$ for $r := a - qb$. □

In particular, every element of $\mathbb{Z}[i]$ is a product of prime elements. Examples of such prime factorizations are $5 = 2^2 + 1^2 = (2 + i)(2 - i)$ and $13 = 3^2 + 2^2 = (3 + 2i)(3-2i)$. By the general theory of unique factorization domains, the factorizations are unique up to multiplication by units.

Exercise 1.8. Show that $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Deduce that an element $a \in \mathbb{Z}[i]$ is prime if its norm $N(a)$ is a prime number.

The exercise shows that if $p = (x + iy)(x - iy)$ for some $x, y \in \mathbb{Z}[i]$, then $x \pm iy$ are the prime factors of p in $\mathbb{Z}[i]$, i.e., p is not a prime element in the Gaussian integers.

Lemma 1.9. *Let $\mathbb{F}_p$ be the finite field with p elements. The following are equivalent:*

(1) *There exist* $x, y \in \mathbb{Z}$ *such that* $p = (x + iy)(x - iy)$ *in* $\mathbb{Z}[i]$.
(2) *The element* p *is not prime in* $\mathbb{Z}[i]$.
(3) *The polynomial* $T^2 + 1$ *is not irreducible in* $\mathbb{F}_p[T]$.
(4) *The element* -1 *is a square in* $\mathbb{F}_p$.

Proof. We leave the equivalence of (1) and (2) to the reader (Hint: For the implication (2) $\implies$ (1), consider the prime factorization of p in $\mathbb{Z}[i]$ and use the norm to conclude that p has exactly two prime factors.). For the equivalence of (2) and (3) we note that there are ring isomorphisms

$$\mathbb{Z}[i]/p\mathbb{Z}[i] \overset{i \leftarrow\!\shortmid T}{=} \mathbb{Z}[T]/(T^2 + 1, p) = \mathbb{F}_p[T]/(T^2 + 1). \tag{1.3}$$

Thus, p is prime $\mathbb{Z}[i]$ if and only if the ideal $p\mathbb{Z}[i]$ is a prime ideal if and only if the ring (1.3) is a domain if and only if $T^2 + 1$ is irreducible. Finally, condition (3) is equivalent to (4) because a quadratic polynomial over a field is not irreducible if and only if it has a zero. □

Thus, we are reduced to studying when -1 is a square in $\mathbb{F}_p$.

Exercise 1.10. Show that the following sequence of abelian groups

$$1 \longrightarrow (\mathbb{F}_p^\times)^2 \overset{\text{inclusion}}{\longrightarrow} \mathbb{F}_p^\times \overset{x \mapsto x^{\frac{p-1}{2}}}{\longrightarrow} \{\pm 1\} \longrightarrow 1$$

is exact where $(\mathbb{F}_p^\times)^2 = \{x^2 \mid x \in \mathbb{F}_p\}$.

For an element $x \in \mathbb{F}_p^\times$, the *Legendre symbol* is defined as

$$\left(\frac{x}{p}\right) := x^{\frac{p-1}{2}} \overset{1.10}{=} \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{F}_p \\ -1, & \text{else.} \end{cases} \tag{1.4}$$

Now, a calculation shows that $(\frac{-1}{p}) = 1$ if and only if $p \equiv 1 \mod 4$, which finishes the proof Proposition 1.5(1). More generally, the Legendre symbol $(\frac{x}{p})$ can be calculated using the quadratic reciprocity law [KKS00, Chapter 2.2, Theorem 2.2] proved by Gauss in 1796.

Upshot. Given a finite field extension $K \supset \mathbb{Q}$, also called a *number field*, its *ring of integers* is defined as

$$O_K = \{a \in K \mid a \text{ integral over } \mathbb{Z}\}, \tag{1.5}$$

where an element $a \in K$ is called *integral* if there exists a monic (i.e., the leading coefficient is equal to 1) polynomial $f \in \mathbb{Z}[T]$ with $f(a) = 0$. For example, for $K = \mathbb{Q}[i] = \{x + iy \mid x, y \in \mathbb{Q}\}$, one can show that $O_K = \mathbb{Z}[i]$, which is the ring of Gaussian integers that popped up while studying Proposition 1.5(1). Likewise, (2), (3) and (4) in Proposition 1.5 naturally lead to the number fields $\mathbb{Q}[\sqrt{-2}]$, $\mathbb{Q}[\sqrt{-3}]$ and $\mathbb{Q}[\sqrt{2}]$ respectively.

Thus, a major part of this course will consist in studying prime factorizations in O_K for general number fields K. A problem, to be addressed in the lecture, is that the ring O_K is usually not a unique factorization domain, in particular, not a principal ideal domain and not euclidean. We have to understand how far O_K is from admitting unique factorizations into primes and develop the necessary theory in order to deal with such rings.

2. Dedekind domains

The number rings O_K from (1.5) are examples of Dedekind domains, which are generalizations of principal ideal domains. An important technical observation is that their localizations at non-zero prime ideals are discrete valuation rings. In the final subsection, we define the so-called fundamental exact sequence which measures the failure of O_K from being a principal ideal domain:

2.1. **Discrete valuation rings.** All rings are assumed to be unital and commutative. Recall that every ring $R \neq 0$ has a maximal ideal, and that R is called *local* if it has exactly one maximal ideal. Further, a ring R is called a *domain* if (0) is a prime ideal in R, i.e., $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in R$. Domains are called *principal ideal domains* if, in addition, every ideal can be generated by a single element. We note that a domain with exactly one prime ideal is a field.

Definition 2.1. A *discrete valuation ring* is a local principal ideal domain that is not a field.

Remark 2.2. Let R be a discrete valuation ring. Any generator $\pi \in R$ of the maximal ideal is called a *uniformizer*. Then, π is, up to multiplication by units, the unique prime element in R. Every non-zero element $a \in R$ can be written in the form $a = u_a \pi^{n_a}$ for unique elements $u_a \in R^\times$ and $n_a \in \mathbb{Z}_{\geq 0}$. In particular, we can define a multiplicative map $v\colon R - \{0\} \to \mathbb{Z}$ by $v(a) := n_a$. It can be extended to the fraction field $K := \mathrm{Frac}(R)$ by the rule $v(\frac{a}{b}) = v(a) - v(b)$ for non-zero $a, b \in R$, and then defines a group homomorphism $v\colon K^\times \to \mathbb{Z}$ such that $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K$ with $a, b, a + b$ non-zero. We have $R - \{0\} = \{a \in K^\times \mid v(a) \geq 0\}$.

Definition 2.3. A *valuation (of rank 1)* on a field K is a group homomorphism $v\colon K^\times \to \mathbb{R}$ such that $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K$ with $a, b, a + b$ non-zero. It is *discrete* if $v(K^\times) = \alpha\mathbb{Z}$ for some non-zero $\alpha \in \mathbb{R}$ ($\iff$ $v(K^\times) \subset \mathbb{R}$ non-zero, discrete subgroup), and *normalized* if $v(K^\times) = \mathbb{Z}$.

We extend the valuation $v\colon K \to \mathbb{R} \cup \{\infty\}$ by setting $v(0) := \infty$. By convention, ∞ is bigger than all elements of $\mathbb{R}$.

Proposition 2.4. *Let K be a field, and $v\colon K \to \mathbb{R} \cup \{\infty\}$ a valuation. Then,*

$$O_K := \{a \in K \mid v(a) \geq 0\}$$

is a local subring with maximal ideal $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$ and unit group $O_K^\times = \{a \in K \mid v(a) = 0\}$. Further, for all $a \in K^\times$ either $a \in O_K$ or $a^{-1} \in O_K$ (or, both). If v is discrete, then O_K is a discrete valuation ring.

Proof. Let $a, b \in O_K$, i.e., $a, b \in K$ and $v(a), v(b) \geq 0$. Then, $v(ab) = v(a)+v(b) \geq 0$ and $v(a+b) \geq \min\{v(a), v(b)\} \geq 0$, so $ab, a+b \in O_K$. As $v(1) = v(1\cdot 1) = v(1)+v(1)$ we see $v(1) = 0$ and so $1 \in O_K$. This shows that O_K is a (necessarily commutative, unital) subring of K, hence a domain.

The equality $O_K^\times = \{a \in K \mid v(a) = 0\}$ is checked using $v(a^{-1}) = -v(a)$ for $a \in K^\times$. In particular, for every ideal $I \subset O_K$, we have either $I \subset \mathfrak{m}$ or $I = O_K$

(the latter happens if there exists $a \in I$ with $v(a) = 0$, so $a \in O_K^\times$ by the description of units). This shows that $\mathfrak{m}$ is the unique maximal ideal in O_K.

Next, if $a \in K^\times$, then $v(a) \geq 0$ or $v(a) \leq 0$. In the latter case, $a \neq 0$ and $v(a^{-1}) = -v(a) \geq 0$, i.e., $a^{-1} \in O_K$. We also see $K = \mathrm{Frac}(O_K)$.

Finally, assume v is discrete and choose $\alpha \in \mathbb{R}_{>0}$ with $V(K^\times) = \alpha\mathbb{Z}$. Since $v(O_K \backslash \{0\}) = \alpha\mathbb{Z}_{\geq 0}$, the domain O_K is not a field. Choose $\pi \in \mathfrak{m}$ of minimal valuation, i.e., $v(\pi) = \alpha$. Let $I \subset O_K$ be an ideal. We claim that $I = (\pi^n)$ where $n \in \mathbb{Z}_{\geq 0}$ is minimal such that $n\alpha \in v(I\backslash\{0\})$, the latter regarded as a subset of $\alpha\mathbb{Z}_{\geq 0}$. Indeed, if $a \in I\backslash\{0\}$, then $v(a\pi^{-n}) = v(a) - v(\pi^n) = v(a) - n\alpha \geq 0$, i.e., $a = \pi^n b$ for some $b \in O_K$. This shows $I \subset (\pi^n)$. If $a \in I\backslash\{0\}$ is of minimal valuation, then $v(a) = n\alpha = v(\pi^n)$ by construction and so $\pi^n = ua$ for some $u \in O_K^\times$. This shows $\pi^n \in I$. In particular, O_K is a principal ideal domain. □

Example 2.5.
(1) For a prime number $p \in \mathbb{Z}$, the ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ p \nmid b\}$ is a discrete valuation ring with uniformizer p. The associated valuation $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is called the *p-adic valuation*. We note that $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal (p).
(2) Let k be a field. For an irreducible polynomial $p \in k[T]$, the ring $k[T]_{(p)} = \{\frac{a}{b} \in k(T) \mid a, b \in k[T],\ p \nmid b\}$ is a discrete valuation ring with uniformizer p. It is the localization of $k[T]$ at the prime ideal (p).

The following exercise generalizes the examples:

Exercise 2.6. Let R be a principal ideal domain, and $p \in R$ a prime element. Show that $R_{(p)} = \{\frac{a}{b} \in \mathrm{Frac}(R) \mid a, b \in R,\ p \nmid b\}$ is a discrete valuation ring with uniformizer p. It is the localization of R at the prime ideal (p).

Reminder 2.7. Some of the following properties might be known from algebra lectures during the past semesters:

(1) A ring R is called *noetherian* if every ideal is finitely generated.
(2) The *(Krull) dimension* $n \in \mathbb{N} \cup \{\infty\}$ of a ring R is the supremum of the length of strict chains of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_n$. It is denoted $\dim(R) := n$.
(3) A domain R is called *normal* (or, *integrally closed*) if the inclusion
$$R \subset \{a \in \mathrm{Frac}(R) \mid \exists f \in R[T] \text{ monic: } f(a) = 0\}$$
is an equality. A domain R is normal if and only if the localizations $R_\mathfrak{p}$ are normal for all prime ideals $\mathfrak{p} \subset R$ if and only if the localizations $R_\mathfrak{m}$ are normal for all maximal ideals $\mathfrak{m} \subset R$, see [Sta18, 030B].

One has the following implications:

$$\text{DVR} \implies \text{euclidean} \implies \text{PID} \implies \text{UFD} \implies \text{normal domain} \implies \text{domain}$$

Here DVR:="discrete valuation ring", UFD:="unique factorization domain" and PID:="principal ideal domain". In addition, every principal ideal domain is noetherian of dimension ≤ 1.

Theorem 2.8. *For a ring R, the following are equivalent:*

(1) The ring R is a discrete valuation ring.
(2) The ring R is a domain, and there exists a discrete valuation $v \colon \mathrm{Frac}(R) \to \mathbb{R} \cup \{\infty\}$ such that
$$R = \{a \in \mathrm{Frac}(R) \mid v(a) \geq 0\}.$$

(3) *The ring R is noetherian, local, has dimension > 0 and its maximal ideal is principal.*
(4) *The ring R is a noetherian, local, normal domain of dimension* 1.

The proof is given below and uses the following result from commutative algebra. We apply this result to local rings R, in which case the Jacobson radical $\mathrm{Jac}(R)$ appearing below is the maximal ideal.

Lemma 2.9 (Krull's intersection theorem)**.** *Let R be a noetherian ring and $I \subset \mathrm{Jac}(R)$. Then, for any finitely generated R-module, one has*

$$\bigcap_{n\geq 1} I^n M = \{0\}.$$

Proof. See [Sta18, 00IP, 00IQ] for details. □

Proof of Theorem 2.8. (1) $\iff$ (2): Follows from Remark 2.2 and Proposition 2.4.

(1) $\implies$ (3) & (1) $\implies$ (4): Follows from Reminder 2.7.

(3) $\implies$ (2): Let $(\pi) \subset R$ be the maximal ideal. Then, π is not nilpotent: indeed, if $\pi^n = 0$ for some $n \in \mathbb{Z}_{\geq 1}$, then π is contained in every prime ideal and so is the maximal ideal (π), which contradicts the assumption $\dim(R) > 0$.

Now, for $a \in R$ define

$$v(a) := \sup\{n \in \mathbb{N} \mid a \in (\pi^n)\} \subset \mathbb{N} \cup \{\infty\}.$$

Lemma 2.9 shows that $a = 0$ if and only if $v(a) = \infty$. Also, $v(a) = n \in \mathbb{N}$ if and only if $a = u\pi^n$ for some $u \in R\backslash(\pi) = R^\times$. Using this, one checks that R is a domain, $v(ab) = v(a) + v(b)$ and $v(a + b) \geq \min\{v(a), v(b)\}$. Then, v can be extended to the fraction field $\mathrm{Frac}(R)^\times$ by the rule $v(\frac{a}{b}) = v(a) - v(b)$ for non-zero $a, b \in R$. It defines a discrete valuation such that $R = \{a \in \mathrm{Frac}(R) \mid v(a) \geq 0\}$.

(4) $\implies$ (3): We need to show that the maximal ideal $\mathfrak{m} \subset R$ is principal. Since R is a domain with $\dim(R) = 1$, the ideals $(0) \subsetneq \mathfrak{m}$ are the only prime ideals in R. Hence, for any non-zero $a \in \mathfrak{m}$, we have

$$\sqrt{(a)} = \bigcap_{a\in\mathfrak{p}} \mathfrak{p} = \mathfrak{m}$$

where the intersection runs over all prime ideals $\mathfrak{p} \subset R$ with $a \in \mathfrak{p}$. Since R is noetherian, the ideal $\mathfrak{m}$ is finitely generated. So, there exists $n \geq 1$ such that $\mathfrak{m}^n \subset (a)$. Assume n is minimal with the property, i.e., $\mathfrak{m}^{n-1} \not\subset (a)$. Choose $b \in \mathfrak{m}^{n-1}\backslash(a)$ and set $\pi := \frac{a}{b} \in K := \mathrm{Frac}(R)$. We claim that $\mathfrak{m} = (\pi)$. For this, we observe the following properties:

(1) $\pi^{-1}\mathfrak{m} = \frac{b}{a}\mathfrak{m} \subset \frac{1}{a}\mathfrak{m}^n \subset R$
(2) $\pi^{-1} \notin R$ (indeed, $\pi^{-1} = \frac{b}{a} \in R \implies b \in (a)\lightning$)
(3) $\pi^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ (hence, $\pi^{-1}\mathfrak{m} = R$ by (1) and so $\mathfrak{m} = (\pi)$)

Property (1) follows from the definition and (2) is proven above. For (3), assume $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$. Then, we have an endomorphism $\mathfrak{m} \to \mathfrak{m}$, $x \mapsto \pi^{-1}x$. Since $\mathfrak{m}$ is finitely generated, we can apply Cayley-Hamiliton. So, there exist $r \in \mathbb{N}$ and $a_1, \ldots, a_r \in R$ with $(\pi^{-1})^r + a_1(\pi^{-1})^{r-1} + \cdots + a_r = 0$, i.e., π^{-1} is integral over R. Since R is assumed to be normal, we get $\pi^{-1} \in R$, which contradicts (2). Hence, (3) holds, which shows the claim and finishes the proof. □

2.2. **Dedekind domains.**

Definition 2.10. A noetherian domain R is called *Dedekind domain* if for every prime ideal $\mathfrak{p} \neq (0)$ the localization $R_\mathfrak{p}$ is a discrete valuation ring.

Remark 2.11. If R is a Dedekind domain, then $\dim(R) \leq 1$. In this case, $\dim(R) = 0$ if and only if R is a field. If $\dim(R) = 1$, then the prime ideals $\mathfrak{p} \neq 0$ are exactly the maximal ideals of R. Further, Exercise 2.6 shows that all principal ideal domains are Dedekind domains.

Theorem 2.12. *Let R be a Dedekind domain and M a finitely generated R-module. Then, the following are equivalent:*

(1) The module M is torsion free, i.e., for all $a \in R, 0 \neq m \in M$ with $am = 0$ one has $a = 0$.
(2) The module M is projective.
(3) The localization $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m} \subset R$.

In this case, the number $\operatorname{rank}_{R_\mathfrak{m}}(M_\mathfrak{m})$ in (3) is independent of $\mathfrak{m}$ and equal to $\dim_K(M \otimes_R K)$ where $K = \operatorname{Frac}(R)$ is the fraction field.

For the proof we use the following result from commutative algebra:

Lemma 2.13. *Let R be a noetherian ring and M a finitely generated R-module. Then, the following are equivalent:*

(1) The R-module M is projective.
(2) The localization $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module for all prime ideals $\mathfrak{p} \subset R$.
(3) The localization $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m} \subset R$.

Moreover, if there exists no idempotent e (i.e., $e^2 = e$) with $e \neq 0, 1$, then the map $\{\text{prime ideals}\} \to \mathbb{N}$, $\mathfrak{p} \mapsto \operatorname{rank}_{R_\mathfrak{p}}(M_\mathfrak{p})$ is constant. It is called the rank of M.

Proof. See [Sta18, 00NX] for details. Note that over noetherian rings any finitely generated module is finitely presented. So, the conditions in *loc. cit.* are satisfied. □

Exercise 2.14. Let R domain, $K = \operatorname{Frac}(R)$ and M an R-module. Show the following statements:

(1) The module M is torsion free if and only if $M \to M \otimes_R K, m \mapsto m \otimes 1$ is injective.
(2) If M torsion free and $S \subset R \backslash \{0\}$ multiplicative subset (i.e., $1 \in S$ and S closed under multiplication), then $M[S^{-1}]$ is a torsion free $R[S^{-1}]$-module.
(3) The module M is torsion free if and only if $M_\mathfrak{p}$ is a torsion free $R_\mathfrak{p}$-module for all prime ideals $\mathfrak{p} \subset R$.

Proof of Theorem 2.12. The final statement on the rank follows from Lemma 2.13 and the fact that the fraction field K is the localization of R at the prime ideal (0), i.e., $K = R_{(0)}$.

(2) $\iff$ (3): Follows from Lemma 2.13.

(1) $\iff$ (3): Using Exercise 2.14, we can pass to $R_\mathfrak{p}$ for $\mathfrak{p} \subset R$ prime ideal and assume without loss of generality that R is a principal ideal domain. In this case, M is torsion free if and only if M is free is well-known from "Introduction to Algebra", see also [Sta18, 0AUW] for details. □

Definition 2.15. Let R domain and $K := \operatorname{Frac}(R)$.

(1) A *fractional ideal of* R is a finitely generated R-submodule I of K such that $I \neq 0$.
(2) For a fractional I of R, set
$$I^{-1} = \{a \in K \mid aI \subset R\}.$$
Then, I is called *invertible* if $I^{-1}I = R$.

The name "fractional ideal" is justified by the following observation: For any fractional ideal I, there exists some $x \in R$ such that $xI \subset R$. Indeed, if I generated by $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ with $a_i, b_i \in R$, $b_i \neq 0$, then we can take $x := b_1 \cdot \ldots \cdot b_n$. In fact, we have $I = x^{-1}\mathfrak{a}$ where $\mathfrak{a} = xI$ is an ideal in R.

Example 2.16. Let R be a discrete valuation ring and $\pi \in R$ a uniformizer. Then, the fractional ideals are $\pi^n R$ for $n \in \mathbb{Z}$. One has $(\pi^n R)^{-1} = \pi^{-n} R$ and every fractional ideal is invertible.

Exercise 2.17. Let I be an invertible fractional ideal of a noetherian domain R. Then, I is projective and of rank 1.

Theorem 2.18. *Let R domain. Then, the following are equivalent:*
(1) The ring R is a Dedekind domain.
(2) The ring R is noetherian, normal and of dimension ≤ 1.
(3) Every fractional ideal is invertible.
(4) Every non-zero ideal of R is a finite product of maximal ideals.
Moreover, the factorization in (4) is unique up to order.

We only use and prove the following impliciations

$$(1) \iff (2) \implies (3) \;\&\; (1) \implies (4) + \text{ uniqueness} \tag{2.1}$$

For the other implications, the reader is referred to [Mat80, Theorem 11.6].

Proof of (1) $\iff$ (2) $\implies$ (3). (1) $\iff$ (2): Since a domain of dimension 0 is field, we may assume $\dim(R) = 1$. Then, we can replace R by $R_{\mathfrak{m}}$ for a maximal ideal $\mathfrak{m}$ (being normal can be tested on localizations by Reminder 2.7(1)). In this case, the equivalence of (1) and (2) follows from Theorem 2.8.

(2) $\implies$ (3): Let $I \subset R$ be a fractional ideal. Then, $I^{-1}I \subset R$ by definition and equality can be checked after localization. So, we may assume R to be either a field or a discrete valuation ring, where the equality is clear. □

To prove "(1) $\implies$ (4) + uniqueness", the following definition is useful:

Definition 2.19. Let R be a Dedekind domain, $K := \mathrm{Frac}(R)$ and $\mathfrak{p} \neq 0$ a prime ideal.

(1) The $\mathfrak{p}$-*adic valuation* $v_{\mathfrak{p}}$ *on* K is the normalized valuation defined by the discrete valuation ring $R_{\mathfrak{p}}$.
(2) For a fractional ideal I on R, one defines
$$v_{\mathfrak{p}}(I) := v_{\mathfrak{p}}(x_{\mathfrak{p}}) \in \mathbb{Z},$$
where $I_{\mathfrak{p}} = x_{\mathfrak{p}} R_{\mathfrak{p}}$ for some $x_{\mathfrak{p}} \in K^{\times}$.

Proposition 2.20. *Let R be a Dedekind domain . Then, for fractional ideals I, J and prime ideals $\mathfrak{p} \neq 0$ in R, the following hold:*
(1) $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$

(2) $v_{\mathfrak{p}}(I+J) \geq \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$
(3) $v_{\mathfrak{p}}(xR) = v_{\mathfrak{p}}(x)$ *for all* $x \in K^\times$

In addition, one has $v_{\mathfrak{p}}(I) \neq 0$ *for only finitely many prime ideals* $\mathfrak{p} \neq 0$ *in* R.

Proof. Parts (1), (2) and (3) are left to the reader. For the final statement, write $I = x^{-1}\mathfrak{a}$ for some $x \in R$ and some ideal $\mathfrak{a} \subset R$. Using (1) and (3), we may assume that I is an ideal in R. The proposition follows from Lemma 2.21 below. □

Lemma 2.21. *Let* R *be a Dedekind domain, and* $0 \neq \mathfrak{a} \subset R$ *an ideal. Then, there exist only finitely many prime ideals containing* $\mathfrak{a}$.

Proof. The map $I \mapsto I^{-1}$ induces a bijection

$$\{I \subset R \text{ ideal} \mid \mathfrak{a} \subset R\} \xrightarrow{1:1} \{I \text{ fractional ideal of } R \mid R \subset I \subset \mathfrak{a}^{-1}\}.$$

Since $\mathfrak{a}^{-1}$ is a noetherian R-module and the bijection reverses inclusions, every *descending* chain of ideals of R containing $\mathfrak{a}$ becomes stationary. Now assume $\mathfrak{a} \subset \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ for pairwise distinct prime ideals $0 \neq \mathfrak{p}_i \subset R$. Then, the sequence

$$\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdot \mathfrak{p}_2 \supset \ldots \supset \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \supset \ldots$$

becomes stationary, i.e., for $r \gg 0$ we have $\mathfrak{p}_{r+1} \supset \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$. Since all $\mathfrak{p}_i$ are prime ideals, there exists some $j \in \{1, \ldots, r\}$ such that $\mathfrak{p}_j \subset \mathfrak{p}_{r+1}$. As $\dim(R) = 1$ and both ideals are $\neq 0$, they must be maximal and hence, $\mathfrak{p}_j = \mathfrak{p}_{r+1}$ ↯. □

The next result finishes the proof of (2.1). It is a generalization of the fundamental theorem of arithmetic (i.e., every number can be written as a product of prime numbers) to Dedekind domains:

Corollary 2.22. *Let* R *be a Dedekind domain. Every fractional* I *of* R *can be written uniquely in the form*

$$I = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$$

where the product runs over non-zero prime ideals in R.

Proof. First off, the product is finite by Proposition 2.20. So, $I' := \prod_{\mathfrak{p}\neq 0} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ is a well-defined fractional ideal. Since $I_{\mathfrak{p}} = I'_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subset R$ by construction, we have $I = I'$. (Hint: $(I + I')/I$ is an R-module all whose localizations are zero, so it is zero [Sta18, 00HN].) □

Appendix A. Commutative algebra

The amount of commutative algebra used during the lectures roughly corresponds to [AM69, Chapters 1–3], which some readers might know from past lectures or past seminars in algebra. The author highly recommends reading these chapters. Here we collect some important properties, but do not give full details or references:

A great source to look up specific definitions, properties and proofs is also the Stacks Project [Sta18] - just google some keywords and add the words "stacks project". Further results from commutative algebra will be discussed during the lectures whenever needed.

A.1. **Spectrum of a ring.** All rings are assumed to be unital and commutative. Let A be a ring. Recall that an ideal $\mathfrak{p} \subset A$ is called *prime* if $A/\mathfrak{p}$ is a domain, i.e., $\mathfrak{p} \neq A$ and if $a, b \in A$ with $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both). An ideal $\mathfrak{m} \subset A$ is called *maximal* if $A/\mathfrak{m}$ is a field ($\implies$ $\mathfrak{m}$ is prime), i.e., $\mathfrak{m} \neq A$ and for any ideal I in A containing $\mathfrak{m}$ one has $I = \mathfrak{m}$ or $I = A$. Recall that every ring $A \neq 0$ has a maximal ideal, and that A is called *local* if it has exactly one maximal ideal.

Definition A.1. The spectrum of A is the set

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subset A \text{ prime ideal}\}.$$

By the discussion above, $\mathrm{Spec}(A)$ is empty if and only if A is the zero ring.

Exercise A.2. Show the following statements:

(1) Let $\varphi\colon A \to B$ be a ring homomorphism. Then, taking the preimage $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$ induces a map of sets $\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$.
(2) Let A be a ring and I an ideal in A. Then, the map $\varphi\colon A \to A/I, a \mapsto a \mod I$ induces an injection

$$\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(A/I) \hookrightarrow \mathrm{Spec}(A),$$

whose image consists of all prime ideals $\mathfrak{p} \subset A$ that contain I.

For every $\mathfrak{p} \in \mathrm{Spec}(A)$, the localization $A_\mathfrak{p} := A[(A\backslash\mathfrak{p})^{-1}]$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. It is called the *local ring of A at $\mathfrak{p}$*.

Exercise A.3. Show that the map $A \to A_\mathfrak{p}, a \mapsto \frac{a}{1}$ induces an injection $\mathrm{Spec}(A_\mathfrak{p}) \hookrightarrow \mathrm{Spec}(A)$ with image the prime ideals $\mathfrak{p}' \subset A$ with $\mathfrak{p}' \subset \mathfrak{p}$.

Definition A.4. The field

$$\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = \mathrm{Frac}(A/\mathfrak{p})$$

is called the *residue field of A at $\mathfrak{p}$*.

This allows to establish a (very rough) dictionary

$$\text{(elements of } A) \;\leftrightarrow\; \text{(functions on } \mathrm{Spec}(A)) \tag{A.1}$$

as follows: For an element $f \in A$ and some $\mathfrak{p} \in \mathrm{Spec}(A)$, we denote by

$$f(\mathfrak{p}) := f \mod \mathfrak{p} \in \kappa(\mathfrak{p})$$

the *value of f at $\mathfrak{p}$*. Note that the residue fields $\kappa(\mathfrak{p})$ for varying $\mathfrak{p}$ are not isomorphic, so the definition comes at the expense of allowing the "target of the function" to vary. Making (A.1) precise is the content of Algebraic Geometry. Here we only point out the following property:

Exercise A.5. Let A be a ring and $f \in A$. Show that $f \in A^\times$ if and only if $f(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$. (Hint: Consider $\mathrm{Spec}(A/fA)$.)

Example A.6. One has $\mathrm{Spec}(\mathbb{Z}) = \{(p) \mid p \text{ prime number}\} \cup \{(0)\}$. The localizations at (p) and (0) are $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ and $\mathbb{Q}$ respectively. The residue fields are $\mathbb{F}_p$ and $\mathbb{Q}$ respectively.

Exercise A.7. Let k be a field and denote by $k[T]$ the polynomial ring in an indeterminate T. Describe the spectrum, the localizations and the residue fields for analogously as in Example A.6 for $k[T]$. Also, study how this simplifies if k is algebraically closed. (Hint: Use that $k[T]$ is a principal ideal domain.)

For an A-module M and $\mathfrak{p} \in \mathrm{Spec}(A)$, we extend the above notation by defining $M_\mathfrak{p} := M[(A\backslash\mathfrak{p})^{-1}]$ to be the localization of M at the multiplicative subset $A\backslash\mathfrak{p}$.

Definition A.8. The support of an A-module M is the set

$$\mathrm{supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid M_\mathfrak{p} \neq 0\}.$$

Example A.9. Let $n \in \mathbb{Z}$, $n \neq 0$. Then, we have

$$\mathrm{supp}(\mathbb{Z}/n\mathbb{Z}) = \{(p) \mid p \text{ prime number dividing } n\}.$$

A.2. **Radical of ideals.** Let A be a ring.

Definition A.10. For an ideal $I \subset A$, the set

$$\sqrt{I} = \{a \in A \mid \exists n \geq 1 : a^n \in I\}$$

is called the *radical of* I. The radical of $I = (0)$ is also called the *Nilradical of* A.

We leave it to the reader to check that $\sqrt{I}$ defines an ideal in A. One always has $I \subset \sqrt{I}$ with equality if and only if 0 is the only nilpotent element in A/I. However, if $I = \mathfrak{p}$ is a prime ideal, then $\sqrt{\mathfrak{p}} = \mathfrak{p}$.

Exercise A.11. Show the following statements:

(1) Let A be a principal ideal domain and $a \in A$ non-zero. Let $a = u \cdot p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ with $r \in \mathbb{Z}_{\geq 0}$, $u \in A^\times$, p_i pairwise non-associated prime elements in A and $e_i \in \mathbb{Z}_{\geq 1}$ for $i = 1, \ldots, r$. Then, one has $\sqrt{(a)} = (p_1 \cdot \ldots \cdot p_r)$.
(2) Let A be a Noetherian ring and I an ideal in A. Then, there exists some $m \in \mathbb{Z}_{\geq 1}$ such that $(\sqrt{I})^m \subset I$.

Proposition A.12. *Let A be a ring and I an ideal in A. Then, one has*

$$\sqrt{I} = \bigcap_{I \subset \mathfrak{p}} \mathfrak{p}, \tag{A.2}$$

where the intersection runs over all prime ideals $\mathfrak{p} \subset A$ that contain I. In particular, one has

$$\sqrt{0} = \bigcap_{\mathfrak{p}} \mathfrak{p}, \tag{A.3}$$

where the intersection runs over all prime ideals $\mathfrak{p} \subset A$.

Proof. Taking the preimage of subsets along the map $A \to A/I, a \mapsto a \mod I$ induces a bijection between prime ideals in A/I and prime ideals in A that contain I, see Exercise A.2(2). So, replacing A by A/I it suffices to prove (A.3). We leave the inclusion "$\subset$" to the reader and prove "$\supset$". Let $x \in A$ be not nilpotent. We need to show that there exists a prime ideal $\mathfrak{p} \subset A$ with $x \notin \mathfrak{p}$. Set $\Sigma := \{\mathfrak{a} \subset A \text{ ideal} \mid \forall n \in \mathbb{N} : x^n \notin \mathfrak{a}\}$. Since x is not nilpotent, we have $(0) \in \Sigma$ and so $\Sigma \neq \varnothing$. We define a partial order on Σ by the inclusion of ideals. One checks that every chain has an upper bound given by the set theoretic union (check that this is an ideal). By Zorn's lemma, Σ has a maximal element $\mathfrak{p}$. We claim that $\mathfrak{p}$ is a prime ideal. Let $f, g \in A\backslash\mathfrak{p}$. Then, $(f) + \mathfrak{p}, (g) + \mathfrak{p} \notin \Sigma$ by maximality of $\mathfrak{p}$. So,

there exists $m, n \in \mathbb{N}$ with $x^m \in (f) + \mathfrak{p}$ and $x^n \in (g) + \mathfrak{p}$, hence $x^{n+m} \in (fg) + \mathfrak{p}$. This shows that $(fg) + \mathfrak{p} \notin \Sigma$, i.e., $fg \notin \mathfrak{p}$. □

Corollary A.13. *Let A be a ring and $I \subset A$ be an ideal. Then, the map $A/I \to A/\sqrt{I}, a \mod I \mapsto a \mod \sqrt{I}$ induces a bijection*

$$\operatorname{Spec}(A/\sqrt{I}) \xrightarrow{1:1} \operatorname{Spec}(A/I).$$

Proof. This follows from A.2 and Exercise A.2(2). □

A.3. **Cayley–Hamilton.** Let A be a ring. Let $u\colon M \to N$ be a map of A-modules. Assume that M, N are finitely generated. Let $(m_1, \dots, m_r)$ and $(n_1, \dots, n_s)$ be systems of generators for M and N respectively. Then, for all $j = 1, \dots, r$, there exist $t_{1j}, \dots, t_{sj} \in A$ such that

$$u(m_j) = \sum_{i=1}^{s} t_{ij} n_i. \tag{A.4}$$

This defines a matrix $T = (t_{ij}) \in \operatorname{Mat}_{s\times r}(A)$.

Remark A.14.
(1) The matrix T is not uniquely determined by u, only if $(n_1, \dots, n_s)$ is a basis of N.
(2) Not every matrix in $\operatorname{Mat}_{s\times r}(A)$ defines a linear map u by (A.4), only if $(m_1, \dots, m_r)$ is a basis of M.

Theorem A.15 (Cayley–Hamilton)**.** *Let M be a finitely generated A-module with generators $(m_1, \dots, m_r)$. Let $u\colon M \to M$ be an A-linear map and $T \in \operatorname{Mat}_{r\times r}(A)$ the matrix of u with respect to $(m_1, \dots, m_r)$. Denote by $\chi_T := \det(XI_r - T) \in A[X]$ the characteristic polynomial of T, and write*

$$\chi_T = X^r + a_1 X^{r-1} + \ldots + a_{r-1} X + a_r.$$

Then, one has

$$\chi_T(u) = u^r + a_1 u^{r-1} + \ldots + a_{r-1} u + a_r I_r = 0 \in \operatorname{End}_A(M).$$

Moreover, if $I \subset A$ is an ideal with $u(M) \subset IM$, then one can choose T such that $a_i \in I^i$ for all $i = 1, \dots, r$.

Remark A.16. It is also possible to give a proof by reduction to the case where A is a field, see [Sta18, 05G6]. Here we give a direct proof.

Reminder A.17. Let $r \in \mathbb{N}$, $T \in \operatorname{Mat}_{r\times r}(A)$. Then, there exists $S \in \operatorname{Mat}_{r\times r}(A)$ with

$$ST = TS = \det(T) I_r,$$

where $I_r \in \operatorname{Mat}_{r\times r}(A)$ denotes the identity matrix. Namely, take $S = (s_{ij})$ with $s_{ij} = \det(T_{ji})$ where $T_{ji} \in \operatorname{Mat}_{(r-1)\times(r-1)}(A)$ arises from T by deleting the j-th row and the i-th column. The matrix S is called the *adjoint* of T.

Proof of Theorem A.15. If $u(M) \subset IM$, then we can choose the entries of T in (A.4) to lie in I. Since a_i is a sum of i-fold products of the entries, it is contained in I^i.

Next, let us write ${}^tT = (t_{ij})$ for the transposed of T. So, we have $u(m_j) = \sum_{i=1}^{r} t_{ji} m_i$ and thus

$$\sum_{i=1}^{r} (u\delta_{ji} - t_{ji}) m_i = 0. \tag{A.5}$$

Consider the matrix $C(X) := (X\delta_{ji} - t_{ji}) = XI_r - {}^tT \in \mathrm{Mat}_{r\times r}(A[X])$. Let $D(X) = (d_{kj}(X))$ be the adjoint of C, hence

$$D(X)C(X) = \chi_T(X)I_r \tag{A.6}$$

using that $\chi_T = \chi_{{}^tT}$. The map $f \mapsto f(u)$ induces a homomorphism of commutative A-algebras

$$A[X] \to A[u] := \{f(u) \in \mathrm{End}_A(M) \mid f \in A[X]\}.$$

Thus, we get $C(u), D(u) \in \mathrm{Mat}_{r\times r}(A[u])$. Multiplying (A.5) with $d_{kj}(u)$ and applying $\sum_j$ gives

$$0 = \sum_i \sum_j d_{kj}(u)(u\delta_{ji} - t_{ji})m_i = \chi_T(u)m_k$$

for all $k = 1, \ldots, r$ by using (A.6) for the second equality. Since the m_k generate M, this shows $\chi_T(u) = 0 \in \mathrm{End}_A(M)$. □

Corollary A.18. *Let A be a ring and M a finitely generated A-module. Let $I \subset A$ be an ideal such that $M = IM$. Then, there exists some $f \in 1 + I$ with $fM = 0$.*

Proof. Apply Theorem A.15 to $u = \mathrm{id}_M$ to get $f \cdot \mathrm{id}_M = 0$ with $f := 1 + a_1 + \ldots + a_r$ and $a_i \in I^i \subset I$. This shows $fM = 0$. □

Exercise A.19. Let A be a ring and M a finitely generated A-module. Let $u\colon M \to M$ be an A-linear endomorphism. Assume that u is surjective. Show that u is an isomorphism. (Hint: Consider M as an $A[X]$-module via $X \cdot m := u(m)$ for all $m \in M$.)

Is every injective endomorphism of a finitely generated module an automorphism?

A.4. **Nakayama's lemma.**

Definition A.20. Let A be a ring. Then, the ideal

$$\mathrm{Jac}(A) = \bigcap_{\mathfrak{m} \subset A \text{ maximal ideal}} \mathfrak{m}$$

is called the *Jacobson radical of A*.

Proposition A.21. *Let A be a ring and I be an ideal in A. Then, one has $I \subset \mathrm{Jac}(A)$ if and only if $1 + I \subset A^\times$.*

Proof. First, let $I \subset \mathrm{Jac}(A)$. We argue by contraction. So, assume there exists an $x \in I$ such that $1 + x \notin A^\times$. Then, $A/(1 + x) \neq 0$ and there exists a maximal ideal $\mathfrak{m} \subset A$ with $1 + x \in \mathfrak{m}$. Since $x \in \mathrm{Jac}(A) \subset \mathfrak{m}$, it follows $1 \in \mathfrak{m}$ ↯.

Conversely, let $1 + I \subset A^\times$. Assume $I \not\subset \mathrm{Jac}(A)$. Then, there exists $x \in I$ and a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. Thus, $(x) + \mathfrak{m} = A$, i.e., there exists $y \in A$, $v \in \mathfrak{m}$ such that $xy + v = 1$. This implies $1 + (-xy) \in \mathfrak{m}$ and $-xy \in I$, so $1 + I \not\subset A^\times$ ↯. □

Exercise A.22. Let A be a ring and I an ideal in A with $I \subset \mathrm{Jac}(A)$. Consider the map $\varphi\colon A \to A/I, a \mapsto a \mod I$. Show that an element $a \in A$ is a unit if and only if $\varphi(a)$ is a unit in A/I. Deduce that for a local ring A with maximal ideal $\mathfrak{m}$ one has $A^\times = A \backslash \mathfrak{m}$.

Exercise A.23. Let $\varphi\colon A \to B$ be a ring map such that the induced map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective. Then, an element $f \in A$ is a unit if and only if $\varphi(f) \in B$ is a unit. (Hint: Use Exercise A.23.)

Lemma A.24 (Nakayama's lemma)**.** *Let A be a ring and $u\colon N \to M$ be a map of A-modules. Let $I \subset A$ be an ideal with $I \subset \mathrm{Jac}(A)$. Assume that M is finitely generated. Then, the map $u\colon N \to M$ is surjective if and only if the induced map*

$$\bar{u}\colon N/IN \to M/IM, \quad n \mod IN \mapsto u(n) \mod IM$$

is surjective.

Proof. If u is surjective, so is $\bar{u}$ as one checks readily (without assuming that M is finitely generated). Conversely, assume that $\bar{u}$ is surjective. Then, one has

$$0 = \mathrm{coker}(\bar{u}) = \mathrm{coker}(u)/I\mathrm{coker}(u),$$

i.e., $\mathrm{coker}(u) = I\mathrm{coker}(u)$. Since M is finitely generated, so is $\mathrm{coker}(u)$. Hence, Corollary A.18 shows that $f \cdot \mathrm{coker}(u) = 0$ for some $f \in 1 + I$. Since $1 + I \subset A^\times$ by Proposition A.21, the element f is invertible and we get $\mathrm{coker}(u) = 0$, i.e., u is surjective. □

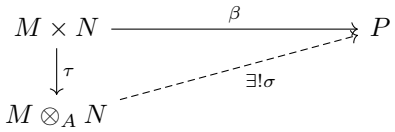
Exercise A.25. Let A be a ring and M a finitely generated A-module. Let I be an ideal in A with $I \subset \mathrm{Jac}(A)$. If $M = IM$, then $M = 0$.

Corollary A.26. *For every finitely generated A-module and prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, one has $M_\mathfrak{p} = 0$ if and only if $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} = 0$.*

Proof. This follows from Exercise A.25 applied to the finitely generated module $M_\mathfrak{p}$ over the local ring $A_\mathfrak{p}$ and its Jacobson radical $I = \mathfrak{p}A_\mathfrak{p}$. □

A.5. **Tensor products.** Let A be a ring and M, N, P be A-modules. Recall that a map $\beta\colon M \times N \to P$ is called *A-bilinear* if for all $m \in M$, $n \in N$ the maps $\beta(m, -)$ and $\beta(-, n)$ are A-linear.

Definition A.27. Let M, N be A-modules. A *tensor product of M and N* is an A-module $M \otimes_A N$ together with a A-bilinear map $\tau\colon M \times N \to M \otimes_A N, (m, n) \mapsto m \otimes n$ such that the following universal property holds: For every A-module P and every A-bilinear map $\beta\colon M \times N \to P$ there exists a unique map $\sigma\colon M \otimes_A N \to P$ such that $\beta = \sigma \circ \tau$, i.e., the following diagram commutes:



Properties A.28. *For the following basic properties, the reader is referred to* [AM69, Proposition 2.12ff.]*:*

(1) The pair $(M \otimes_A N, \tau)$ exists and is unique up to unique isomorphism. One puts

$$M \otimes_A N := \mathrm{Free}_A\{m \otimes n \mid m \in M, n \in N\}/\mathrm{Span}_A\{(3a)\text{–}(3c)\},$$

where $m \otimes n$ are formal symbols, $\mathrm{Free}_A\{-\}$ is the free A-module generated on these symbols and $\mathrm{Span}_A\{-\}$ denotes its submodule generated by the relations (3a)–(3c) below. The map $\tau\colon M \times N \to M \otimes_A N, (m, n) \mapsto m \otimes n$ is given by $\tau(m, n) = m \otimes n$.

(2) If $(m_i)_{i \in I}$ and $(n_j)_{j \in J}$ is a generating system of M and N respectively, then $(m_i \otimes n_j)_{i \in I, j \in J}$ is a generating system of $M \otimes_A N$. Note that an arbitrary element in $M \otimes_A N$ is a finite sum of the form $\sum_{i,j} a_{ij} m_i \otimes n_j$ for some $a_{ij} \in A$.

(3) *The bilinearity of τ means that for all $m, m' \in M$, $n, n' \in N$ and $a \in A$:*
   (a) $(m + m') \otimes n = m \otimes n + m' \otimes n$
   (b) $m \otimes (n + n') = m \otimes n + m \otimes n'$
   (c) $(am) \otimes n = a(m \otimes n) = m \otimes (an)$

Lemma A.29. *Let $u\colon M \to M'$ and $v\colon N \to N'$ be maps of A-modules. Then, there exists a unique map of A-modules*

$$u \otimes v\colon M \otimes_A N \to M' \otimes_A N'$$

with $(u \otimes v)(m \otimes n) = u(m) \otimes v(n)$ for all $m \in M$, $n \in N$.

Proof. Consider the following diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{u \times v} & M' \times N' \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} \\ M \otimes_A N & \xrightarrow{\exists! u \otimes v} & M' \otimes_A N' \end{array}$$

Since the composition $\tau \circ (u \times v)$ is A-bilinear, we get the existence of a unique map $u \otimes v$ as indicated. □

Lemma A.30. *Let M, N, P be A-modules.*

(1) *There exists a unique isomorphism*

$$(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$$

such that $(m \otimes n) \otimes p \mapsto m \otimes (n \otimes p)$ for all $m \in M$, $n \in N$, $p \in P$.

(2) *There exists a unique isomorphism*

$$M \otimes_A N \cong N \otimes_A M$$

such that $m \otimes n \mapsto n \otimes m$ for all $m \in M$, $n \in N$.

(3) *One has $M \otimes_A A \cong M$ given by $m \otimes a \mapsto am$ for all $m \in M$, $a \in A$.*

Proof. (1): This is left to the reader.

(2): We consider the following diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow[\cong]{\varphi\colon (m,n) \mapsto (n,m)} & N \times M \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} \\ M \otimes_A N & \underset{\exists! \rho}{\overset{\exists! \sigma}{\rightleftarrows}} & N \otimes_A M \end{array}$$

Since $\tau' \circ \varphi$ and $\tau \circ \varphi^{-1}$ are A-bilinear, there exist unique maps σ and ρ respectively. One necessarily has $\rho \circ \sigma = \mathrm{id}$ and $\sigma \circ \rho = \mathrm{id}$.

(3): The inverse map is given by $m \mapsto m \otimes 1$. □

Remark A.31. The functor $(-) \otimes_A N$ is left adjoint to the functor $\mathrm{Hom}_A(N, -)$, both viewed as endofunctors on the category of A-modules. More precisely, for all A-modules M, N, P, there are bijections

$$\begin{array}{ccc} \mathrm{Hom}_A(M \otimes_A N, P) & \overset{u \mapsto u \circ \tau}{=} & \{\beta\colon M \times N \to P \ A\text{-bilinear maps}\} \\ & & \overset{\beta \mapsto \left(m \mapsto (n \mapsto \beta(m,n))\right)}{=} \\ & & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \end{array} \tag{A.7}$$

that are functorial in M, N and P. Functorial in N means that a map $v\colon N \to N'$ of A-modules induces a diagram

$$\begin{array}{ccc} \mathrm{Hom}_A(M \otimes_A N, P) & \xrightarrow[(\text{A.7})]{\cong} & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \\ {\scriptstyle u' \mapsto u' \circ (\mathrm{id}_M \otimes v)}\uparrow & & \uparrow{\scriptstyle w \mapsto (m \mapsto w(m) \circ v)} \\ \mathrm{Hom}_A(M \otimes_A N', P) & \xrightarrow[(\text{A.7})]{\cong} & \mathrm{Hom}_A(M, \mathrm{Hom}_A(N', P)) \end{array}$$

that commutes as one verifies. We leave it to the reader to spell out the functoriality in M and P, which requires writing down similar diagram and checking their commutativity.

Corollary A.32. *Let N be an A-module. Then, the functor $(-) \otimes_A N\colon \mathrm{Mod}_A \to \mathrm{Mod}_A$ commutes with colimits. In particular, the following hold:*

(1) If $(M_i)_{i \in I}$ is a family of A-modules, then the canonical map

$$\Big(\bigoplus_{i \in I} M_i\Big) \otimes_A N \xrightarrow{\cong} \bigoplus_{i \in I} (M_i \otimes_A N)$$

is an isomorphism. In other words, the functor $(-) \otimes_A N$ commutes with direct sums (=coproducts in Mod_A).

(2) If $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ is an exact sequence of A-modules, then the sequence

$$M' \otimes_A N \xrightarrow{u \otimes \mathrm{id}_N} M \otimes_A N \xrightarrow{v \otimes \mathrm{id}_N} M'' \otimes_A N \longrightarrow 0$$

is exact. In other words, the functor $(-) \otimes_A N$ commutes with finite colimits (and Mod_A is an abelian category).

Proof. This follows from Remark A.31 because left adjoint functors commute with colimits (and the category of A-modules admits all colimits). □

Example A.33. For $0 \neq n \in \mathbb{Z}$, we consider the exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

Tensoring with $(-) \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ induces the sequence

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{n=0} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

In particular, we see that tensoring does not preserve injective maps in general, i.e., if $u\colon M \to M'$ is injective, then $u \otimes \mathrm{id}_N\colon M \otimes_A N \to M' \otimes_A N$ is not injective in general.

Exercise A.34. Show the following statements:

(1) Let $u\colon M \to M'$, $v\colon N \to N'$ be surjective maps of A-modules. Then, the map $u \otimes v\colon M \otimes_A N \to M' \otimes_A N'$ is surjective with kernel

$$\ker(u \otimes v) = \mathrm{Span}_A\{m \otimes n \mid m \in \ker(u) \text{ or } n \in \ker(v)\},$$

where $\mathrm{Span}_A\{-\}$ denotes the A-submodule generated by $(-)$. Deduce that for an ideal $I \subset A$ one has $M \otimes_A A/I = M/IM$.

(2) Let I, J be ideals in a ring A. Then, there is a canonical isomorphism

$$A/I \otimes_A A/J \cong A/(I + J).$$

Deduce that for $m, n \in \mathbb{Z}$ one has $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$ if and only if m, n are prime to each other. Note that this is equivalent to $\operatorname{supp}(\mathbb{Z}/m\mathbb{Z}) \cap \operatorname{supp}(\mathbb{Z}/n\mathbb{Z}) = \varnothing$, see Example A.9.

Reminder A.35. Let M be an A-module. Then, M is called

(1) *free* if $M \cong \oplus_{i \in I} A =: A^{(I)}$ for some set I. In this case, the cardinality $\operatorname{rank}_A(M) := \#I$ depends only on I and is called the *rank of* M.
(2) *projective* if M is a direct summand of a free A-module, i.e., there exists a free A-module E such that $M \oplus N \simeq E$ for some A-module N. Equivalently, for every short exact sequence of A-modules

$$0 \longrightarrow K \xrightarrow{i} N \xrightarrow{p} M \longrightarrow 0$$

there exists $s\colon M \to N$ such that $p \circ s = \mathrm{id}_M$. In this case, $K \oplus M \simeq N, (k, m) \mapsto i(k) + s(m)$.

Exercise A.36. Let M, N be A-modules. Show the following properties:

(1) If M is free of rank r and N is free of rank s, then $M \otimes_A N$ is free of rank rs.
(2) If M, N are projective, then so is $M \otimes_A N$.
(3) If M, N are finitely generated, then so is $M \otimes_A N$. (Hint: An A-module M is finitely generated if and if there exists a surjection $A^r \to M$ for some $r \in \mathbb{N}$.)

A.6. **Base change.** Let $\rho\colon A \to B$ be a map of rings. We also say that B is a (commutative) *A-algebra with structure map ρ*. If ρ is understood, then we simply say that B is an *A-algebra*. Equivalently, B is an A-module together with an A-bilinear, commutative, unital map $B \times B \to B$.

Remark A.37. The base change of an module or algebra is defined as follows:

(1) Let M be an A-module. Then, $B \otimes_A M$ becomes a B-module by scalar multiplication on the first factor:

$$B \times (B \otimes_A M) \to B \otimes_A M,$$
$$(b, b' \otimes m) \mapsto bb' \otimes m$$

(2) Let C be an A-algebra. Then, $B \otimes_A C$ becomes a B-algebra with multiplication

$$B \otimes_A C \times B \otimes_A C \to B \otimes_A C,$$
$$(b_1 \otimes c_1, b_2 \otimes c_2) \mapsto b_1 b_1 \otimes c_1 c_2$$

and structure map $B \to B \otimes_A C, b \mapsto b \otimes 1$. Note that the situation is symmetric in B and C, i.e., $B \otimes_A C$ is also a C-algebra.

We call $B \otimes_A M$ and $B \otimes_A C$ the *base change* of the A-module M and the A-algebra C respectively.

Properties A.38. *Let $\rho\colon A \to B$ be a ring map. The following are important:*

(1) The map

$$B \otimes_A A[T_1, \ldots, T_n] \xrightarrow{\cong} B[T_1, \ldots, T_n]$$
$$b \otimes \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} T_1^{i_1} \cdots T_n^{i_n} \mapsto \sum_{i_1, \ldots, i_n \geq 0} b\rho(a_{i_1 \ldots i_n}) T_1^{i_1} \cdots T_n^{i_n}$$

is an isomorphism of B-algebras for all $n \in \mathbb{N}$. An analogous statement holds for polynomial rings in infinitely many variables.

(2) *Let I be an ideal in A and consider the projection $A \to A/I, a \mapsto a \mod I$. Then, the map $B = B \otimes_A A \to B \otimes_A A/I$ induces an isomorphism of B-algebras*

$$B/IB \cong B \otimes_A A/I,$$

where IB is the ideal in B generated by $\rho(I)$.

Properties A.38 (1) and (2) allow for a description in the general case: Let C be an A-algebra. Choose generators $(c_\lambda)_{\lambda\in\Lambda}$ of C as an A-algebra. We get a surjective homomorphisms of A-algebra

$$\pi\colon A[(T_\lambda)_{\lambda\in\Lambda}] \to C, \quad T_\lambda \mapsto c_\lambda.$$

Set $I := \ker(\pi)$, so $C \cong A[(T_\lambda)_{\lambda\in\Lambda}]/I$. Then, we compute:

$$\begin{aligned} B \otimes_A C &\cong \big(B \otimes_A A[(T_\lambda)_{\lambda\in\Lambda}]\big) \otimes_{A[(T_\lambda)_{\lambda\in\Lambda}]} A[(T_\lambda)_{\lambda\in\Lambda}]/I \\ &\overset{(1)}{\cong} B[(T_\lambda)_{\lambda\in\Lambda}] \otimes_{A[(T_\lambda)_{\lambda\in\Lambda}]} A[(T_\lambda)_{\lambda\in\Lambda}]/I \\ &\overset{(2)}{\cong} B[(T_\lambda)_{\lambda\in\Lambda}]/IB[(T_\lambda)_{\lambda\in\Lambda}] \end{aligned}$$

Example A.39. Let $\rho\colon A \to B$ be a ring map. Let $C := A[T_1, \dots, T_n]/(f_1, \dots, f_r)$ for some $n \in \mathbb{N}$ and $f_1, \dots, f_r \in A[T_1, \dots, T_n]$. Then, we have

$$B \otimes_A C \cong B[T_1, \dots, T_n]/(\rho(f_1), \dots, \rho(f_r)),$$

where for $f = \sum_{i_1,\dots,i_n \geq 0} a_{i_1\dots i_n} T_1^{i_1} \cdots T_n^{i_n} \in A[T_1, \dots, T_n]$ we write

$$\rho(f) := \sum_{i_1,\dots,i_n \geq 0} \rho(a_{i_1\dots i_n}) T_1^{i_1} \cdots T_n^{i_n} \in B[T_1, \dots, T_n].$$

As concrete examples, we consider the following special cases:

(1) Let $\rho\colon A := \mathbb{Z} \to \mathbb{F}_p =: B$ and $C := \mathbb{Z}[i]$. Then, $\mathbb{Z}[T]/(T^2+1) \cong \mathbb{Z}[i], T \mapsto i$ induces an isomorphism of $\mathbb{F}_p$-algebras

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

compare also the computation (1.3) in the proof of Lemma 1.9.

(2) Let $\rho\colon A := \mathbb{R} \to \mathbb{C} =: B$ and $C := \mathbb{C} = \mathbb{R}[i] = \mathbb{R}[T]/(T^2+1)$. Then,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[T]/(T^2+1) = \mathbb{C}[T]/(T+i) \times \mathbb{C}[T]/(T-i) \cong \mathbb{C} \times \mathbb{C},$$

where we use the Chinese remainder theorem for the 2nd identification.

Exercise A.40. Let $d \in \mathbb{Z}$ be not a square. Show the following properties:

(1) One has $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{d}] \cong \mathbb{Q}[\sqrt{d}]$ as $\mathbb{Q}$-algebras.

(2) For any prime number p, one has an isomorphism of $\mathbb{F}_p$-algebras

$$\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{d}] \cong \mathbb{F}_p[T]/(T^2 - \bar{d}),$$

where $\bar{d} \equiv d \mod p$. Is this always a field?

The following lemma gives some permanence properties for the base change of modules:

Lemma A.41. *Let M be an A-module, B an A-algebra and κ some cardinal. If M is a free of rank κ (respectively finitely generated, respectively projective) A-module, then so is the B-module $B \otimes_A M$.*

Proof. First, assume $M \cong A^{(I)} := \oplus_{i\in I} A$ for some set I with $\#I = \kappa$. Then, $B \otimes_A M = \oplus_{i\in I}(B \otimes_A A) = B^{(I)}$ by Corollary A.32(1) and Lemma A.30(3). Hence, $B \otimes_A M$ is free of rank κ.

Next, assume M is finitely generated and pick a surjection $A^r \to M$ for some $r \in \mathbb{N}$. Then, the induced map $B^r = B \otimes_A A^r \to B \otimes_A M$ is surjective as well by Corollary A.32(2). Hence, $B \otimes_A M$ is a finitely generated B-module.

Finally, assume M is projective and pick some free A-module E with $M \oplus N \cong E$ for some A-module N. Since direct sums commute with tensor products, one gets as A-modules

$$\big(B \otimes_A M\big) \oplus \big(B \otimes_A N\big) = B \otimes_A E$$

which is checked to be B-linear. As $B \otimes_A E$ is a free B-module, we see that $B \otimes_A M$ is projective. □

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. 11, 16

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, 1986. Reprint of the 1967 original. 1

[Eme21] Matthew Emerton. Langlands reciprocity: L-functions, automorphic forms, and Diophantine equations. In *The genesis of the Langlands Program*, volume 467 of *London Math. Soc. Lecture Note Ser.*, pages 301–386. Cambridge Univ. Press, Cambridge, 2021. 4

[GW10] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010. Schemes with examples and exercises.

[KKS00] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Number theory. 1*, volume 186 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 2000. Fermat's dream, Translated from the 1996 Japanese original by Masato Kuwata, Iwanami Series in Modern Mathematics. 1, 3, 4, 5

[KKS11] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Number theory. 2*, volume 240 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 2011. Introduction to class field theory, Translated from the 1998 Japanese original by Masato Kuwata and Katsumi Nomizu, Iwanami Series in Modern Mathematics. 1

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994. 1

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, MA, second edition, 1980. 10

[Mil] James Milne. Algebraic number theory. 1

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. 1

[Sta18] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018. 7, 8, 9, 11, 12, 14

[Zag81] D. B. Zagier. *Zetafunktionen und quadratische Körper*. Hochschultext. [University Textbooks]. Springer-Verlag, Berlin-New York, 1981. Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory]. 1