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 authors thank 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:

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. Since R is a unique factorization domain, 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 M, 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 $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module for all prime ideals $\mathfrak{p} \subset R$.

In this case, the number $\operatorname{rank}_{R_\mathfrak{p}}(M_\mathfrak{p})$ in (3) is independent of $\mathfrak{p}$ 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 $\mathfrak{p} \subset R$ if and only if $M_\mathfrak{m}$ is a torsion free $R_\mathfrak{m}$-module for all maximal ideals $\mathfrak{m} \subset R$.

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 $K := \mathrm{Frac}(R)$.

(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 Dedekind domain R. Then, I is a projective R-module and of rank 1.

Theorem 2.18. *Let R be a 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:

(2.1) $\qquad (1) \iff (2) \implies (3)$ and $(1) \implies (4) +$ uniqueness

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

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

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

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

becomes stationary, i.e, for $r \gg 0$ we have $\mathfrak{p}_{r+1} \supset \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r \supset \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$. 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].) □

2.3. **Fundamental exact sequence.**

Definition 2.23. Let R be a Dedekind domain. Then, the *divisor group of* R is the set

$$\mathrm{Div}(R) := \{I \text{ fractional ideal of } R\}.$$

Lemma 2.24. *Let* R *be a Dedekind domain. Then,* $\mathrm{Div}(R)$ *has the structure of an abelian group under multiplication. It is canonically isomorphic to the free abelian group with basis* $\{\mathfrak{p} \mid 0 \neq \mathfrak{p} \subset R \text{ prime ideal}\}$.

Proof. This follows from Theorem 2.18 and Corollary 2.22. □

Definition 2.25. Let R be a Dedekind domain with fraction field K.

(1) A fractional ideal $I \in \mathrm{Div}(R)$ is called *principal* if it is of the form xR for some $x \in K^\times$, i.e., if it lies in the image of the group homomorphism
$$\delta\colon K^\times \to \mathrm{Div}(R), x \mapsto xR.$$
Set $\mathrm{PrincDiv}(R) := \mathrm{Im}(\delta) \subset \mathrm{Div}(R)$ the subgroup of principal fractional ideals.
(2) The *(divisor) class group of* R is the quotient $\mathrm{Cl}(R) := \mathrm{Div}(R)/\mathrm{PrincDiv}(R)$, i.e., the cokernel of δ.

Exercise 2.26. For those who have attended the algebraic geometry lectures: Show that $\mathrm{Cl}(R)$ agrees with the Picard group of R.

Theorem 2.27. *Let R be a Dedekind domain with fraction field K. Then, the sequence*
$$1 \to R^\times \to K^\times \xrightarrow{\delta} \mathrm{Div}(R) \to \mathrm{Cl}(R) \to 0$$
is exact. It is called the fundamental exact sequence.

Proof. This follows from the definition. □

Proposition 2.28. *Let R be a Dedekind domain. Then, the following are equivalent:*

(1) One has $\mathrm{Cl}(R) = 0$.
(2) The ring R is a principal ideal domain.
(3) The ring R is a unique factorization domain.

Proof. (1) $\iff$ (2): This follows because every fractional ideal I is of the form $x\mathfrak{a}$ for some $x \in \mathrm{Frac}(R)^\times$ and some ideal $\mathfrak{a} \subset R$.
(2) $\implies$ (3): A fact from the algebra lectures during the past semesters.
(3) $\implies$ (2): See [Bourbaki, Comm. Alg., VII, §3.2, Theorem 1] for details. □

Example 2.29. We will see later that $R = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain. The ideal $\mathfrak{m} = (2, 1+\sqrt{-5})$ in R is maximal: indeed, under $X = \sqrt{-5}$ one has $R/\mathfrak{m} \cong \mathbb{Z}[X]/(X^2+5, 2, 1+X)$, which is the field with 2 elements. On the other hand $\mathfrak{m}$ is not principal: indeed, if $\mathfrak{m} = (a + \sqrt{-5}b)$ for some $a, b \in \mathbb{Z}$, then by taking norms (compare with the proof of Lemma 1.7) we get equalities of ideals in $\mathbb{Z}$:
$$2\mathbb{Z} = (2^2, 1^2+5)\mathbb{Z} = (a^2+5b^2)\mathbb{Z}$$
Since the equation $\pm 2 = a^2 + 5b^2$ has no solutions with $(a, b) \in \mathbb{Z}$, we get a contradiction and $\mathfrak{m}$ cannot be principal. Also, one computes $\mathfrak{m}^2 = 2\mathbb{Z}$. Hence, $\mathfrak{m}$ defines a non-trivial, 2-torsion element of $\mathrm{Cl}(R)$. In fact, one can show that $\mathbb{Z}/2\mathbb{Z} \cong \mathrm{Cl}(R), 1 \mapsto \mathfrak{m}$. So, the failure of R to be a principal ideal domain is –informally speaking– as small as possible.

Example 2.30. Here is a more geometric example: One can check that $R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ is a 1-dimensional normal noetherian domain, hence a Dedekind domain. The ideal $\mathfrak{m} = (x-1, y)$ in R is maximal because $R/\mathfrak{m} = \mathbb{R}$ is a field. One can show that $\mathfrak{m}$ is not principal (in fact, as a projective rank 1 module it defines a line bundle on the real unit circle, which is the Möbius stripe) and that $\mathfrak{m}^2 = (X-1)$. Hence, $\mathfrak{m}$ defines a non-trivial, 2-torsion element of $\mathrm{Cl}(R)$. In particular, $\mathrm{Cl}(R) \neq 0$.

On the other hand, $R \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[X, Y](X^2 + Y^2 - 1) \cong \mathbb{C}[U, V]/(UV - 1) = \mathbb{C}[U][U^{-1}]$ with $U = X + iY$ and $V = X - iY$, which is a principal ideal domain because it is a localization of $\mathbb{C}[U]$. Hence, $\mathrm{Cl}(R \otimes_{\mathbb{R}} \mathbb{C}) = 0$.

3. Extensions

Starting from a finite field extension $K \subset \mathbb{Q}$, we aim to show that its ring of integers O_K defined in (1.5) is a Dedekind domain. This leads to the following commutative diagram of subrings:

$$\begin{array}{ccc} K & \longleftarrow & O_K \\ \uparrow & & \uparrow \\ \mathbb{Q} & \longleftarrow & \mathbb{Z}. \end{array}$$

The inclusion $\mathbb{Z} \subset O_K$ is an example of an integral ring map, which are defined and studied in §3.1. We apply this in §3.2 to show that O_K is a Dedekind domain, see Example 3.20. The subsections §§3.3–3.5 study how prime numbers in $\mathbb{Z}$ decompose as products of prime ideals in O_K:

3.1. Integral ring homomorphisms.

Definition 3.1. Let $\varphi\colon A \to B$ be a ring homomorphism. Then, φ is called

(1) *of finite type* if B is a finitely generated A-algebra (via φ), i.e., if there exists a surjective A-algebra map $A[T_1, \ldots, T_n] \to B$ for some $n \in \mathbb{N}$.
(2) *finite* if B is a finitely generated A-module (via φ).
(3) *integral* if every $b \in B$ is integral over A, i.e., there exists $a_1, \ldots, a_n$ such that $b^n + \varphi(a_1)b^{n-1} + \ldots + \varphi(a_n) = 0$.

Exercise 3.2. Let $\varphi\colon A \to B$ and $\psi\colon B \to C$ be ring homomorphisms. Show the following properties:

(1) φ, ψ of finite type $\implies$ $\psi \circ \varphi$ of finite type
(2) φ, ψ finite $\implies$ $\psi \circ \varphi$ finite
(3) φ, ψ integral $\implies$ $\psi \circ \varphi$ integral

Hint: For (3.2) use Proposition 3.3 below.

Proposition 3.3. *Let $\varphi\colon A \to B$ be a ring homomorphism. Then, φ is finite if and only if it is integral and of finite type.*

Proof. Assume φ is finite. Then, it is of finite type and we need to show it is integral. Let $b \in B$ and consider the A-module morphism $B \to B$, $x \mapsto bx$. Since B is a finitely generated A-module, Cayley–Hamilton implies that there exists an integrality equation for b.

For the converse direction, let $B = A[b_1, \ldots, b_m]$ with $b_i \in B$ integral over A. By induction (using that finite morphisms are integral as already shown), we may and do assume $m = 1$, i.e., $B = A[b]$ for some $b \in B$ integral over A. Then, there exist $a_1, \ldots, a_n \in A$ such that $b^{n+r} = -(\varphi(a_1)b^{n-1+r} + \ldots + \varphi(a_n)b^r)$ for all $r \in \mathbb{N}$ (take an integrality equation and multiply it by b^r). Inductively, we see that b^i is contained in the A-submodule of B generated by $1, b, \ldots, b^{n-1}$. Hence, $A[b]$ is generated as an A-module by $1, b, \ldots, b^{n-1}$. □

Definition 3.4. Let $\varphi\colon A \to B$ be a ring homomorphism.

(1) The subring

$$C := \{b \in B \mid b \text{ integral over } A\} \subset B$$

is called the *integral closure of A in B (with respect to φ).*

(2) The ring A is called *integrally closed in B (with respect to φ)* if $C = \varphi(A)$.

Remark 3.5. Let A be a domain. Then, A is normal if and only if A is integrally closed in its fraction field $\mathrm{Frac}(A)$ (with respect to the inclusion).

Exercise 3.6. Let $\varphi\colon A \to B$ be a ring homomorphism and $S \subset A$ a multiplicative subset. Show the following statements:

(1) Let C be the integral closure of A in B. Then, $C[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in $B[S^{-1}]$.
(2) Assume φ is integral. Then, $B[S^{-1}]$ is integral over $A[S^{-1}]$.

Proposition 3.7. *Let B be a domain and $\varphi\colon A \to B$ be an injective, integral ring homomorphism. Then, A is a field if and only if B is a field.*

Proof. Since φ is injective, we may replace A by $\varphi(A)$ and assume that $A \subset B$ is a subring.

First, assume that A is a field. Let $0 \neq y \in B$ and choose $a_1, \dots, a_n \in A$ with $n \in \mathbb{N}$ minimal such that

$$y^n + a_1 y^{n-1} + \dots + a_n = 0. \tag{3.1}$$

Since B is a domain, we have $a_n \neq 0$ by minimality of n. So, $a_n \in A - \{0\} = A^\times$ as A is a field. Multiplying (3.1) by a_n^{-1}, we get

$$1 = -y(y^{n-1} + a_1 y^{n-2} + \dots + a_{n-1}),$$

which shows $y \in B^\times$. So, $B - \{0\} = B^\times$, and B is a field.

Conversely, assume that B is a field. Let $0 \neq x \in A$. Then, $x^{-1} \in B$ is integral over A. Let $a_1, \dots, a_n \in A$ such that $x^{-n} + a_1 x^{-n+1} + \dots + a_n = 0$. Multiplying this equation by x^{n-1} shows $x^{-1} \in A$ as desired. □

Corollary 3.8. *Let $\varphi\colon A \to B$ be an integral ring homomorphism, $\mathfrak{q} \subset B$ be a prime ideal and $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) \subset A$. Then, $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof. The map φ induces an injective, integral ring homomorphism $A/\mathfrak{p} \to B/\mathfrak{q}$. So, the corollary follows from Proposition 3.7. □

Proposition 3.9. *Let $\varphi\colon A \to B$ be an integral ring homomorphism, $\mathfrak{q} \subset \mathfrak{q}' \subset B$ prime ideals with $\varphi^{-1}(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q}')$. Then, $\mathfrak{q} = \mathfrak{q}'$. In particular,* $\dim(B) \leq \dim(A)$.

Proof. Set $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Then, φ induces an integral ring map $\psi = \varphi_\mathfrak{p}\colon A_\mathfrak{p} \to B_\mathfrak{p}$ by Exercise 3.6. Let $\mathfrak{m} := \mathfrak{p}A_\mathfrak{p}$ be the maximal ideal of $A_\mathfrak{p}$, and $\mathfrak{n} := \mathfrak{q}B_\mathfrak{p} \subset \mathfrak{n}' := \mathfrak{q}'B_\mathfrak{p}$ prime ideals of $B_\mathfrak{p}$. So, $\psi^{-1}(\mathfrak{n}) = \psi^{-1}(\mathfrak{n}') = \mathfrak{m}$ by assumption. Corollary 3.8 implies that $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal, hence they are equal. This implies $\mathfrak{q} = \mathfrak{q}'$. □

Proposition 3.10. *Let $\varphi\colon A \to B$ be an injective, integral ring homomorphism, and $\mathfrak{p} \subset A$ a prime ideal. Then, there exists a prime ideal $\mathfrak{q} \subset B$ with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.*

Proof. Consider the commutative diagram of rings

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle 1_B} \\ A_{\mathfrak{p}} & \xrightarrow{\psi=\varphi_{\mathfrak{p}}} & B_{\mathfrak{p}}. \end{array}$$

Since φ is injective, so is ψ and thus $B_{\mathfrak{p}} \neq 0$. Choose a maximal ideal $\mathfrak{n} \subset B_{\mathfrak{p}}$. Then, $\psi^{-1}(\mathfrak{n}) = \mathfrak{p}A_{\mathfrak{p}}$ by Corollary 3.8. Set $\mathfrak{q} := 1_B^{-1}(\mathfrak{n}) \subset B$, which is a prime ideal. Then, $\varphi^{-1}(\mathfrak{q}) = 1_A^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p}$ as desired. □

3.2. **Finiteness properties of integral closures.**

Situation 3.11. Let A be a normal domain with fraction field K. Let $L \supset K$ be an algebraic field extension. Denote by $B := \{x \in L \mid x \text{ integral over } A\}$ the integral closure of A in L. This gives the following commutative diagram of injective ring maps

$$\begin{array}{ccc} L & \longleftarrow & B \\ \uparrow & & \uparrow \\ K & \longleftarrow & A. \end{array} \tag{3.2}$$

such that $B \cap K = A$.

Proposition 3.12. *In Situation 3.11, set $S := A - \{0\}$. Then, the following hold:*

1. *The ring B is a normal domain with $\mathrm{Frac}(B) = B[S^{-1}] = L$. In particular, the left column in (3.2) is the localization at S of the right one.*
2. *Let $x \in L$ and let*
$$\mu_{K,x} = T^m + \tilde{a}_1 T^{m-1} + \ldots + \tilde{a}_m \in K[T]$$
be its minimal polynomial. Let $\mathfrak{a} \subset A$ be an ideal with $\sqrt{\mathfrak{a}} = \mathfrak{a}$ (e.g., $\mathfrak{a}$ prime ideal or $\mathfrak{a} = A$). Then, $\tilde{a}_1, \ldots, \tilde{a}_m \in \mathfrak{a}$ if and only if x satisfies an integrality equation
$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \tag{3.3}$$
with $a_1, \ldots, a_n \in \mathfrak{a}$.
3. *For $x \in L$, one has $x \in B$ if and only if $\mu_{K,x} \in A[T]$.*

Proof. (1): By construction, B is a normal domain. One has the inclusions $B[S^{-1}] \subset \mathrm{Frac}(B) \subset L$. By Exercise 3.6, $B[S^{-1}]$ is the integral closure of $A[S^{-1}] = K$ in L. Since $L \supset K$ is algebraic (i.e., the inclusion is an integral ring map), we have $B[S^{-1}] = L$.

(2): Assume $x \in L$ satisfies (3.3) with $a_1, \ldots, a_n \in \mathfrak{a}$. Let Ω be an algebraic closure of L and write $\mu_{K,x} = (T - x_1) \cdot \ldots \cdot (T - x_m)$ with $x_i \in \Omega$. Then, $x_i = \sigma_i(x)$ for some K-embedding $\sigma_i \colon L \to \Omega$. Hence, (3.3) shows

$$x_i^n + a_1 x_i^{n-1} + \ldots + a_n = \sigma_i(x^n + a_1 x^{n-1} + \ldots + a_n) = 0. \tag{3.4}$$

So, all x_i are integral over A. Set $B' := A[x_1, \ldots, x_m]$, which is a finite A-algebra. Let $\mathfrak{p} \subset A$ be a prime ideal containing $\mathfrak{a}$. By Proposition 3.10, there exists some prime ideal $\mathfrak{q}' \subset B'$ with $\mathfrak{q}' \cap A = \mathfrak{p}$. From (3.4) we get $x_i^n \in \mathfrak{a}B' \subset \mathfrak{p}B' \subset \mathfrak{q}'$, thus $x_i \in \mathfrak{q}'$ for all $i = 1, \ldots, m$. Since the coefficients $\tilde{a}_j$ of $\mu_{K,x}$ are polynomials in the x_i, we see that

- $\tilde{a}_j \in \mathfrak{q}' \subset B'$, and

- $\tilde{a}_j$ is integral over A, so $\tilde{a}_j \in B \cap K = A$

for all $j = 1, \dots, m$. This shows $\tilde{a}_j \in \cap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p} = \sqrt{\mathfrak{a}} = \mathfrak{a}$ for all $j = 1, \dots, m$.

(3): Follows from (2) with $\mathfrak{a} = A$. □

Example 3.13. In Situation 3.11, we assume $\mathrm{char}(K) \neq 2$ and $L := K[\sqrt{d}]$ for some $d \in K^\times \backslash (K^\times)^2$. Then, $L \supset K$ is a Galois extension of degree 2. Denote $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$ with $\sigma(\sqrt{d}) = -\sqrt{d}$. Let $x = a + \sqrt{d}b \in L$ with $b \neq 0$, i.e., $x \in L \backslash K$. Then,

$$\mu_{K,x} = (T - x)(T - \sigma(x)) = T^2 - 2aT + (a^2 - b^2 d).$$

Hence, Proposition 3.12 shows

$$\begin{aligned} B &= \{x \in L \mid \text{x integral over } A\} \\ &= \{a + b\sqrt{d} \in L \mid a \in A, b = 0 \text{ or } 2a, a^2 - b^2 d \in A\} \\ &= \{a + b\sqrt{d} \in L \mid 2a, a^2 - b^2 d \in A\}. \end{aligned}$$

Exercise 3.14. Let B be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ square free. Show that $B = \mathbb{Z}[\theta]$ with

$$\theta := \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \mod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Situation 3.15. Let A be a Dedekind domain with fraction field K. Let $L \supset K$ be a finite field extension. Then, $B := \{x \in L \mid x \text{ integral over } A\} = \{x \in L \mid \mu_{K,x} \in A[T]\}$ and $L = \{\frac{b}{a} \mid b \in B, a \in A - \{0\}\} = \mathrm{Frac}(B)$ by Proposition 3.12.

Hypothesis 3.16. In Situation 3.15, the ring B is a finite A-algebra.

Theorem 3.17. *In Situation 3.15 assume Hypothesis 3.16. Then, the following hold:*

1. *The ring B is a Dedekind domain. It is a field if and only if A is so.*
2. *The ring B is a finitely generated, projective A-module of rank $[L : K]$. It is free of rank $[L : K]$ if A is a principal ideal domain.*

Remark 3.18. Theorem 3.17(1) holds without Hypothesis 3.16, see [Sta18, 00PG].

Proof of Theorem 3.17. (1): The ring B is a normal domain by definition and $\dim(B) \leq \dim(A) \leq 1$ by Proposition 3.9. Then, Hypothesis 3.16 implies that B is Noetherian and hence a Dedekind domain by Theorem 2.18. Finally, B is a field if and only if A is so by Corollary 3.7.

(2): The A-module B is torsion free because $B \subset L$. Since it is finitely generated by Hypothesis 3.16, Theorem 2.12 implies that it is projective of rank $\dim_K(B \otimes_A K) = [L : K]$. □

Proposition 3.19. *In Situation 3.15, Hypothesis 3.16 is satisfied in each of the following cases:*

1. *The extension $L \supset K$ is separable (e.g., if $\mathrm{char}(K) = 0$).*
2. *The ring A is a finitely generated k-algebra for some field k.*
3. *The ring A is a complete, discrete valuation ring.*

Proof. See later. □

At this point, we have established the basic structural properties of number rings:

Example 3.20. For a finite field extension $K \supset \mathbb{Q}$, the preceding discussion shows that $O_K := \{x \in K \mid x \text{ integral over } \mathbb{Z}\}$ is a 1-dimensional Dedekind ring that is free of rank $[K : \mathbb{Q}]$ as a $\mathbb{Z}$-module. In particular, we have seen that every (fractional) ideal of O_K admits a unique decomposition into prime ideals.

3.3. **Ramification index and inertia degree.** In Situation 3.15 and under Hypothesis 3.16, we use without further mentioning the results of the previous section: namely, B is a Dedekind domain that is a finitely generated, projective A-module of rank $[L : K]$. Further, for a prime ideal $0 \neq \mathfrak{p} \subset A$ we denote by $\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = A/\mathfrak{p}$ the *residue field*, where the last equality holds by maximality of $\mathfrak{p}$.

Definition 3.21. In Situation 3.15 assume Hypothesis 3.16. For a prime ideal $0 \neq \mathfrak{p} \subset A$ one writes $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_r^{e_r}$ with prime ideals $0 \neq \mathfrak{q}_i \subset B$ and all $e_i \geq 1$ as in Corollary 2.22. The prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are called *divisors of* $\mathfrak{p}$ *in* B. One writes $\mathfrak{q}_i \mid \mathfrak{p}$ for $i = 1, \ldots, r$ and also says that $\mathfrak{q}_i$ *lies above* $\mathfrak{p}$. Further, one calls

(1) $e_i = e_{\mathfrak{q}_i}$ the *ramification index of* $\mathfrak{q}_i$, and
(2) $f_i = f_{\mathfrak{q}_i} = [B/\mathfrak{q}_i : A/\mathfrak{p}]$ the *inertia degree of* $\mathfrak{q}_i$.

Remark 3.22. For all prime ideals $\mathfrak{q} \subset B$, one has:

$$\mathfrak{q} \mid \mathfrak{p} \iff \mathfrak{p}B \subset \mathfrak{q} \iff \mathfrak{p} = \mathfrak{q} \cap A$$

Remark 3.23. For the reader familiar with some algebraic geometry: The inclusion $A \subset B$ induces a map $f\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ on spectra. For some $0 \neq \mathfrak{p} \in \operatorname{Spec}(A)$ its preimage $f^{-1}(\mathfrak{p})$ consists exactly of the prime ideals $\mathfrak{q} \in \operatorname{Spec}(B)$ lying above $\mathfrak{p}$, i.e., $\mathfrak{q} \mid \mathfrak{p}$. In the following we will study the geometry of the map f. The reader knowing how to translate between rings and affine schemes should think about f when appropriate.

Theorem 3.24. *In Situation 3.15 assume Hypothesis 3.16. Let $0 \neq \mathfrak{p} \subset A$ be a prime ideal. Then, one has the following equality of numbers:*

$$\sum_{\mathfrak{q} \mid \mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q} = [L : K] \tag{3.5}$$

It is called the fundamental equality.

Proof. By Theorem 2.12, $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank $[L : K]$. Hence, $B_\mathfrak{p} \otimes_{A_\mathfrak{p}} \kappa(\mathfrak{p}) = B/\mathfrak{p}B$ is a $\kappa(\mathfrak{p})$-vector space of rank $[L : K]$. It remains to identify $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B)$ with the left hand side in (3.5).

Since all prime ideals $\mathfrak{q} \mid \mathfrak{p}$ are maximal in B, we get $\mathfrak{q}^{e_\mathfrak{p}} + \tilde{\mathfrak{q}}^{e_{\tilde{\mathfrak{q}}}} = B$ for all $\mathfrak{q} \neq \tilde{\mathfrak{q}}$ dividing $\mathfrak{p}$. Thus, the Chinese remainder theorem implies $B/\mathfrak{p}B = \prod_{\mathfrak{q}\mid\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$. It remains to show $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q} f_\mathfrak{q}$ for all $\mathfrak{q} \mid \mathfrak{p}$.

So, fix a prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$. We proceed by induction on $e_\mathfrak{q}$. For $e_\mathfrak{q} = 1$, we have $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{q}) = f_\mathfrak{q}$ by definition. For $e_\mathfrak{q} > 1$, we have an exact sequence of $\kappa(\mathfrak{p})$-vector spaces

$$0 \to \mathfrak{q}B/\mathfrak{q}^{e_\mathfrak{q}} \to B/\mathfrak{q}^{e_\mathfrak{q}} \to B/\mathfrak{q} \to 0.$$

Since $\mathfrak{q}$ is invertible, multiplication by a uniformizer of $B_\mathfrak{q}$ induces an isomorphism $B/\mathfrak{q}^{e_\mathfrak{q}-1} \cong \mathfrak{q}B/\mathfrak{q}^{e_\mathfrak{q}}$. Thus, we can conclude by induction. This finishes the proof of the theorem. □

Corollary 3.25. *In Situation 3.15 assume Hypothesis 3.16. Let $0 \neq \mathfrak{p} \subset A$ be a prime ideal. Then, there are at most $[L:K]$-many prime ideals $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$.*

Definition 3.26. In Situation 3.15 assume Hypothesis 3.16. A prime ideal $0 \neq \mathfrak{p} \subset A$ is called

(1) *unramified (in L)* if for all prime ideals $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$ one has $e_{\mathfrak{q}} = 1$ and $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ is separable.
(2) *ramified (in L)* if it is not unramified in L.
(3) *totally split (in L)* if $e_{\mathfrak{q}} = f_{\mathfrak{q}} = 1$ for all prime ideals $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$.

Remark 3.27. Later $\kappa(\mathfrak{p})$ is often a finite field. In this case, the separability condition in Definition 3.26(1) is automatic. Further, we have:

(1) The prime ideal $\mathfrak{p}$ is unramified if and only if $B/\mathfrak{p}B$ is a finite product of finite separable field extensions of $\kappa(\mathfrak{p})$, i.e., $B/\mathfrak{p}B$ is an étale $\kappa(\mathfrak{p})$-algebra.
(2) The prime $\mathfrak{p}$ is totally split if and only if $\#\{\mathfrak{q} \mid \mathfrak{p}\} = [L:K]$ if and only if $B/\mathfrak{p}B \simeq \kappa(\mathfrak{p}) \times \ldots \times \kappa(\mathfrak{p})$.

Remark 3.28. In Situation 3.15 assume Hypothesis 3.16. The decomposition behavior of $\mathfrak{p}$ in B is completely controlled by the $\kappa(\mathfrak{p})$-algebra $B/\mathfrak{p}B$ as follows:

(1) One has $\dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B) = [L:K]$.
(2) The Chinese remainder theorem induces a ring isomorphism
$$B/\mathfrak{p}B \cong (B/\mathfrak{p}B)_{\overline{\mathfrak{q}_1}} \times \ldots \times (B/\mathfrak{p}B)_{\overline{\mathfrak{q}_1}}$$
where $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \subset B$ are the pairwise distinct prime ideals lying above $\mathfrak{p}$ and $\overline{\mathfrak{q}_1}, \ldots, \overline{\mathfrak{q}_r}$ their images in $B/\mathfrak{p}B$.
(3) Each ring $B_i := (B/\mathfrak{p}B)_{\overline{\mathfrak{q}_i}}$ is a 0-dimensional local ring with maximal ideal $\mathfrak{m}_i = \overline{\mathfrak{q}_i}B_i$ and residue field $B_i/\mathfrak{m}_i = \kappa(\mathfrak{q}_i)$. Then, one has $e_{\mathfrak{q}_i} = \min\{e \geq 1 \mid \mathfrak{m}_i^e = 0\}$ and $f_{\mathfrak{q}_i} = [B_i/\mathfrak{m}_i : \kappa(\mathfrak{p})]$.

Hence, passing to the localization in $\mathfrak{p}$ does not change the decomposition behavior. More precisely, replacing A by $A_{\mathfrak{p}}$, $\mathfrak{p}$ by $\mathfrak{p}A_{\mathfrak{p}}$ and B by $B_{\mathfrak{p}}$ and $\mathfrak{q}$ by $\mathfrak{q}B_{\mathfrak{p}}$ for all $\mathfrak{q} \mid \mathfrak{p}$ does not change K, L and $B/\mathfrak{p}B$, so does not change $\kappa(\mathfrak{p})$, $\kappa(\mathfrak{q})$, $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}}$.

Proposition 3.29. *In Situation 3.15 assume Hypothesis 3.16. In addition, assume that $L \supset K$ is finite separable, and let $\theta \in B$ such that $L = K[\theta]$ (note that θ always exists by the theorem of the primitive element [Sta18, 09HZ]). Let $\mathfrak{c} := \{x \in B \mid xB \subset A[\theta]\} \subset B$ ideal, and let $0 \neq \mathfrak{p} \subset A$ prime ideal with $\mathfrak{p}B + \mathfrak{c} = B$ (if $B = A[\theta]$, then $\mathfrak{c} = B$ and so $\mathfrak{p}B + \mathfrak{c} = B$ holds for all prime ideals). Let $f := \mu_{K,\theta} \in A[T]$ be the minimal polynomial of θ, and let $\bar{f} = f \mod \mathfrak{p} \in (A/\mathfrak{p})[T]$. Let $\bar{f} = \bar{f}_1^{e_1} \cdot \ldots \cdot \bar{f}_r^{e_r}$ be the decomposition into irreducible factors with $\bar{f}_i$ pairwise prime to each other. Choose monic polynomials $f_i \in A[T]$ with $\bar{f}_i \equiv f_i \mod \mathfrak{p}$. Then, the ideals*
$$\mathfrak{q}_i := \mathfrak{p}B + f_i(\theta)B, \quad i = 1, \ldots, r$$
are precisely the prime ideals of B lying above $\mathfrak{p}$ and $e_{\mathfrak{q}_i} = e_i$, $f_{\mathfrak{q}_i} = \deg(\bar{f}_i)$ for all $i = 1, \ldots, r$.

Example 3.30. Let $L = \mathbb{Q}[\sqrt{d}]$ with $d \in \mathbb{Z}$ be square free and $d \equiv 2, 3 \mod 4$. Then, $B = \mathbb{Z}[\sqrt{d}]$ by Exercise 3.14. Apply Proposition 3.29 to $f = \mu_{\mathbb{Q},\sqrt{d}} = X^2 - d$ and some prime number $p \in \mathbb{Z}$. So, consider $\bar{f} = T^2 - \bar{d} \in \mathbb{F}_p[T]$. There are three cases:

(1) *Assume* $p \mid d$ *or* $p = 2$. Then, $\bar{f} = (T - \bar{d})^2$. There exists a unique prime ideal $\mathfrak{q} \subset \mathbb{Z}[\sqrt{d}]$ over (p) and $e_\mathfrak{q} = 2$, $f_\mathfrak{q} = 1$. More precisely, for $p \mid d$ one has $\bar{f} = T^2$ and $\mathfrak{q} = (p, \sqrt{d})$. For $p = 2$ and d odd, one has $\bar{f} = T^2 - 1 = (T-1)^2$ and $\mathfrak{q} = (p, \sqrt{d} - 1)$.
(2) *Assume* $p \nmid 2d$ *and* $(\frac{d}{p}) = 1$ *(i.e.,* $\bar{d} = \bar{\delta}^2$ *for* $\bar{\delta} \in \mathbb{F}_p$*).* Then, $\bar{f} = (T - \bar{\delta})(T + \bar{\delta})$. Choose lift $\delta \in \mathbb{Z}$ of $\bar{\delta}$. Then, there exist two prime ideals $\mathfrak{q}_+$, $\mathfrak{q}_-$ in $\mathbb{Z}[\sqrt{d}]$ over (p). One has $\mathfrak{q}_\pm = (p, \sqrt{d} \pm \delta)$ and $e_{\mathfrak{q}_\pm} = f_{\mathfrak{q}_\pm} = 1$.
(3) *Assume* $p \nmid 2d$ *and* $(\frac{d}{p}) = -1$. Then, $\bar{f}$ irreducible and there exists a unique $\mathfrak{q}$ lying above (p). One has $\mathfrak{q} = pB$ and $e_\mathfrak{q} = 1$, $f_\mathfrak{q} = 2$.

Hence, p ramified in $\mathbb{Q}[\sqrt{d}]$ if and only if $p \mid 2d$, which happens only for finitely many primes. The other two possible cases happen "equally often", in particular infinitely many times.

Exercise 3.31. (1) Do Example 3.30 for square free $d \in \mathbb{Z}$ with $d \equiv 1 \mod 4$, compare with Exercise 3.14. Note that for $d = 5$ the decomposition behavior only depends on $p \mod 5$.
(2) Let ζ_5 be a primitive 5th root of unity, $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \mathbb{Q}[\zeta_5]$. Show the following properties:
   (a) $\mu_{\mathbb{Q},\zeta_5} = T^4 + T^3 + T^2 + T + 1$
   (b) $B = \mathbb{Z}[\zeta_5]$
   (c) Determine the decomposition behavior and ramification behavior for all prime numbers $p \in \mathbb{Z}$. Note that this depends only on $p \mod 5$.

   Hint: It can be helpful to note that $\mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}[\zeta_5]$ because $(\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4)^2 = 5$.

Proof of Proposition 3.29. Set $B' := A[\theta] \subset B$. First off, we prove that the inclusion $B' \subset B$ induces $B'/\mathfrak{p}B' \cong B/\mathfrak{p}B$. Indeed, the composition $\varphi\colon B' \hookrightarrow B \to B/\mathfrak{p}B$ is surjective because $\mathfrak{c} + \mathfrak{p}B = B$. Hence, the desired isomorphism follows from

$$\mathfrak{p}B' \subset \mathfrak{p}B \cap B' = \ker(\varphi) = (\mathfrak{p}B + \mathfrak{c})(\mathfrak{p}B \cap B') \subset \mathfrak{p}B',$$

where we use $\mathfrak{c}B \subset B'$ for the last inclusion.

Next, we observe that the map $T \mapsto \theta$ induces a ring isomorphism $A[T]/(f) \cong A[\theta] =: B'$. This gives ring isomorphisms

$$B'/\mathfrak{p}B' = B' \otimes_A A/\mathfrak{p} = A[T]/((f) + \mathfrak{p}) = \kappa(\mathfrak{p})[T]/(\bar{f}) = \prod_{i=1}^{r} \kappa(\mathfrak{p})[T]/(\bar{f}_i^{e_i}),$$

which implies the proposition. □

3.4. **Discriminant.**

Reminder 3.32 (On trace and norm)**.** (1) Let K be a field and A a finite K-algebra of dimension $n \in \mathbb{N}$. For $a \in A$, consider the K-linear map $m_a\colon A \to A$, $x \mapsto ax$ and its characteristic polynomial

$$\chi_{A/K,a} = T^n - \mathrm{tr}(m_a)X^{n-1} + \ldots + (-1)^n \det(m_a) \in K[T].$$

The *norm of* a *with respect to* A/K is defined as $N_{A/K}(a) := \det(m_a)$ and the *trace of* a *with respect to* A/K is defined as $\mathrm{Tr}_{A/K}(a) := \mathrm{tr}(m_a)$. Then, $\mathrm{Tr}_{A/K}\colon A \to K$ is K-linear and one has $N_{A/K}(ab) = N_{A/K}(a)N_{A/K}(b)$ for all $a, b \in A$. In particular, $N_{A/K}\colon A^\times \to K^\times$ is a group homomorphism.

Furthermore, for an algebraic closure Ω of K, the following are equivalent [Sta18, 0BIE]:
(a) One has $A \simeq K_1 \times \ldots \times K_r$ for separable, finite field extensions $K_i \supset K$.
(b) One has $A \otimes_K \Omega \simeq \Omega \times \ldots \times \Omega$.
(c) The trace pairing $A \times A \to K$, $(a, b) \mapsto \mathrm{Tr}_{A/K}(ab)$ is non-degenerate.
If $A = L \supset K$ is a finite field extension, then these properties are equivalent to $\mathrm{Tr}_{L/K} \neq 0$.

(2) Let $L \supset K$ be a finite field extension, and choose an algebraic closure Ω of K. Let $\{\sigma_1, \ldots, \sigma_s\}$ be the set of K-embeddings of L in Ω (recall that $[L : K] = sq$ where s is the separability degree of L/K, e.g., $q = 1$ if $\mathrm{char}(K) = 0$, otherwise q is a power of $\mathrm{char}(K)$). Then, for all $a \in L$ we have the following equalities:

$$N_{L/K}(a) = \left(\prod_{i=1}^{r} \sigma_i(a) \right)^q$$

$$\mathrm{Tr}_{L/K}(a) = q \sum_{i=1}^{r} \sigma_i(a)$$

Furthermore, if $M \supset L \supset K$ are finite field extensions, then $N_{M/K} = N_{L/K} \circ N_{M/L}$ and $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$.

Remark 3.33. In Situation 3.15, one has $N_{L/K}(b), \mathrm{Tr}_{L/K}(b) \in A$ for all $b \in B$. Indeed, we have $\mu_{K,b} \in A[T]$ by Proposition 3.12(3), which implies $\chi_{L/K,b} \in A[T]$ (e.g., using Cayley–Hamilton to see that $\chi_{L/K,b}$ is a power of $\mu_{K,b}$).

We can now give the proof of Proposition 3.19(1), saying that in Situation 3.15 the Hypothesis 3.16 (i.e., that B is a finitely generated A-module) holds if $L \supset K$ is a *separable* field extension.

Proof of Proposition 3.19(1). For an A-submodule $M \subset L$, set

$$M^\vee = \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in A \text{ for all } y \in M\},$$

which is called the dual A-submodule of L with respect to the trace pairing. Note that $B \subset B^\vee$ by Remark 3.33. Let $(e_1, \ldots, e_n)$ be a K-basis of L with all $e_i \in B$. Consider the A-submodule of B generated by $e_1, \ldots, e_n$. Then, $V \subset B \subset B^\vee \subset V^\vee$ and $V^\vee$ generated by the dual basis of $(e_1, \ldots, e_n)$ with respect to the *non-degenerate* trace pairing. Since A is noetherian, the finitely generated A-module $V^\vee$ is noetherian and so is its submodule B. This shows that B is a finitely generated A-module. □

Remark 3.34. The preceding proof shows that $B^\vee$ is a finitely generated A-module, hence a finitely generated generated B-module. In particular, $B^\vee \in \mathrm{Div}(B)$ is a fractional ideal and its inverse $D_{B/A} := (B^\vee)^{-1} \in \mathrm{Div}(B)$ is called the *different of B over A*.

Definition 3.35. In Situation 3.15 assume that $L \subset K$ is separable. The *norm of divisors* is the group homomorphism $N_{L/K} \colon \mathrm{Div}(B) \to \mathrm{Div}(A)$ defined by $N_{L/K}(\mathfrak{q}) := (\mathfrak{q} \cap A)^{f_\mathfrak{q}}$.

Exercise 3.36. In Situation 3.15 assume that $K \subset L$ is separable. Then, the following properties hold:

(1) For $0 \neq a \in L$, one has $N_{L/K}((a)) = N_{L/K}(a)A$ as elements of $\mathrm{Div}(A)$.

(2) Let I be a fractional ideal of A. Then, IB is a fractional ideal of B and $N_{L/K}(IB) = I^{[L:K]}$.

Definition 3.37. In Situation 3.15 assume that $L \subset K$ is separable.

(1) Let $x_1, \dots, x_n \in L$ and form the matrix $(\mathrm{Tr}_{L/K}(x_i x_j))_{i,j} \in \mathrm{Mat}_{n\times n}(K)$. Then, its determinant
$$\Delta(x_1, \dots, x_n) := \det((\mathrm{Tr}_{L/K}(x_i x_j))_{i,j})$$
is called the *discriminant of B over A*.

(2) Let $\Delta_{B/A} \subset A$ be the ideal generated by $\Delta(x_1, \dots, x_n)$ where $(x_1, \dots, x_n)$ runs through all K-basis of L with $x_1, \dots, x_n \in B$. The ideal $\Delta_{B/A}$ is called the *discriminant of B over A*.

Remark 3.38. The analogue of the preceding definition for inseparable field extensions $L \supset K$ is not useful since $\mathrm{Tr}_{L/K} = 0$ in this case. Furthermore, let us point out the following properties in the context of Definition 3.37:

(1) If $(x_1, \dots, x_n)$ is a K-basis of L, then $\Delta(x_1, \dots, x_n) \neq 0$ since $\mathrm{Tr}_{L/K}$ is non-degenerate.

(2) For $(x_1, \dots, x_n)$ is a K-basis of L and $x_1', \dots, x_n' \in L$, let $u\colon L \to L$ be the K-linear map with $u(x_i) = x_i'$. Then, one has
$$\Delta(x_1', \dots, x_n') = \det(u)^2 \Delta(x_1, \dots, x_n).$$

(3) Assume B is a free A-module (e.g., this holds if A is a principal ideal domain). Choose an A-basis $(x_1, \dots, x_n)$ of B. Then, one has $\Delta_{B/A} = (\Delta(x_1, \dots, x_n))$ by (2).

Example 3.39. Let $L = \mathbb{Q}[\sqrt{d}]$ for a square free $d \in \mathbb{Z}$ and B the integral closure of $\mathbb{Z}$ in L. Assume $d \equiv 1 \mod 4$. Then, $B = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ by Exercise 3.14, which is a free $\mathbb{Z}$-module with ordered basis $1, \frac{1+\sqrt{d}}{2}$. The associated trace matrix is given by
$$\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix}.$$
Thus, we compute $\Delta(1, \frac{1+\sqrt{d}}{2}) = d$ for its determinant. By Remark 3.38(3), we get $\Delta_{B/\mathbb{Z}} = (d)$.

Exercise 3.40. In the situation of Example 3.39, show that $\Delta_{B/A} = (4d)$ if $d \equiv 2, 3 \mod 4$.

Exercise 3.41. In Situation 3.15 assume $A = \mathbb{Z}$. Define $d_L := \Delta(x_1, \dots, x_n) \in \mathbb{Z}$ where $(x_1, \dots, x_n)$ is a $\mathbb{Z}$-basis of B. Show that d_L is independent of the choice of $(x_1, \dots, x_n)$. (Hence, we can consider the discriminant as a number rather than as an ideal in this case.)

Lemma 3.42. *Let $L \supset K$ be a separable, finite field extension. Let Ω be an algebraic closure of K and let $\sigma_1, \dots, \sigma_n\colon L \to \Omega$ be the K-embeddings with $n = [L : K]$.*

(1) For every K-basis $x_1, \dots, x_n$ of L one has $\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j)_{i,j})^2$.

(2) Let $\theta \in L$ with $L = K[\theta]$. Then, one has
$$\Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{1\leq i<j\leq n} (\theta_i - \theta_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \mu'_{K,\theta}(\theta_i)$$

where $\theta_i := \sigma_i(\theta)$ for all $i = 1, \dots, n$ and $\mu'_{K,\theta}$ denotes the first derivative of $\mu_{K,\theta}$.

Proof. (1): Using Reminder 3.32(2), we compute

$$\mathrm{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j).$$

Hence, we get a factorization of matrices $(\mathrm{Tr}_{L/K}(x_i x_j))_{i,j} = {}^t(\sigma_k(x_i))_{k,i}(\sigma_k(x_j))_{k,j}$. This implies (1) by taking determinants.

(2): Part (1) implies

$$\Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \det \begin{pmatrix} 1 & \theta_1 & \dots & \theta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \dots & \theta_n^{n-1} \end{pmatrix}^2,$$

which is equal to $\prod_{i<j}(\theta_i - \theta_j)^2$ by linear algebra (use induction on n). This can be rewritten as

$$(-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\theta_i - \theta_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \mu'_{K,\theta}(\theta_i),$$

noting that $\mu_{K,\theta} = \prod_{i=1}^{n}(T - \theta_i)$. □

Example 3.43. Let $L = \mathbb{Q}[\theta]$ with $\theta = \sqrt[3]{2}$. Then, $\mu_{K,\theta} = X^3 - 2$ and $\mu'_{K,\theta} = 3X^2$. Further, $\theta_i = \zeta_3^i \theta$ for $i = 0, 1, 2$ with ζ_3 a primitive 3rd root of unity. Lemma 3.42(2) implies

$$\Delta(1, \sqrt[3]{2}, \sqrt[3]{4}) = (-1)^3 27 \zeta_3^3 (\sqrt[3]{2}^2)^3 = -2^2 3^3.$$

In fact, one can show $B = \mathbb{Z}[\sqrt[3]{2}]$ and so $\Delta_{B/\mathbb{Z}} = (2^2 3^3)$, see [Con].

Lemma 3.44. *In Situation 3.15 let $0 \notin S \subset A$ be a multiplicative subset. Then, one has $\Delta_{B[S^{-1}]/A[S^{-1}]} = \Delta_{B/A}[S^{-1}]$ as ideals in $A[S^{-1}]$.*

Proof. First off, $A[S^{-1}]$ is a Dedekind ring and $B[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in L, see Exercise 3.6. So, the left hand side of the equality is well-defined to begin with. Now, let $x_1, \dots, x_n \in B$ be a K-basis of L. Since $x_1, \dots, x_n \in B[S^{-1}]$ we get $\Delta_{B/A} \subset \Delta_{B[S^{-1}]/A[S^{-1}]}$ and so $\Delta_{B/A}[S^{-1}] \subset \Delta_{B[S^{-1}]/A[S^{-1}]}$. Conversely, let $x_1, \dots, x_n \in B[S^{-1}]$ be a K-basis of L. Choose $s \in S$ with $sx_1, \dots, sx_n \in B$, which is still a K-basis of L. Then, we have

$$\Delta(sx_1, \dots, sx_n) = \det(\mathrm{Tr}_{L/K}(sx_i sx_j)_{i,j}) = s^{2n}\Delta(x_1, \dots, x_n).$$

In particular, $\Delta(x_1, \dots, x_n) = \frac{1}{s^{2n}}\Delta(sx_1, \dots, sx_n) \in \Delta_{B/A}[S^{-1}]$. □

Theorem 3.45. *In Situation 3.15 assume $L \supset K$ is separable. For a prime ideal $0 \neq \mathfrak{p} \subset A$, the following are equivalent:*

(1) The prime ideal $\mathfrak{p}$ is unramified in B.
(2) One has $\mathfrak{p} \nmid \Delta_{B/A}$.

In particular, there exist only finitely many prime ideals of A that are ramified in B.

Proof. By Remark 3.28 and Lemma 3.44 we may and do replace A by $A_{\mathfrak{p}}$, so assume without loss of generality that A is a discrete valuation ring. In this case, B is a free A-module of rank $[L:K]$. Let $x_1,\dots,x_n$ be an A-basis of B. So, $\Delta_{B/A} = (\Delta(x_1,\dots,x_n))$ by Remark 3.38(3). Denote by $B \to B/\mathfrak{p}B =: \bar{B}$, $x \mapsto \bar{x}$ the reduction map. Then, $\mathfrak{p} \nmid \Delta_{B/A}$ if and only if $\Delta(x_1,\dots,x_n) \notin \mathfrak{p}$ if and only if

$$0 \neq \overline{\Delta(x_1,\dots,x_n)} = \overline{\det(\mathrm{Tr}_{L/K}(x_i x_j)_{i,j})} = \det(\mathrm{Tr}_{\bar{B}/\kappa(\mathfrak{p})}(\bar{x}_i\bar{x}_j)_{i,j})$$

if and only if the pairing $\bar{B}\times\bar{B}\to\kappa(\mathfrak{p})$, $(\bar{x},\bar{y})\mapsto \mathrm{Tr}_{\bar{B}/\kappa(\mathfrak{p})}(\bar{x}\bar{y})$ is non-degenerate if and only if $\bar{B}$ is a finite product of separable, finite field extensions of $\kappa(\mathfrak{p})$ if and only if $\mathfrak{p}$ is unramified in B, see Reminder 3.32(1). □

Exercise 3.46. In Situation 3.15 assume that $L \subset K$ is separable. Let $D_{B/A}$ be the different defined in Remark 3.34. Show that $N_{L/K}(D_{B/A}) = \Delta_{B/A}$.

3.5. **Galois extensions.** In this subsection, we assume we are in Situation 3.15 with $L \supset K$ a Galois extension, i.e., a separable and normal extension. We denote by

$$G := \mathrm{Gal}(L/K) := \mathrm{Aut}_{K\text{-alg}}(L)$$

its Galois group, i.e., the K-algebra automorphisms of L. Recall that G is a finite group of order $[L:K]$, and that the map $H \mapsto L^H := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ induces a bijection between subgroups of G and intermediate field extensions of $L \supset K$ by Galois theory [Sta18, 09DW].

Proposition 3.47. *For each prime ideal $0 \neq \mathfrak{p} \subset A$, the map*

$$\mathrm{Gal}(L/K) \times \left\{ \begin{matrix} \mathfrak{q} \subset B \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p} \end{matrix} \right\} \to \left\{ \begin{matrix} \mathfrak{q} \subset B \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p} \end{matrix} \right\}$$
$$(\sigma, \mathfrak{q}) \mapsto \sigma(\mathfrak{q})$$

is well-defined and transitive.

Proof. First off, for $\sigma \in G = \mathrm{Gal}(L/K)$ one has $\sigma(B) = B$: Indeed, we have

$$x \in B \iff x \text{ integral over } A \iff \sigma(x) \text{ integral over } A \iff \sigma(x) \in B$$

for all $x \in L$. In particular, we can form the fixed points

$$B^G := \{b \in B \mid \sigma(b) = b \text{ for all } \sigma \in G\},$$

which is equal to $B \cap K = A$ by Galois theory. So, the action is well-defined.

Let $\mathfrak{q}, \mathfrak{q}' \subset B$ be prime ideals lying above $\mathfrak{p}$. Assume that $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in G$. By the Chinese remainder theorem, there exists $x \in B$ such that $x \equiv 0 \mod \mathfrak{q}'$ (i.e., $x \in \mathfrak{q}'$) and $x \equiv 1 \mod \sigma(\mathfrak{q})$ (i.e., $x \notin \sigma(\mathfrak{q})$) for all $\sigma \in G$. The first congruence implies $N_{L/K}(x) = \prod_{\sigma\in G}\sigma(x) \in \mathfrak{q}' \cap A = \mathfrak{p}$. The second congruence implies $\sigma(x) \notin \mathfrak{q}$ for all $\sigma \in G$, so $N_{L/K}(x) \notin \mathfrak{q}$ as $\mathfrak{q}$ is a prime ideal $\lightning$. □

Corollary 3.48. *Let $0 \neq \mathfrak{p} \subset A$ be a prime ideal and $\mathfrak{q}, \mathfrak{q}' \subset B$ prime ideals lying above $\mathfrak{p}$. Then, one has $e_{\mathfrak{q}} = e_{\mathfrak{q}'} =: e$ and $f_{\mathfrak{q}} = f_{\mathfrak{q}'} =: f$. In particular, $\mathfrak{p}B = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^e$ with $r = \#\{\mathfrak{q} \mid \mathfrak{p}\}$ and $[L:K] = ref$.*

Proof. By Remark 3.28(2), the numbers $e_{\mathfrak{q}}$, $f_{\mathfrak{q}}$ are determined by $(B/\mathfrak{p}B)_{\overline{\mathfrak{q}}}$. By Proposition 3.47 there exists some $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Since σ is a ring automorphism of B which fixes $\mathfrak{p}$, it induces a ring isomorphism $(B/\mathfrak{p}B)_{\overline{\mathfrak{q}}} \cong (B/\mathfrak{p}B)_{\overline{\mathfrak{q}'}}$. The corollary follows. □

Definition 3.49. Let $0 \neq \mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ be prime ideals with $\mathfrak{q} \mid \mathfrak{p}$. Then, the group

$$G_{\mathfrak{q}} := \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\} = \mathrm{Stab}_G(\mathfrak{q})$$

is called the *decomposition group of* $\mathfrak{q}$. The corresponding fixed field $Z_{\mathfrak{q}}$ is called the *decomposition field of* $\mathfrak{q}$.

Remark 3.50. With the notation of Definition 3.49 we have:

(1) For $\sigma \in G$, one has $G_{\sigma(\mathfrak{q})} = \sigma G_{\mathfrak{q}} \sigma^{-1}$ as subgroups of G.
(2) The map $\sigma \mapsto \sigma(\mathfrak{q})$ induces a bijection

$$G/G_{\mathfrak{q}} \xrightarrow{1:1} \left\{ \begin{array}{c} \mathfrak{q} \subset B \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p} \end{array} \right\}.$$

Both sets are finite of cardinality $[Z_{\mathfrak{q}} : K]$ by Galois theory.
(3) One has $G_{\mathfrak{q}} = 1$ if and only if $Z_{\mathfrak{q}} = L$ if and only if $\mathfrak{p}$ is *completely decomposed (or, totally split) in* L, i.e., $e_{\mathfrak{q}} = f_{\mathfrak{q}} = 1$ for all prime ideals $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$.
(4) One has $G_{\mathfrak{q}} = G$ if and only if $Z_{\mathfrak{q}} = K$ if and only if $\mathfrak{p}B = \mathfrak{q}^e$ for some prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid \mathfrak{p}$.
(5) In general, $\mathfrak{p}$ totally decomposes in $Z_{\mathfrak{q}}$ and $\mathfrak{q}$ is the unique prime ideal lying above $\mathfrak{q} \cap Z_{\mathfrak{q}}$. One has $e_{\mathfrak{q} \cap Z_{\mathfrak{q}}} = f_{\mathfrak{q} \cap Z_{\mathfrak{q}}} = 1$ for $\mathfrak{q} \cap Z_{\mathfrak{q}}$ lying above $\mathfrak{p}$ and $e_{L/Z_{\mathfrak{q}},\mathfrak{q}} = e_{\mathfrak{q}}$, $f_{L/Z_{\mathfrak{q}},\mathfrak{q}} = f_{\mathfrak{q}}$ for $\mathfrak{q}$ lying above $\mathfrak{q} \cap Z_{\mathfrak{q}}$.

Proposition 3.51. *With the notation of Definition 3.49 let* $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ *and* $\kappa(\mathfrak{q}) = B/\mathfrak{q}$. *Then,* $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ *is a normal field extension and one has a surjective group homomorphism*

$$\begin{aligned} G_{\mathfrak{q}} &\to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) := \mathrm{Aut}_{\kappa(\mathfrak{p})\text{-}alg}(\kappa(\mathfrak{q})) \\ \sigma &\mapsto \sigma|_B \mod \mathfrak{q}. \end{aligned}$$

Proof. Let $Z_{\mathfrak{q}}$ be the decomposition field of $\mathfrak{q}$. By Remark 3.50(5), we have $f_{\mathfrak{q} \cap Z_{\mathfrak{q}}} = 1$, so $\kappa(\mathfrak{q} \cap Z_{\mathfrak{q}}) = \kappa(\mathfrak{p})$ on residue fields. Hence, we may and do assume $Z_{\mathfrak{q}} = K$, equivalently $G = G_{\mathfrak{q}}$ by Remark 3.50(4). Note that $L \supset K$ is still a Galois extension.

Next, we show that $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ is normal: Let $\bar{\theta} \in \kappa(\mathfrak{q})$ and choose a lift $\theta \in B$. Then, the minimal polynomial $\mu_{\kappa(\mathfrak{p}),\bar{\theta}} \in \kappa(\mathfrak{p})[T]$ divides the reduction $\overline{\mu_{K,\theta}} := \mu_{K,\theta} \mod \mathfrak{p}$ of the minimal polynomial $\mu_{K,\theta} \in K[T]$, which has coefficients in A by Proposition 3.12(3). Since $L \supset K$ is normal, the polynomial $\mu_{K,\theta}$ decomposes in $L[T]$ in linear factors, which we may assume to be monic and hence automatically lie in $B[T]$. Thus, $\overline{\mu_{K,\theta}}$ decomposes in $\kappa(\mathfrak{q})[T]$ into linear factors and so does its divisor $\mu_{\kappa(\mathfrak{p}),\bar{\theta}}$. As this holds for all elements $\bar{\theta} \in \kappa(\mathfrak{q})$, we see that $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ is normal.

In order to show that the map $\sigma \mapsto \sigma|_B \mod \mathfrak{q}$ is surjective, let $\kappa(\mathfrak{q})_{\mathrm{sep}}$ be the maximal subfield in $\kappa(\mathfrak{q})$ that is separable over $\kappa(\mathfrak{p})$. Then, $\kappa(\mathfrak{q})_{\mathrm{sep}} \supset \kappa(\mathfrak{p})$ is a Galois extension [Sta18, 0EXM] and $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) = \mathrm{Gal}(\kappa(\mathfrak{p})[\bar{\theta}]/\kappa(\mathfrak{p}))$ by [Sta18, 09HS]. Choose a primitive element $\bar{\theta} \in \kappa(\mathfrak{q})_{\mathrm{sep}}$, i.e., $\kappa(\mathfrak{p})[\bar{\theta}] = \kappa(\mathfrak{q})_{\mathrm{sep}}$, see [Sta18, 030N] for the existence of such elements. Let $\bar{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) = \mathrm{Gal}(\kappa(\mathfrak{p})[\bar{\theta}]/\kappa(\mathfrak{p}))$ any element. Choose a lift $\theta \in B$ of $\bar{\theta}$. Then, $\mu_{\kappa(\mathfrak{p}),\bar{\theta}}(\bar{\sigma}(\bar{\theta})) = 0$ implies $\overline{\mu_{K,\theta}}(\bar{\sigma}(\bar{\theta})) = 0$. Since $\mu_{K,\theta}$ decomposes in $B[T]$ into linear factors, there exists some $\theta' \in B$ with $\mu_{K,\theta}(\theta') = 0$ and $\theta' \equiv \bar{\sigma}(\bar{\theta}) \mod \mathfrak{q}$. By normality of $L \supset K$ there exists some $\sigma \in \mathrm{Gal}(L/K)$ with $\theta' = \sigma(\theta)$ and $(\sigma|_B \mod \mathfrak{q})(\bar{\theta}) = \bar{\sigma}(\bar{\theta})$. This shows $(\sigma|_B \mod \mathfrak{q}) = \bar{\sigma}$ and finishes the proof. □

Definition 3.52. With the notation of Proposition 3.51, the kernel

$$I_{\mathfrak{q}} := \ker\left(G_{\mathfrak{q}} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))\right)$$

is called the *inertia group of* $\mathfrak{q}$.

Remark 3.53. The inertia group sits in an exact sequence of groups

$$1 \to I_{\mathfrak{q}} \to G_{\mathfrak{q}} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \to 1$$

by Proposition 3.51.

Remark 3.54. Let $e := e_{\mathfrak{q}}$, $f := f_{\mathfrak{q}}$ and $r = \#\{\mathfrak{q} \mid \mathfrak{p}\}$. Then, one has $\#G = ref$ and $\#G_{\mathfrak{q}} = ef$. In addition, $\#I_{\mathfrak{q}} = e$ and $\#\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) = f$ if $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ is separable, e.g., $\kappa(\mathfrak{p})$ perfect.

Corollary 3.55. *Let $0 \neq \mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ be prime ideals with $\mathfrak{q} \mid \mathfrak{p}$. Assume that $\mathfrak{p}$ unramified in L. Then, $\kappa(\mathfrak{q}) \supset \kappa(\mathfrak{p})$ is a Galois extension and the map $G_{\mathfrak{q}} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ from Proposition 3.51 is an isomorphism.*

Proof. The field extension is separable by unramifiedness and normal by Proposition 3.51, hence it is Galois. Further, we have $\#I_{\mathfrak{q}} = e_{\mathfrak{q}} = 1$ by Remark 3.54 and unramifiedness, i.e., $I_{\mathfrak{q}} = 1$. So, the corollary follows from Remark 3.53. □

The corollary allows to define the so-called *Frobenius substitution*:

Remark 3.56. Let $0 \neq \mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ be prime ideals with $\mathfrak{q} \mid \mathfrak{p}$. Assume that $\mathfrak{p}$ unramified in L and that $\kappa(\mathfrak{p})$ is a finite field. Then, $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ is cyclic generated by the automorphism $x \mapsto x^{\#\kappa(\mathfrak{p})}$. By Corollary 3.55, it has a unique preimage $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}} \in G_{\mathfrak{q}} \subset \mathrm{Gal}(L/K)$, called the *Frobenius substitution*.

For $\mathfrak{q}, \mathfrak{q}'$ lying above $\mathfrak{p}$, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Then, $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}'} = \sigma \mathrm{Frob}_{\mathfrak{p},\mathfrak{q}} \sigma^{-1}$ by Remark 3.50(1). We define the set

$$\mathrm{Frob}_{\mathfrak{p},L} = \mathrm{Frob}_{\mathfrak{p}} := \{\sigma \mathrm{Frob}_{\mathfrak{p},\mathfrak{q}} \sigma^{-1} \mid \sigma \in G\},$$

which is called the *Frobenius conjugacy class of* $\mathfrak{p}$ *(in L)*. If $L \supset K$ is abelian (i.e., $\mathrm{Gal}(L/K)$ is an abelian group), then the set $\mathrm{Frob}_{\mathfrak{p},L}$ has a single element. So, we can consider $\mathrm{Frob}_{\mathfrak{p},L}$ as an element of $\mathrm{Gal}(L/K)$.

Exercise 3.57. In the situation of Remark 3.56, show the following properties:

(1) One has $\mathrm{Frob}_{\mathfrak{p},L} = \{1\}$ if and only if $\mathfrak{p}$ is completely decomposed.
(2) Let $\mathfrak{q} \subset B$ be a prime ideal above $\mathfrak{p}$. Then, one has

$$\#\left\{\begin{matrix}\mathfrak{q} \subset B \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p}\end{matrix}\right\} = \frac{[L:K]}{\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}})}$$

where $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}})$ denotes the order of $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}}$ in $\mathrm{Gal}(L/K)$.
(3) Let $L \supset L' \supset K$ be an intermediate field extension with L'/K Galois. Then, the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K), \sigma \mapsto \sigma|_{L'}$ sends $\mathrm{Frob}_{\mathfrak{p},L}$ to $\mathrm{Frob}_{\mathfrak{p},L'}$.

Exercise 3.58. Let $L = \mathbb{Q}[\sqrt{d}]$ for a square free $d \in \mathbb{Z}$ with $d \equiv 2, 3 \mod 4$, and $\mathrm{Gal}(L/K) = \{1, \sigma\}$ with $\sigma(\sqrt{d}) = -\sqrt{d}$. For all $p \in \mathbb{Z}$, determine when $\mathrm{Frob}_p \in \mathrm{Gal}(L/K)$ is defined and what it is in this case (i.e., either $\mathrm{Frob}_p = 1$ or $\mathrm{Frob}_p = \sigma$).

4. Cyclotomic fields

In this section, we discuss the theory developed so far in some important special cases, namely cyclotomic fields and quadratic fields:

4.1. **Linearly disjoint extensions.** Let $\Omega \supset L_1, L_2 \supset K$ be field extensions. Then, the *composition of* L_1 *and* L_2 is the subfield $L_1L_2 \subset \Omega$ generated by x_1x_2 for all $x_1 \in L_1$, $x_2 \in L_2$. In particular, we have the homomorphism of K-algebras

$$L_1 \otimes_K L_2 \to L_1L_2,\ x_1 \otimes x_2 \mapsto x_1x_2, \tag{4.1}$$

which is surjective.

Definition 4.1. Let $\Omega \supset L_1, L_2 \supset K$ be field extensions. Then, L_1, L_2 are *linearly disjoint over* K if (4.1) is an isomorphism.

Remark 4.2. The subfields L_1, L_2 are linearly disjoint if and only if every K-basis of L_1 is an L_2-basis of L_1L_2. Furthermore, the following properties hold:

(1) If L_1, L_2 are linearly disjoint, then $L_1 \cap L_2 = K$.
(2) Conversely, if $L_1 \cap L_2 = K$, then L_1, L_2 are linearly disjoint whenever $L_1, L_2 \supset K$ are finite Galois extensions. In this case, $L_1L_2 \supset K$ is a finite Galois extension of degree $[L_1 : K] \cdot [L_2 : K]$, and the map $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$, $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$ is an isomorphism (the map is injective and hence an isomorphism by comparing cardinalities).

Proposition 4.3. *Let A be a Dedekind domain with fraction field K. Let $L_1, L_2 \supset K$ be finite, separable field extensions that are linearly disjoint (with respect to some fixed embeddings in an algebraic closure of K). Let B_i for $i = 1, 2$ be the integral closure of A in L_i, and C the integral closure of A in L_1L_2. Let B_1B_2 be the smallest subring of L_1L_2 that contains B_1 and B_2. Then, the following hold:*

(1) For $i = 1, 2$, one has $\Delta_{B_i/A}C \subset B_1B_2$.
(2) Assume that $\Delta_{B_1/A} + \Delta_{B_2/A} = A$. Then, one has $C = B_1B_2$ and

$$\Delta_{C/A} = \Delta_{B_1/A}^{[L_2:K]}\Delta_{B_2/A}^{[L_1:K]}$$

as ideals of A.

Proof. (1):

(2): Since all elements of B_1B_2 are integral over A we have $B_1B_2 \subset C$. Hence, $C = (\Delta_{B_1/A} + \Delta_{B_2/A})C = \Delta_{B_1/A}C + \Delta_{B_2/A}C \subset B_1B_2$ by Part (1). In particular, the isomorphism $L_1 \otimes_K L_2 \xrightarrow{\sim} L_1L_2$, $x_1 \otimes x_2 \mapsto x_1x_2$ induces an isomorphism $B_1 \otimes_A B_2 \cong C$. Thus, $\Delta_{C/A}$ is generated by $\Delta(x_{1,i}x_{2,j} \mid 1 \le i \le n, 1 \le j \le m)$ where $(x_{k,1}, \dots, x_{k,n})$ is a K-basis of L_k contained in B_k for $k = 1, 2$. Interpreting the trace matrix $(\mathrm{Tr}(x_{k,i}x_{k,j}))_{i,j}$ as an endomorphism of B_k... the claim follows from Lemma 4.4 below. □

Lemma 4.4. *Let K be a field and V_1, V_2 finite dimensional K-vector spaces. Then, for all endomorphisms $f_i \colon V_i \to V_i$, $i = 1, 2$, one has the following equality:*

$$\det(f_1 \otimes f_2) = \det(f_1)^{\dim(V_2)} \cdot \det(f_2)^{\dim(V_1)} \tag{4.2}$$

Proof. Choose an algebraic closure $\Omega \supset K$. Then, $\det(f) = \det(f \otimes_K \Omega)$ for any endomorphism f of some finite dimensional K-vector space. So, we may and do assume that $K = \Omega$ is algebraically closed. Further, one computes that (4.2) holds for $f_i = f_i' \oplus f_i''$ whenever its analogue for f_i' and f_i'' holds for $i = 1, 2$. Using the Jordan decomposition we may therefore assume that each f_i consists of a single Jordan block in a suitable basis of V_i. In this case, (4.2) follows from a calculation. This finishes the proof. □

4.2. **Cyclotomic fields.** Let $m \in \mathbb{N}$ with $m \geq 2$. Set $\mathbb{Q}(m) := \mathbb{Q}[\zeta_m]$ where ζ_m is a primitive m-th root of unity.

Reminder 4.5. Let $m = p_1^{e_1} \cdot \ldots p_r^{e_r}$ with $p_1, \ldots, p_r$ being pairwise distinct prime numbers.

(1) One has $\mathbb{Q}(m) = \mathbb{Q}(p_1^{e_1}) \cdots \mathbb{Q}(p_r^{e_r})$ and $\mathbb{Q}(p_1^{e_1}), \ldots, \mathbb{Q}(p_r^{e_r})$ are pairwise linearly disjoint.

(2) The field extension $\mathbb{Q}(m) \supset \mathbb{Q}$ is finite Galois with Galois group

$$(\mathbb{Z}/m)^\times = \prod_{i=1}^r (\mathbb{Z}/p_i^{e_i})^\times .$$

In particular, $[\mathbb{Q}(m) : \mathbb{Q}] = \varphi(m) = \prod_{i=1}^r \varphi(p_i^{e_i})$ and $\varphi(p^e) = p^e - p^{e-1}$ for all prime numbers p and $e \geq 1$.

(3) Let $\phi_m := \mu_{\mathbb{Q},\zeta_m}$ be the minimal polynomial. Then, one has $\phi_m = \prod_{i=1}^r \phi_{p_i^{e_i}}$ and

$$\phi_{p^e} = \frac{T^{p^e} - 1}{T^{p^{e-1}} - 1} = \tau^{p-1} + \tau^{p-2} + \ldots + 1$$

with $\tau := T^{p^{e-1}}$ for all prime numbers p and $e \geq 1$.

Lemma 4.6. *Let $m = p^e$ for some prime number p and some $e \in \mathbb{N}$. Then, for $\zeta = \zeta_m$, one has*

$$\Delta(1, \zeta, \ldots, \zeta^{\varphi(p^e)-1}) = \epsilon p^s$$

for some $\epsilon \in \{\pm 1\}$ and $s = p^{e-1}(ep - e - 1)$.

Proof. By direct calculation, using Lemma 3.42(2), we get

$$\Delta(1, \zeta, \ldots, \zeta^{\varphi(p^e)-1}) = N_{\mathbb{Q}(p^e)/\mathbb{Q}}(\phi_{p^e}'(\zeta)).$$

Further, $(T^{p^{e-1}} - 1)\phi_{p^e} = T^{p^e} - 1$. Taking derivatives and evaluating in ζ gives

$$(\zeta^{p^{e-1}} - 1)\phi_{p^e}'(\zeta) = p^e \zeta^{p^e - 1} = p^e \zeta^{-1}. \tag{4.3}$$

Using the multiplicativity of norms we need to calculate both sides.

We start with the term $\zeta^{p^{e-1}} - 1$ on the left hand side of (4.3). Put $\xi := \zeta^{p^{e-1}}$, which is a primitive p-th root of unity. We calculate

$$N_{\mathbb{Q}(p)/\mathbb{Q}}(\xi - 1) = \prod_{j=1}^{p-1} (\xi^j - 1) = (-1)^{p-1} \prod_{j=1}^{p-1} (1 - \xi^j),$$

which is the same as $= (-1)^{p-1}\phi_p(1) = (-1)^{p-1}p$ because ξ^j, $j = 1, \ldots, p-1$ are the zeros of ϕ_p (use that p is a prime number). Using $N_{\mathbb{Q}(p^e)/\mathbb{Q}} = N_{\mathbb{Q}(p)/\mathbb{Q}} \circ N_{\mathbb{Q}(p^e)/\mathbb{Q}(p)}$, this implies

$$N_{\mathbb{Q}(p^e)/\mathbb{Q}}(\xi - 1) = N_{\mathbb{Q}(p)/\mathbb{Q}}(\xi - 1)^t = (-1)^{(p-1)t} p^t, \tag{4.4}$$

where $t := [\mathbb{Q}(p^e)\colon \mathbb{Q}(p)] = \varphi(p^e)(p-1)^{-1}$.

Now, we consider the right hand side of (4.3). We calculate

$$N_{\mathbb{Q}(p^e)/\mathbb{Q}}(p^e\zeta^{-1}) = p^{e\varphi(p^e)}N_{\mathbb{Q}(p^e)/\mathbb{Q}}(\zeta^{-1}), \tag{4.5}$$

and $N_{\mathbb{Q}(p^e)/\mathbb{Q}}(\zeta^{-1}) \in \{\pm 1\}$. Resubstituting Equations (4.4) and (4.5) in Equation (4.3) implies the lemma. □

Remark 4.7. From $s = p^{e-1}(ep-e-1) \geq 0$ in Lemma 4.6, we see that $s = 0$ if and only if $p = 2$ and $e = 1$.

Proposition 4.8. *Let $m = p^e$ for some prime number p and some $e \in \mathbb{N}$. Let $\zeta = \zeta_m$ be a primitive m-th root of unity. Let B be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(p^e)$. Then, one has*

$$pB = (\lambda)^{\varphi(p^e)} \tag{4.6}$$

where $\lambda := 1-\zeta \in B$. In particular, (λ) is a prime ideal in B with $f_{(\lambda)} = 1$.

Proof. First off, we note that

$$p = \phi_{p^e}(1) = \prod_{\sigma \in (\mathbb{Z}/p^e)^\times} (1-\zeta^\sigma). \tag{4.7}$$

For $\sigma \in (\mathbb{Z}/p^e)^\times$, set $\epsilon_\sigma := \frac{1-\zeta^\sigma}{1-\zeta} = 1+\zeta+\ldots+\zeta^{\sigma-1} \in B$. Then, for $\sigma' := \sigma^{-1}$, we have

$$\epsilon_\sigma^{-1} = \frac{1-\zeta}{1-\zeta^\sigma} = \frac{1-(\zeta^\sigma)^{\sigma'}}{1-\zeta^\sigma} = 1+\zeta^\sigma+\ldots+(\zeta^\sigma)^{\sigma'-1} \in B.$$

This implies $\epsilon_\sigma \in B^\times$. Hence, (4.7) gives

$$pB = \prod_{\sigma \in (\mathbb{Z}/p^e)^\times} (1-\zeta^\sigma)B = \prod_{\sigma \in (\mathbb{Z}/p^e)^\times} (1-\zeta)B = (\lambda)^{\varphi(p^e)},$$

which implies the proposition. □

Theorem 4.9. *For $m \in \mathbb{Z}_{\geq 2}$, let $\zeta := \zeta_m$ be a primitive m-th root of unity. Then, the following hold:*

1. *The ring $\mathbb{Z}[\zeta]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(m)$.*
2. *A prime number $p \in \mathbb{Z}$ is ramified in $\mathbb{Q}(m)$ if and only if either $p \mid m$ for $p \neq 2$ or $p^2 \mid m$ for $p = 2$.*

Proof. (1): Let B be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(m)$. Abbreviate $d := \varphi(m)$.

Special case. Let $m = p^e$ for some prime number $p \in \mathbb{Z}$. By Lemma 4.6, there exists some $s \geq 0$ such that

$$p^s B = \Delta(1,\zeta,\ldots,\zeta^{d-1})B \subset \Delta(1,\zeta,\ldots,\zeta^{d-1})B^\vee \subset \mathbb{Z}[\zeta],$$

where the final inclusion follows from the proof of Proposition 3.19(1) using $B^\vee \subset \mathbb{Z}[\zeta]^\vee$. Set $\lambda := 1-\zeta$. So, $B/\lambda B \cong \mathbb{Z}/p\mathbb{Z}$ by Proposition 4.8 and hence, $\mathbb{Z}+\lambda B = B$. This implies $\mathbb{Z}[\zeta] + \lambda B = B$ and by induction $\mathbb{Z}[\zeta] + \lambda^t B = \lambda B$ for all $t \geq 0$ (multiply previous equation by λ and substitute). Choosing $t = \varphi(p^e)s$ and using Proposition 4.8 gives

$$B = \mathbb{Z}[\zeta] + \lambda^t B = \mathbb{Z}[\zeta] + p^s B = \mathbb{Z}[\zeta].$$

General case. Let $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ for pairwise distinct prime numbers $p_i \in \mathbb{Z}$. Set $\zeta_i := \zeta_{p_i^{e_i}}$ for $i = 1,\ldots,r$. Since the subfields $\mathbb{Q}(p_i^{e_i})$ are pairwise linearly

disjoint in $\overline{\mathbb{Q}}$ and the ideals $\Delta_{\mathbb{Z}[\zeta_i]/\mathbb{Z}} = (p_i^{s_i})$ for some $s_i \geq 0$ are pairwise coprime, Proposition 4.3(2) implies that

$$B = \mathbb{Z}[\zeta_1] \cdot \ldots \cdot \mathbb{Z}[\zeta_r] = \mathbb{Z}[\zeta_1, \ldots \zeta_r] = \mathbb{Z}[\zeta_1 \cdot \ldots \cdot \zeta_r] = \mathbb{Z}[\zeta].$$

(2): By Theorem 3.45, the prime p is ramified in $\mathbb{Q}(m)$ if and only if $p \mid \Delta_{\mathbb{Z}[\zeta]/\mathbb{Z}}$ if and only if $p \mid \Delta_{\mathbb{Z}[\zeta_i]/\mathbb{Z}}$, by Proposition 4.3(2), for some $i = 1, \ldots, r$. Finally, Remark 4.7 finishes the proof. □

Exercise 4.10. Let $B = \mathbb{Z}[\zeta]$ where $\zeta = \zeta_{\ell^n}$ is a primitive ℓ^n-th root of unity for some prime number $p \in \mathbb{Z}$ and some $n \in \mathbb{N}$. For a prime number $p \in \mathbb{Z}$ define the natural numbers $e_p := e_{\mathfrak{q}}$, $f_p := f_{\mathfrak{q}}$ for some prime ideal $\mathfrak{q} \subset B$ with $\mathfrak{q} \mid (p)$ and

$$r_p := \# \left\{ \begin{matrix} \mathfrak{q} \subset B \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p} \end{matrix} \right\}.$$

Show the following properties:

(1) One has

$$e_p = \begin{cases} 1 & \text{if } p \neq \ell, \\ \varphi(\ell^n) & \text{if } p = \ell. \end{cases}$$

(2) One has

$$f_p = \begin{cases} \min\{f \geq 1 \mid p^f \equiv 1 \mod \ell^n\} & \text{if } p \neq \ell, \\ 1 & \text{if } p = \ell. \end{cases}$$

(3) One has

$$r_p = \begin{cases} \frac{\varphi(\ell^n)}{f_p} & \text{if } p \neq \ell, \\ 1 & \text{if } p = \ell. \end{cases}$$

4.3. **Quadratic fields.**

Proposition 4.11. *Let $\ell \in \mathbb{N}$ be an odd prime number, $\ell^\flat := (-1)^{\frac{\ell-1}{2}}\ell$ and $\zeta = \zeta_\ell$ a primitive ℓ-th root of unity. Then, there exists a unique intermediate field*

$$\mathbb{Q}[\zeta] \supset K \supset \mathbb{Q}$$

with $[K : \mathbb{Q}] = 2$. Furthermore, one has $K = \mathbb{Q}[\sqrt{\ell^\flat}]$.

Proof. The field extension $\mathbb{Q}[\zeta] \supset \mathbb{Q}$ is Galois with Galois group $\mathbb{Z}/(\ell-1)\mathbb{Z}$, which has a unique subgroup H of index 2. Galois theory [Sta18, 09DW] implies that the fixed field $K = \mathbb{Q}[\zeta]^H$ is the unique intermediate extension with of degree 2 over $\mathbb{Q}$.

It remains to show $K = \mathbb{Q}[\sqrt{\ell^\flat}]$. Since $K \supset \mathbb{Q}$ is quadratic, there exists a square free integer $d \in \mathbb{Z}$ such that $K = \mathbb{Q}[\sqrt{d}]$ (use quadratic substitution to modify the minimal polynomial of some element in $K \backslash \mathbb{Q}$). Then, a prime number $p \in \mathbb{Z}$ is ramified in K if and only if

$$p \text{ divides } \begin{cases} 4d & \text{if } d \equiv 2, 3 \mod 4, \\ d & \text{if } d \equiv 1 \mod 4. \end{cases}$$

by Example 3.39 and Exercise 3.40. Further, if p is ramified in K, then it is ramified in $\mathbb{Q}[\zeta]$ and so $p \mid \ell$ by Theorem 4.9(2). This gives the conditions $d = \pm\ell$ and $d \equiv 1 \mod 4$, which imply $d = (-1)^{\frac{\ell-1}{2}}\ell = \ell^\flat$. □

Proposition 4.12. *Let $p, \ell \in \mathbb{N}$ be distinct prime numbers with ℓ odd, $\ell^\flat := (-1)^{\frac{\ell-1}{2}}\ell$ and $\zeta := \zeta_\ell$. Then, the following are equivalent:*

(1) *The prime p is completely decomposed in $\mathbb{Q}[\sqrt{\ell^\flat}]$.*
(2) *The number*

$$r_p := \#\left\{\begin{array}{l}\mathfrak{q} \subset \mathbb{Z}[\zeta] \text{ prime} \\ \text{ideal with } \mathfrak{q} \mid \mathfrak{p}\end{array}\right\}.$$

is even.
(3) *One has $(\frac{p}{\ell}) = 1$ for the Legendre symbol, i.e., $p \in \mathbb{F}_\ell$ is a square.*

Furthermore, if p is odd, then (1), (2) and (3) are equivalent to the following:

(4) *One has $(\frac{\ell^\flat}{p}) = 1$.*

Proof. Write $K := \mathbb{Q}[\sqrt{\ell^\flat}] \subset \mathbb{Q}[\zeta] =: L$. Let A and B be the integral closure of $\mathbb{Z}$ in K and L respectively. Then, B is the integral closure of A in L and we have $\mathbb{Z} \subset A \subset B = \mathbb{Z}[\zeta]$ where the last equality holds by Theorem 4.9(1). Let $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset B$ be prime ideals with $(p) \subset \mathfrak{p} \subset \mathfrak{q}$.

(1) $\iff$ (2): The number r_p agrees with the index of $\mathrm{Gal}(L/\mathbb{Q})_\mathfrak{q}$ in $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$, and is even if and only if $\mathrm{Gal}(L/\mathbb{Q})_\mathfrak{q}$ is contained in the unique subgroup $\mathrm{Gal}(\mathbb{Q}[\zeta]/K)$ of index 2. Equivalently, for each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ with $\sigma(\mathfrak{q}) = \mathfrak{q}$ one has $\sigma|_K = \mathrm{id}_K$. As $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ is surjective this is equivalent to $\mathrm{Gal}(K/\mathbb{Q})_\mathfrak{p} = 1$, which is equivalent to (p) being completely decomposed in K.

(2) $\iff$ (3): The number r_p is even if and only if $\frac{\ell-1}{f}$ is so where $f = \min\{f \geq 1 \mid p^f \equiv 1 \mod \ell\}$ by Exercise 4.10(2). Equivalently, $f \mid \frac{\ell-1}{2}$, which holds if and only if $p^{\frac{\ell-1}{2}} \equiv 1 \mod \ell$, i.e., $(\frac{p}{\ell}) = 1$.

(1) $\iff$ (4.12): One has $\ell^\flat \equiv 1 \mod 4$ for all odd prime numbers $\ell \in \mathbb{N}$. We conclude using Exercise 3.31(1). □

Theorem 4.13 (Quadratic reciprocity law)**.** *Let $p, \ell \in \mathbb{N}$ be distinct, odd prime numbers. Then, the following hold:*

(1) *One has $(\frac{p}{\ell})(\frac{\ell}{p}) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$, i.e.,*

$$\left(\frac{p}{\ell}\right) = \begin{cases} -\left(\frac{\ell}{p}\right) & \text{if } p \equiv \ell \equiv 3 \mod 4, \\ \left(\frac{\ell}{p}\right) & \text{otherwise.} \end{cases}$$

(2) *One has*

$$\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}}.$$

Proof. (1): One has $(\frac{p}{\ell}) = (\frac{\ell^\flat}{p})$ by Proposition 4.12. This is equal to

$$\left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\frac{\ell}{p}\right).$$

(2): One has $(\frac{2}{\ell}) = 1$ if and only if (2) splits in $\mathbb{Q}[\sqrt{\ell^\flat}]$ if and only if $\ell^\flat \equiv 1 \mod 8$ if and only if $\ell \equiv \pm 1 \mod 8$, which is equivalent to $\frac{\ell^2-1}{8}$ being even. □

Exercise 4.14. Show that 7600 is not a square modulo 4049.

5. Completions

The notion of completion may be familiar from basic analysis. One common construction of the real numbers is to complete the rationals $\mathbb{Q}$. One considers the space of all Cauchy sequences in $\mathbb{Q}$ (up to equivalence), and obtains a complete metric space, which is the real line $\mathbb{R}$. In this section, we discuss the general notion of completion. To any (pseudo-)metric space X you can attach a space $\widehat{X}$ in which every Cauchy sequence converges. Discrete valuations give rise to absolute values on fields, and the construction of $\mathbb{R}$ from $\mathbb{Q}$ is a special case of completing a valued field with respect to a given absolute value. For example, the discrete valuation v_p on $\mathbb{Q}$ gives rise to the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$, and the completion is $\mathbb{Q}_p$, the field of p-adic numbers. Here is a quick overview of the topics.

5.1. Topological groups, rings and fields.

Definition 5.1. (1) A *topological group* G is a topological space which is a group with operation $\cdot$ and for which

$$G \times G \to G, (x, y) \mapsto x \cdot y$$

and

$$\text{inv} : G \to G, x \mapsto x^{-1}$$

are continuous.

(2) A *topological ring* R is a topological space which is a ring and for which addition and multiplication are continuous. Note that this is implies $(R, +)$ is a topological group, as $-x = x \cdot (-1)$.

(3) A *topological field* K is a topological space which is a field, and such that K is a topological ring, and $K^\times \to K^\times, x \mapsto x^{-1}$ is continuous for the subspace topology on $K^\times$.

Example 5.2. (1) The real numbers $\mathbb{R}$ with the usual topology form a topological field for the usual addition and multiplication.

(2) Similarly, $\mathbb{C}$ is a topological field

(3) Let $G = (\mathbb{R}, +)$, but we endow $\mathbb{R}$ with the topology generated by half-open invervals $[a, b)$. This is called the Sorgenfrey line, and is not a topological group. The addition map is continuous, but inversion is not.

(4) Let X be a topological space, and $C(X)$ the set of continuous maps $X \to \mathbb{R}$. Then, $C(X)$ is a ring via pointwise addition and multiplication. We can define a topology on $C(X)$ as follows. We take the unique topology in which convergent nets are those nets which converge pointwise. In particular, a sequence $(f_n)_n$ in $C(X)$ is convergent if it converges pointwise. Here, (f_n) converges pointwise to $f \in C(X)$ if for all $x \in X$, $\lim_{n\to\infty} f_n(x) = f(x)$.

Remark 5.3. Let G be a group with neutral element $e \in G$. Let $\mathcal{U}$ be a set of subset of G such that the following holds.

a) We have $e \in U$ for all $U \in \mathcal{U}$.

b) If $U, V \in \mathcal{U}$, then $U \cap V \in \mathcal{U}$.
c) For all $U \in \mathcal{U}$ exists a $V \in \mathcal{U}$ such that $V \cdot V := \{vv' \mid v, v' \in V\} \subset U$.
d) For all $U \in \mathcal{U}$ exists a $V \in \mathcal{U}$ such that $V^{-1} := \{v^{-1} \mid v \in V\} \subset U$.
e) For all $U \in \mathcal{U}$ and $g \in G$, there exists a $V \in \mathcal{U}$ such that $gVg^{-1} \subset U$.

Then there exists a unique topology on G making it into a topological group such that $\mathcal{U}$ is a neighborhood basis of e. This means $e \in W \subset G$ is a neighborhood of e if and only if there is a $U \in \mathcal{U}$ with $U \subset W$. Here, recall that a neighborhood of e is any subset of G containing an open neighborhood of e (an open set containing e).

Indeed, for any $g \in G$ we can translate $\mathcal{U}$ to obtain a collection $\mathcal{U}_g$ satisfying appropriate axioms as above. We obtain a map $g \mapsto \mathcal{U}_g$. It is a general fact that a topology on a set can be given by assigning a neighborhood basis to each point. You can then check that multiplication and inversion are continuous for this topology.

Moreover, if H is another topological group and $\varphi : H \to G$ is a group homomorphisms, then φ is continuous if and only if $\varphi^{-1}(U)$ is a neighborhood of $e \in H$ for all $U \in \mathcal{U}$.

Example 5.4. Let $(G, +)$ be an abelian group, and let $G \supset G_0 \supset G_1 \supset ... \supset G_n \supset ...$ be a descending chain of subgroups. There is a unique topology on G making it a topological group such that $\mathcal{U} := \{G_n \mid n \geq 0\}$ is a neighborhood basis of e. Moreover, all G_n are open subgroups. Indeed, we can find an open U with $e \in U \subset G_n$, and hence $\bigcup_{g \in G_n} gU = G_n$ is open.

Definition 5.5. A *pseudo-metric* d on a set X is a map $d : X \times X \to \mathbb{R}_{\geq 0}$ such that

a) $d(x, x) = 0$ for all $x \in X$,
b) $d(x, y) = d(x, y)$ for all $x, y \in X$, and
c) $d(x, z) \leq d(x, y) + d(x, z)$ for all $x, y, z \in X$.

A pseudo-metric on X induces a topology generated by open balls $B_r(x) = \{y \in X \mid d(y, x) < r\} \subset X$, where $r \in \mathbb{R}_{>0}$ (any set which is a union of open balls is open). A pseudo-metric is a metric if $d(x, y) = 0$ implies $x = y$.

We can define a pseudo-metric on G as follows. Let $c \in \mathbb{R}$ with $0 < c < 1$, and let $d(g, h) = c^n$, where

$$n = \sup\{n \geq 0 \mid g - h \in G_n\} \in \mathbb{Z}_{\geq 0} \cup \{\pm\infty\}.$$

Here, $\sup(\emptyset) = -\infty$, and we define $c^{-\infty} := 1, c^{\infty} := 0$. Then, the topology induced by d agrees with the topology induced by the collection $\mathcal{U}$ as before. Moreover, note that for $g, h \in G$ we have $d(g, h) = 0$ if and only if $g - h \in \bigcap_{n \geq 0} G_n$. Therefore, d is a metric if and only if $\bigcap_{n \geq 0} G_n = \{0\}$, and this happens if and only if G is Hausdorff.

Example-Definition 5.6. Let A be a ring, and $I \subset A$ and ideal. Endow $(A, +)$ with the topology induced by $I^0 = A \supset I \supset I^2 \supset ....$ This makes A a topological ring, and this topology is called the I-adic topology on A. Note that A with the I-adic topology is Hausdorff if and only if $\bigcap_{n \geq 0} I^n = \{0\}$. For example, if A is noetherian, if I is contained in the Jacobson radical this condition holds, cf. 2.9. If A is Noetherian and local, then this automatically holds for any ideal.

5.2. **Absolute values.**

Definition 5.7. Let K be a field. An absolute value on K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

a) $|x| = 0$ if and only if $x = 0$,
b) $|xy| = |x||y|$ for all $x, y \in K$, and
c) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

The last condition is called the *triangle inequality*. We call $|\cdot|$ *non-archimedean* if the stronger condition

c') $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$

holds.

Remark 5.8. (1) By a) and b), the map $|\cdot| : K^\times \to \mathbb{R}_{>0}$ is a group homomorphism.
(2) If $\zeta \in K$ is a root of unity, then by the first remark we have $|\zeta| = 1$. This implies $|-1| = 1$, and hence $|-x| = |x|$ for all $x \in K$.

Example 5.9. (1) The usual absolute values on $\mathbb{R}$ and $\mathbb{C}$.
(2) Let L be a field with absolute value $|\cdot|_L$, and $\sigma : K \hookrightarrow L$ an embedding of fields. Then we obtain an absolute value on K by defining $|x|_{K,\sigma} := |\sigma(x)|_L$ for all $x \in K$.
(3) Let K be a field with a valuation $v : K \to \mathbb{R} \cup \{\infty\}$. Let $0 < c < 1$ be a real number. Then, $x \mapsto |x|_v := c^{v(x)}$ is a non-archimedean absolute value. Conversely, let $|\cdot| : K \to \mathbb{R}_{\geq 0}$ be a non-archimedean absolute value. Then,

$$v : K \to \mathbb{R} \cup \{\infty\}$$
$$x \mapsto \log_c |x|$$

is a valuation. Moreover, v is a discrete valuation if and only if $|K^\times|_v \subset \mathbb{R}^\times$ is a non-trivial discrete subgroup.
(4) The *trivial absolute value* is defined as follows. Let K be a field and put

$$|x| = \begin{cases} 0, x = 0 \\ 1, x \neq 0. \end{cases}$$

For example, if K is finite, then there is only the trivial absolute value.

Remark 5.10. Let K be a field with absolute value $|\cdot|$. Then, we can define a metric on K by putting $d(x, y) = |x - y|$ for all $x, y \in K$. This induces a Hausdorff topology, and turns K into a topological field (exercise).

Proposition 5.11. *Let K be a field with non-trivial absolute values $|\cdot|_1, |\cdot|_2$. The following are equivalent*

(i) The absolute values $|\cdot|_1$ and $|\cdot|_2$ induce the same topology on K.
(ii) For all $x \in K$, we have $|x|_1 < 1$ if and only if $|x|_2 < 1$.
(iii) There is a real number $a > 0$ such that $|\cdot|_2 = |\cdot|_1^a$.

If any of these conditions hold we call $|\cdot|_1$ and $|\cdot|_2$ equivalent.

Proof. (i) implies (ii): Let $x \in K$. A sequence (x_n) in K converges to $x \in K$ (with respect to $|\cdot|_1$) if for all $\varepsilon > 0$ there is an $N > 0$ such that $|x_n - x|_1 < \varepsilon$ for every $n \geq N$. Topologically, this can be reformulated as follows. For every open neighborhood U of x there exists an $N > 0$ such that $x_n \in U$ for all $n > N$. Note

that since K is Hausdorff, limit points are unique. Because $|\cdot|_1$ and $|\cdot|_2$ induce the same topology, convergence with respect to $|\cdot|_1$ and with respect to $|\cdot|_2$ agrees.

We apply this to the sequence (x^n), so we find that $\lim |x^n|_1 = 0$ if and only if $\lim |x^n|_2 = 0$. This implies $|x|_1 < 1$ if and only if $|x|_2 < 1$.

(ii) implies (iii): Let $y \in K$ with $|y|_1 > 1$. Then by (ii) for y^{-1} we find $|y|_2 > 1$. Hence there is an $a > 0$ with $|y|_2 = |y|_1^a$ (let $a = \frac{\log |y|_2}{\log |y|_1} > 0$). Now let $x \in K^\times$ be arbitrary. Then we can find $b \in \mathbb{R}$ with $|x|_1 = |y|_1^b$ (take a logarithm again, which is not necessarily $b > 0$ now).

We claim that $|x|_2 = |y|_2^b$. Assume this claim is proven. Then $|x|_2 = |y|_2^b = |y|_1^{ab} = |x|_1^a$ proving (ii) implies (iii). So it remains to prove the claim.

Let $\frac{m}{n} > b$ with $m, n \in \mathbb{Z}$ and $n > 0$. Then we have $|x|_1 < |y|_1^{m/n}$, implying $|x^n/y^m|_1 < 1$. By (ii) we find that $|x^n/y^m|_2 < 1$, which is equivalent to $|x|_2 < |y|_2^{m/n}$. We can take a limit of rational numbers converging to b from above to conclude $|x|_2 \leq |y|_2^b$.

On the other hand, we can repeat this argument with $\frac{m}{n} < b$ converging to b from below. This shows $|x|_2 \geq |y|_2^b$, proving the claim.

(iii) implies (i): This is clear now, because the set of open balls in K agrees when (iii) holds. □

Proposition 5.12. *Let K be a field, $|\cdot|$ an absolute value on K. Then the following are equivalent.*

(i) The absolute value $|\cdot|$ is non-archimedean,
(ii) the set $\{|m \cdot 1| \mid m \in \mathbb{Z}\} \subset \mathbb{R}_{\geq 0}$ is bounded, and
(iii) for all $s > 0$, $|\cdot|^s$ is an absolute value.

Exercise 5.13. Prove the above proposition.

The following is immediate.

Corollary 5.14. *Fields of positive characteristic have only non-archimedean absolute values.*

Exercise 5.15. Let K be a field with non-archimedean absolute value $|\cdot|$. Recall that a sequence $(x_n) \subset K$ is a *Cauchy sequence* if the following holds. For all $\varepsilon > 0$ there is an $N > 0$ such that for all $n, m > N$ we have $|x_n - x_m| < \varepsilon$.

(1) Let (x_n) be a sequence in K. Show that (x_n) is Cauchy if and only if $\varepsilon > 0$ there is an $N > 0$ such that for all $n > N$ we have $|x_n - x_{n+1}| < \varepsilon$. Show moreover that $(\sum_{m=1}^n x_m)_n$ is Cauchy if and only if (x_n) converges to 0 in K. Note that this is in stark contrast to the archimedean situation: the sequence $1/n$ goes to 0 in $\mathbb{R}$ with respect to usual absolute value, but the corresponding series is divergent.
(2) Let $x, y \in K$, and show that if $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

Example-Definition 5.16. Let $K = \mathbb{Q}$, and define absolute valies on $\mathbb{Q}$ as follows.

(1) We let $|\cdot|_\infty$ be the usual absolute value on $\mathbb{Q}$.
(2) For a prime p we define $|x|_p := p^{-v_p(x)}$ where $x = \pm p^{v_p(x)} p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ with $p_i \neq p$ is the prime decomposition of $x \in \mathbb{Q}$. We call $|\cdot|_p$ the p-adic absolute value on $\mathbb{Q}$.

Theorem 5.17 (Ostrowski)**.** *(1) Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Then if $|\cdot|$ is archimedean, it is equivalent to $|\cdot|_\infty$. If $|\cdot|$ is non-archimedean, there is a unique prime p such that $|\cdot|$ is equivalent to $|\cdot|_p$.*

(2) *Let $(K, |\cdot|)$ be a complete valued field (i.e. every Cauchy sequence in K converges), and assume $|\cdot|$ is archimedean. Then there exists an isomorphism of fields $\sigma : K \cong \mathbb{R}$ or $\sigma : K \cong \mathbb{C}$ such that $|\sigma(x)|_\infty = |x|^s$ for some real number $0 < s < 1$.*

Proof. The proofs can be found in [Bou98], Chapter VI, §6.3. Prop. 9 and Chapter VI, §6.4., Theorem 2. □

Exercise 5.18. Show that the sequence $(a_n) = (3, 34, 334, 3334, ...)$ of integers converges to $2/3$ in $\mathbb{Q}$ with respect to the 5-adic absolute value $|\cdot|_5$. Hint: Show $3a_n - 2$ converges to 0.

Theorem 5.19 (Product formula)**.** *For all $x \in \mathbb{Q}^\times$ one has*

$$\prod_{v \text{ prime or } v=\infty} |x|_v = 1.$$

Proof. First note that only finitey many v have $|x|_v \neq 1$ for any given $x \in \mathbb{Q}^\times$. Indeed, only when a prime p divides the numerator or denominator in the reduced expression for x do we have $|x|_v \neq 1$.

Absolute values are multiplicative, so by the prime decomposition the claim reduces to $x = -1$ or $x = p$ for a prime p. In these cases it is clear. □

The next theorem will play a role later when we discuss local-global principles. Applied to p-adic absolute values, it allows for the selection of an element with specified divisibility properties.

Theorem 5.20 (Weak approximation)**.** *Let K be a field, and $|\cdot|_1, ..., |\cdot|_n$ be non-trivial and pair-wise inequivalent absolute values. Moreover, let $a_1, ..., a_n \in K$. Then, for all $\varepsilon > 0$ there exists an $x \in K$ such that $|x - a_i|_i < \varepsilon$ for all $i = 1, .., n$.*

Proof. We proceed in three steps.

i) Claim: There exists $a \in K$ such that $|a|_1 > 1$, and $|a|_i < 1$ for $i = 2, ..., n$. We prove this by induction on n. We start with $n = 2$. Then, since $|\cdot|_1, |\cdot|_2$ are inequivalent, there exist $b, c \in K$ such that $|b|_1 < 1, |b|_2 \geq 1$ and $|c|_1 \geq 1, |c|_2 < 1$. Then $a = \frac{c}{b}$ satisfies the claim for $n = 2$.

Now assume $n \geq 3$. By induction hypothesis there exists $b \in K$ such that $|b|_1 > 1$ and $|b|_i < 1$ for $i = 2, ..., n-1$. Moreover, by the argument for $n = 2$ above we can find $c \in K$ such that $|c|_1 > 1$ and $|c|_n < 1$. Now there are three cases.

If $|b|_n < 1$, we can put $a = b$ and we are done.

If $|b|_n = 1$, since $|b|_i < 1$ for $i = 2, ..., n-1$, we can find a large r such that $|cb^r|_i < 1$ for $i = 2, ..., n-1$. We let $a = cb^r$ for such a large r. Moreover, since $|c|_n < 1$, we have $|cb^r|_n < 1$ as well.

If $|b|_n > 1$, observe that $\frac{b^r}{1+b^r}$ converges to 0 if $|b|_i < 1$ and to 1 if $|b|_i > 1$. We can therefore define $a := c\frac{b^r}{1+b^r}$ for a large enough r.

ii) Claim: for all $\varepsilon > 0$ exists a $b \in K$ such that $|b - 1|_1 < \varepsilon$ and $|b|_i < \varepsilon$ for $i = 2, ..., n-1$.

We choose a as in i) and define $b_r := \frac{a^r}{1+a^r}$. Note that for any $x \in K$ and any absolute value $|\cdot|$ we have $|x| - 1 = |x + 1 - 1| - 1 \leq |x + 1|$ by the triangle inequality. If $|x| - 1 > 0$, this is equivalent to $\frac{1}{|x+1|} \leq \frac{1}{|x|-1}$. We apply this to $x = a^r$ and $|\cdot| = |\cdot|_1$, and find that

$$|b_r - 1| = \frac{1}{|1 + a^r|_1} \leq \frac{1}{|a|_1^r - 1}.$$

The latter converges to 0.

For $i = 2, ..., n$ we have $|a|_i < 1$ and we conclude similarly that

$$|b_r|_i = \frac{|a|_i^r}{|1 + a^r|_i} \leq \frac{|a|_i^r}{1 - |a|_i^r},$$

which converges to 0 as well. We can therefore choose r large enough so that it satisfies the requirement of the claim for a given ε.

iii) We now prove the Theorem. Let $\varepsilon > 0$. Assume that all a_i are non-zero. When some a_i vanishes, the following argument needs only slight modification, and we leave it to the reader. By ii) we can choose $b_1, ..., b_n$ such that $|b_i - 1|_i < \frac{\varepsilon}{n|a_i|_i}$, and such that $|b_i|_j < \frac{\varepsilon}{n|a_j|_i}$ if $i \neq j$. We then define $x := a_1 b_1 + ... + a_n b_n$. Then by the triangle inequality we find that

$$\begin{aligned} |x - a_i|_i &\leq |a_i b_i - a_i|_i + \sum_{j \neq i} |a_j b_j|_i \\ &\leq |a_i|_i |b_i - 1|_i + \sum_{j \neq i} |a_j|_i \ |b_j|_i \\ &< \varepsilon. \end{aligned}$$

This proves the claim. □

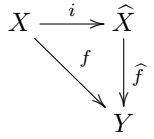
5.3. **Completion.** We define completions in a general setting, but we omit some of the proofs. Recall the following.

Definition 5.21. Let X and Y be sets endowed with pseudo-metrics d_X and d_Y (hence also with topologies). We call X and Y pseudo-metric spaces. A map $f : X \to Y$ is called uniformly continuous if for all $\varepsilon > 0$ there exists a $\delta > 0$ such that for all $x, x' \in X$ with $d_X(x, x') < \delta$ we have $d_Y(i(x), i(x')) < \varepsilon$.

Theorem 5.22 (Completion of pseudo-metric spaces)**.** *Let X be a set with a pseudo-metric $d : X \times X \to \mathbb{R}_{\geq 0}$, and endow it with the induced topology.*

(1) A sequence (x_n) in X is called a Cauchy sequence if and only if for all $\varepsilon > 0$ there exists an $N > 0$ such that for all $n, m > N$ we have $d(x_n, x_m) < \varepsilon$. We call (X, d) complete *if X is Hausdorff and every Cauchy sequence in X converges.*

(2) There exists a complete Hausdorff metric space $(\widehat{X}, \widehat{d})$ and a uniformly continuous map $i : X \to \widehat{X}$ such that given any uniformly continous map $f : X \to Y$ to a complete metric space Y there exists a unique uniformly continous map $\widehat{f} : \widehat{X} \to Y$ making the diagram



commute.

(3) The pair $(\widehat{X}, i)$ is unique up to unique isomorphism and is called the completion *of X.*

(4) For all $x, y \in X$ one has $d(x, y) = \widehat{d}(i(x), i(y))$. In particular, $i(x) = i(y)$ if and only if $d(x, y) = 0$. Therefore X is Hausdorff if and only if i is injective.

(5) *The subspace $i(X) \subset \widehat{X}$ is dense and X carries the inverse image topology, i.e. open subsets of X are of the form $i^{-1}(V)$ for $V \subset \widehat{X}$ open.*
(6) *Let X, Y be pseudo-metric spaces, and $f : X \to X'$ be uniformly continuous. Then there exists a unique uniformly continuous map $\widehat{f} : \widehat{X} \to \widehat{Y}$ making the diagram*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle i_X}\downarrow & & \downarrow{\scriptstyle i_Y} \\ \widehat{X} & \xrightarrow{\widehat{f}} & \widehat{Y} \end{array}$$

commute.
(7) *Let X, Y be pseudo-metric spaces. Then $(X \times Y)^\wedge \cong \widehat{X} \times \widehat{Y}$.*

Proof. The proof is omitted, we refer to [Bou95, Chapter II, §3.7]. □

Theorem 5.23 (Completion of topological rings)**.** *Let A be a ring, not necessarily commutative, endowed with a pseudo-metric which makes A a topological ring. Then addition and multiplication $A \times A \to A$ are continuous and induce on $\widehat{A}$ the structure of a topological ring such that $i : A \to \widehat{A}$ is a ring homomorphism. We call $\widehat{A}$ the* completion *of A. Moreover, the following holds.*

(1) *If A is commutative, so is its completion $\widehat{A}$.*
(2) *Let K be a topological field, and assume that for all Cauchy sequences (x_n) with $x_n \neq 0$ for all n and for which 0 is not an accumulation point, the sequence (x_n^{-1}) is also Cauchy. Then, $\widehat{K}$ is a complete topological field and $\widehat{K}^\times$ with the induced metric is is a complete topological group.*

Proof. The reference is [Bou95, Chapter III, §6.5, §6.8]. □

Example 5.24 (Main Example I)**.** Let K be a field and $|\cdot|$ an absolute value on K. We call $(K, |\cdot|)$ a valued field. There exists a complete valued field $(\widehat{K}, |\cdot|)$ and a uniformly continuous injection $i : K \to \widehat{K}$ such that $|i(x)| = |x|$ for all $x \in K$ and such that $i(K) \subset \widehat{K}$ dense.

Proof. We only need to show that $\widehat{K}$ is a field. Let (x_n) be a Cauchy sequence in K with $x_n \neq 0$ such that 0 is not an accumulation point of x_n. Then, by definition there exists a real number $c > 0$ such that $|x_n| > c$ for all n. Let $\varepsilon > 0$ and $N > 0$ such that $|x_n - x_m| < \varepsilon$ for all $n, m \geq N$. Then

$$|x_n^{-1} - x_m^{-1}| = |x_n^{-1}(x_n - x_m)x_m^{-1}| = |x_n - x_m||x_n|^{-1}|x_m|^{-1} < \frac{\varepsilon}{c^2}$$

for all $n, m \geq N$. This implies that (x_n^{-1}) is a Cauchy sequence. □

Moreover, the absolute value $|\cdot|$ on K is non-archimedean if and only if the absolute value $|\cdot|$ on $\widehat{K}$ is non-archimedean. In this case the following holds.

(1) The map $|\cdot| : K^\times \to \mathbb{R}_{>0}$ is continuous for the discrete topology on $\mathbb{R}_{>0}$.

Proof. We need to show that every fiber (i.e. preimage of a point) of $|\cdot|$ is open. Let $x_0 \in K^\times$, and let $\varepsilon := |x_0| > 0$. Then $x \in B_\varepsilon(x_0)$ if and only if $|x - x_0| < |x_0|$. By Exercise 5.15, (2), this implies $|x| = |x_0|$. This implies that the fiber of $|\cdot|$ over ε contains an open ball around each of its points, hence it is open. □

(2) We have $|K^\times| = |\widehat{K}^\times| \subset \mathbb{R}_{>0}$. In particular, $|\cdot|$ on K is discrete if and only if $|\cdot|$ on $\widehat{K}$ is discrete.

Proof. Let $x \in \widehat{K}^\times$, then we can find a Cauchy sequence (x_n) in $K^\times$ converging to x. Since $|\cdot|$ is continuous for the discrete topology on $\mathbb{R}_{>0}$, we have $\lim_n |x_n| = |x|$. A convergent sequence in the discrete topology eventually stabilizes, so there is a large $k >> 0$ such that $|x| = |x_k| \in |K^\times|$. □

(3) The subring $O_K := \{x \in K \mid |x| \leq 1\}$ is an open and closed local subring, and $\widehat{O}_K := \{x \in \widehat{K} \mid |x| \leq 1\}$ is the closure of O_K in $\widehat{K}$. Moreover, $\mathfrak{m} := \{x \in K \mid |x| < 1\}$ is the maximal ideal of O_K, and $\widehat{\mathfrak{m}} := \{x \in \widehat{K} \mid |x| < 1\}$ is the closure of $\mathfrak{m}$ in $\widehat{K}$. We have that $O/\mathfrak{m} \cong \widehat{O}/\widehat{\mathfrak{m}}$.

Proof. We prove the isomorphism. Injectivity of $O/\mathfrak{m} \to \widehat{O}/\widehat{\mathfrak{m}}$ follows from injectivity of $O \to \widehat{O}$. We prove the map is surjective. For that, we need to show that $\widehat{O}_K = O_K + \mathfrak{m}$. Let $x \in \widehat{O}_K$, and choose $y \in O_K$ with $|x - y| < 1$. This is possible since $O_K \subset \widehat{O}_K$ is dense. Then we have get $x = y + (x - y)$ and $x - y \in \widehat{\mathfrak{m}}$. □

Example 5.25 (Main Example II)**.** Let A be a ring and $I \subset A$ a finitely generated ideal. Endow A with the I-adic topology, i.e. the unique topology making A into a topological ring such that $(I^n)_{n \geq 1}$ is a neighborhood basis of 0 in A. Note that every I^n is open in this topology. In this case, $\widehat{A}$ can be described as follows. Consider the inverse system

$$\ldots \xrightarrow{\pi} A/I^{n+1} \xrightarrow{\pi} A/I^n \xrightarrow{\pi} \ldots \xrightarrow{\pi} A/I$$

where the maps are the natural projections. Recall that the inverse limit of the above inverse system is

$$\lim_n A/I^n := \{(a_n)_{n \geq 1} \mid a_n \in A/I^n, \pi(a_{n+1}) = a_n \text{ for all } n \geq 1\}$$

This limit carries the subspace topology for the inclusion $\lim_n A/I^n \subset \prod_{n \geq 1} A/I^n$, where each A/I^n carries the discrete topology, and the product carries the product topology.

Proposition 5.26. *In this situation, there is a natural isomorphism $\widehat{A} \cong \lim_n A/I^n$. In addition, the ring A is I-adically complete (i.e. complete with respect to the I-adic topology) if and only if $A \cong \lim_{n \geq 1} A/I^n$.*

Proof. We sketch a proof. The completion of A is the set of all Cauchy sequences in A. Denote this set by $\mathfrak{C}(A)$. Moreover, denote by $\mathfrak{C}_0(A)$ the set of all Cauchy sequences converging to 0. The set of Cauchy sequences is a ring, and $\mathfrak{C}_0(A)$ is an ideal in this ring. Then the completion is $\widehat{A} = \mathfrak{C}(A)/\mathfrak{C}_0(A)$. In the I-adic topology, a sequence (x_n) in A is Cauchy if and only if for all $k \in \mathbb{Z}_{\geq 0}$ there is an $N > 0$ such that for all $n, m \geq N$ we have $x_n - x_m \in I^k$.

We want to define a map $\mathfrak{C}(A)/\mathfrak{C}_0(A) \to \lim A/I^n$. In order to do so, we give a map $\mathfrak{C}(A)/\mathfrak{C}_0(A) \to A/I^k$ for every k. These maps are constructed as follows. Let $k \geq 0$, and let (x_n) be a Cauchy sequence in A. By definition, for this k we find an N such that $x_n - x_m \in I^k$ for $n, m > N$. In other words, the image of $x_n - x_m$ in A/I^k vanishes, hence the residues of x_n and x_m agree for all $n, m > N$. Denote this common value by $y_k \in A/I^k$, which defines a map $\mathfrak{C}(A)/\mathfrak{C}_0(A) \to A/I^k$. It is easy

to check that $\pi(y_{k+1}) = y_k$, so that the maps $\mathfrak{C}(A)/\mathfrak{C}_0(A) \to A/I^k$ together give a map $\mathfrak{C}(A)/\mathfrak{C}_0(A) \to \lim A/I^n$. It remains to check that this map is an isomorphism of topological rings. We leave this to the reader. □

Remark 5.27. One needs to be careful when I is not finitely generated. In that case, it may happen that $\lim_{n\geq 1} A/I^n$ is complete for the limit topology, but not for the I-adic topology. For finitely generated ideals, both topologies agree. We refer to [Sta18, Tags 00M9 & 05JA] for a detailed discussion of completion and some counter-examples.

Definition 5.28. A local ring A is called *complete* if it is $\mathfrak{m}$-adically complete for the unique maximal ideal $\mathfrak{m} \subset A$.

Example-Definition 5.29 (Main example in number theory)**.** Let A be a Dedekind domain with field of fractions $K = \mathrm{Frac}(A)$, and let $0 \neq \mathfrak{p} \subset A$ a prime ideal. Write $R := A_{\mathfrak{p}}$ which is a discrete valuation ring with maximal ideal $\mathfrak{m} := \mathfrak{p}A_{\mathfrak{p}}$. Let $v : K \to \mathbb{Z} \cup \{\infty\} \subset \mathbb{R} \cup \{\infty\}$ be the normalized discrete valuation of K with respect to R. Recall that this means if $\mathfrak{m} = (\pi) \subset R$, then $v(x) = n$ if $x = u\pi^n$ where $u \in R^\times$ is a unit, and $n \in \mathbb{Z}$.

Fix $c \in (0, 1) \subset \mathbb{R}$. Then $|x|_v = c^{v(x)}$ defines a non-archimedean absolute value $|\cdot|_v : K \to \mathbb{R}_{\geq 0}$ on K. We then have $R = \{x \in K \mid |x|_v \leq 1\}$, and $\mathfrak{m}^n = \{x \in K \mid |x|_v \leq c^n\}$ for any $n \geq 0$. Therefore the topology induced by $|\cdot|_v$ on R is the $\mathfrak{m}$-adic topology.

We let $(K_v, |\cdot|_v)$ be the completion of K with respect to $|\cdot|_v$. Then

$$R_v = \{x \in K_v \mid |x|_v \leq 1\} = \lim_n R/\mathfrak{m}^n$$

is the $\mathfrak{m}$-adic completion of R, and is a complete DVR with maximal ideal

$$\mathfrak{m}_v = \{x \in K_v \mid |x|_v < 1\}.$$

Lemma 5.30. *In the notation of 5.29, we have*

$$R/\mathfrak{m}^n \cong R_v/\mathfrak{m}_v^n$$

Proof. The proof is the same as in 5.24. □

Example 5.31 (p-adic numbers)**.** Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, and p a prime number. Then $R = \mathbb{Z}_{(p)}$ is a DVR with p-adic valuation v_p and associated p-adic absolute value $|\cdot|_p = p^{-v(\cdot)}$. We write $\mathbb{Q}_p$ for the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ and call it the field of p-adic numbers. Moreover, we let

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} = \lim \mathbb{Z}/p^n\mathbb{Z},$$

which is called the ring of p-adic integers.

With this new language, we give a reformulation of the Weak Approximation Theorem 5.20.

Corollary 5.32. *Let K be a field and let $|\cdot|_1, ..., |\cdot|_n$ be non-trivial and pair-wise inequivalent absolute values. For $i = 1, ..., n$ let K_i be the completion of K with respect to $|\cdot|_i$. Then the natural map $K \to \prod_{i=1}^n K_i$ has dense image.*

5.4. **Complete discrete valuation rings.** In this section, we let R be a complete DVR with maximal ideal $\mathfrak{m} = (\pi)$, so that $R = \lim_n R/(\pi^n)$. We let v be the normalized discrete valuation on $K = \mathrm{Frac}(R)$ and we fix $c \in (0,1) \subset \mathbb{R}$ to obtain an absolute value $|x| = c^{v(x)}$. Then $(K, |\cdot|)$ is a complete valued field.

Proposition 5.33 (π-adic expansion)**.** *Let $Z \subset R$ be a set of representatives of $R/(\pi)$ (the residue field of R). Then every $x \in K$ can be written uniquely as*

$$x = \sum_{i \in \mathbb{Z}, i \geq n} a_i \pi^i$$

for some $n \in \mathbb{Z}$ where $a_i \in Z$. One has $v(x) = \inf\{i \mid a_i \neq 0\}$.

Proof. Note that $a_i \pi^i$ converges to 0 as i goes to ∞. Thus, by Exercise 5.15, the sequence of partial sums corresponding to the above series is a Cauchy sequence. As K is complete, it converges in K.

Let $x \in K^\times$ and write $x = u\pi^n$ with $u \in R^\times$ and $n \in \mathbb{Z}$. Without loss of generality we may assume that $n = 0$, hence $x \in R^\times$ (otherwise prove the statement for u and multiply by π^n).

First, we have a bijection $Z \cong R/(\pi)$, and can therefore write $x = a_0 + \pi b_1$ with $0 \neq a_0 \in Z$ and $b_1 \in R$ uniquely determined.

Assume we had found unique $a_0, ..., a_{i-1} \in Z$ and $b_i \in R$ with

$$x = a_0 + \pi a_1 + ... + \pi^{i-1} a_{i-1} + \pi^i b_i.$$

Then as before we can write $b_i = a_i + \pi b_{i+1}$ with $a_i \in Z$ and $b_{i+1} \in R$ uniquely determined, and such that

$$x = a_0 + \pi a_1 + ... + \pi^{i-1} a_{i-1} + \pi^i a_i + \pi^{i+1} b_{i+1}.$$

This inductively defines the coefficients of $\sum_{i \geq 0} a_i \pi^i$, which converges to x. □

Example 5.34. Let p be a prime number, $K = \mathbb{Q}_p$, $R = \mathbb{Z}_p$, $\pi = p$. Then $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, the field with p elements. Therefore we can choose $Z = \{0, ..., p-1\}$. Then, every $x \in \mathbb{Q}_p$ has a unique representation

$$x = \sum_{i \geq n} a_i p^i$$

with $a_i \in \{0, ..., p-1\}$, such that $v_p(x) = \inf\{i \in \mathbb{Z} \mid a_i \neq 0\} \in \mathbb{Z} \cup \{\infty\}$. Here is an example.

We have

$$\sum_{i=0}^{m} (p-1)p^i = (p-1)\frac{p^{m+1} - 1}{p-1} = p^{m+1} - 1$$

and the latter converges to -1 for the p-adic absolute value $|\cdot|_p$ (as p^{m+1} goes to 0). Therefore, the series expansion of -1 is

$$-1 = (p-1) + p(p-1) + p^2(p-1) + ...$$

Definition 5.35. Let A be a ring, and $I \subset A$ and ideal. The pair (A, I) is called *Henselian pair* if the following holds.

a) The ideal I is contained in the Jacobson radical of A.

b) For every monic polynomial $f \in A[T]$ with image $\overline{f} \in (A/I)[T]$, and every factorization $\overline{f} = g_0 h_0$ in $(A/I)[T]$ with $g_0, h_0 \in (A/I)[T]$ monic such that $(g_0) + (h_0) = (A/I)[T]$, there exist monic $g, h \in A[T]$ with $f = gh, \overline{g} = g_0$, and $\overline{h} = h_0$. A local ring A with maximal ideal $\mathfrak{m}$ is called *Henselian* if $(A, \mathfrak{m})$ is a Henselian pair.

Lemma 5.36. *Given $g, h \in A[T]$ with $(\overline{g}) + (\overline{h}) = (A/I)[T]$, and g monic, we have*
(1) $(g) + (h) = A[T]$, and
(2) g and h are uniquely determined.

Proof. (1) Since g is monic, $A[T]/(g)$ is a finite free A-module. Therefore $M := A[T]/(g, h)$ is a finite A-module with $M/IM = (A/I)[T]/(\overline{g}, \overline{h}) = 0$. By Nakayama's lemma there exists $r \in R$ with $rM = 0$ and $r - 1 \in I$. Since I is in the Jacobson radical, so is $r - 1$, hence $r \in R^\times$. This implies $M = 0$.

(2) Write $f = g_1 h_1 = g_2 h_2$ with g_i monic and $\overline{g}_1 = \overline{g}_2$, as well as $\overline{h}_1 = \overline{h}_2$. By (1) we have $(g_1) + (h_2) = A[T]$, so we can find $r, s \in A[T]$ with $rg_1 + sh_2 = 1$. Hence $g_2 = rg_1 g_2 + sg_2 h_2 = g_1(rg_2 + sh_1)$, which implies $g_1 \mid g_2$. Since g_1 and g_2 are monic of the same degree, this implies $g_1 = g_2$. Moreover, monic polynomials in $A[T]$ are not zero divisors, so we get $h_1 = h_2$. □

Remark 5.37. Here is an immediate consequence. Let A be a local Henselian ring with residue field k. Let $f \in A[T]$ monic such that $\overline{f} \in k[T]$ has a simple root $\overline{a} \in k$. Then there exists a unique $a \in R$ with image $\overline{a}$ such that $f(a) = 0$. In other words, a simple root of f over k can be lifted to a root over A.

Theorem 5.38 (Hensel's Lemma)**.** *Let A be a ring and $I \subset A$ an ideal such that A is I-adically complete. Then (A, I) is a Henselian pair.*

The proof can be found in [Sta18], Tag 0ALJ.

Corollary 5.39. *Let $(K, |\cdot|)$ be a complete valued field with non-archimedean absolute value $|\cdot|$. Then $O_K = \{x \in K \mid |x| \leq 1\}$ is a Henselian DVR.*

Example 5.40. The ring of p-adic integers contains all $(p-1)$-th roots of unity. Indeed, the polynomial $X^{p-1} - 1 \in \mathbb{Z}_p[X]$ decomposes mod p into distinct linear factors. Since $\mathbb{Z}_p$ is complete, by Hensel's Lemma the polynomial $X^{p-1} - 1$ decomposes into $p - 1$ distinct linear factors.

Proposition 5.41. *Let R be a Henselian DVR with maximal ideal $\mathfrak{m}$ and residue field k, $K = \mathrm{Frac}(R)$, and $|\cdot|$ an absolute value corresponding to R (i.e. $R = \{x \in K \mid |x| \leq 1\}$). Moreover, let $f \in K[X]$ be an irreducible polynomial, and write $f = a_0 X^n + a_1 X^{n-1} + ... + a_n$. Then*

$$\max\{|a_0|, |a_1|, ..., |a_n|\} = \max\{|a_0|, |a_n|\}.$$

In particular, if $a_0, a_n \in R$, then $f \in R[X]$.

Proof. After multiplication with some element in $K^\times$ we may assume that

$$\max\{|a_0|, |a_1|, ..., |a_n|\} = 1.$$

In other words we may assume $f \in R[X]$. Let $r = \max\{i \mid |a_i| = 1\}$, then $a_j \in \mathfrak{m}$ for all $j > r$. Hence $\overline{f} \equiv X^{n-r}(\overline{a}_r + \overline{a}_{r-1} X + ...) \in k[X]$. Now assume $\max\{|a_0|, |a_n|\} < 1$. This implies $0 < r < n$, and $\overline{f}$ has a decomposition into coprime polynomials (since $\overline{a}_i \neq 0$ by assumption). Since R is Henselian, this factorization lifts to R, contradicting irreducibility of f. We conclude that $\max\{|a_0|, |a_n|\} = 1$, proving the claim. □

5.5. **Extensions of Henselian discrete valuation rings.**

Proposition 5.42. *Assume we have A, B, K, L as in Situation 3.15 (i.e. A is a Dedekind domain and B is its integral closure in L), with B a finite A-algebra (Hypothesis 3.16). Recall this implies B is also a Dedekind domain. Let $\mathfrak{p} \in \operatorname{Spec} A$ be a non-zero prime ideal, and $v_\mathfrak{p}$ be the associated discrete valuation, $R = A_\mathfrak{p} = \{x \in K \mid v_\mathfrak{p}(x) \geq 0\}$ the associated DVR, and $|x|_\mathfrak{p} = c^{v_\mathfrak{p}}(x)$ the associated non-archimedean absolute value (for some fixed c). Then, there are bijective correspondences between the following finite sets:*

$$\{\mathfrak{q} \in \operatorname{Spec} B \mid \mathfrak{q} \cap A = \mathfrak{p}\} \overset{1:1}{\longleftrightarrow} \{w \text{ discrete valuation on } L \text{ with } w|_K = v_\mathfrak{p}\}$$
$$\overset{1:1}{\longleftrightarrow} \{|\cdot| \text{ absolute value on } L \text{ with } |\cdot|_{|_K} = |\cdot|_\mathfrak{p}\}.$$

The first map is given by $\mathfrak{q} \mapsto \frac{1}{e_\mathfrak{q}} v_\mathfrak{q}$ where $v_\mathfrak{q}$ is the non-trivial discrete valuation given by $B_\mathfrak{q}$, and $e_\mathfrak{q}$ is the ramification index of $\mathfrak{q}$, and the second map is given by $w \mapsto c^{w(\cdot)}$.

Proof. By Corollary 3.25 there are only finitely many primes $\mathfrak{q}$ lying above $\mathfrak{p}$. The second bijection is clear, so we only prove the first one.

We first check that $\frac{1}{e_\mathfrak{q}} v_\mathfrak{q}$ extends $v_\mathfrak{p}$. It suffices to show this for prime ideals in A. We have $\frac{1}{e_\mathfrak{q}}(\mathfrak{p}B) = \frac{1}{e_\mathfrak{q}} e_\mathfrak{q} = 1$ by definition of $e_\mathfrak{q}$. For $\mathfrak{p} \neq \mathfrak{p}' \in \operatorname{Spec} A$ a non-zero prime ideal, we have $v_\mathfrak{q}(\mathfrak{p}'B) = 0 = v_\mathfrak{p}(\mathfrak{p}')$ (if it were positive, then $\mathfrak{q}$ would lie over $\mathfrak{p}'$ implying $\mathfrak{p} = \mathfrak{p}'$).

Let us check injectivity. Let $\mathfrak{q}, \mathfrak{q}'$ be distinct primes above $\mathfrak{p}$. Then there exists $x \in \mathfrak{q} \setminus \mathfrak{q}'$. For this x we have $v_\mathfrak{q}(x) > 0 \geq v_{\mathfrak{q}'}(x)$. This implies $v_\mathfrak{q} \neq v_{\mathfrak{q}'}$.

For surjectivity let $S := \{x \in L \mid w(x) \geq 0\} \subset L$, which is a DVR. Denote its maximal ideal by $\mathfrak{m}$. Since $w|_K = v$, we have $w|_A \geq 0$ and $w|_\mathfrak{p} > 0$. Therefore $A \subset S$, and $\mathfrak{p} = \mathfrak{m} \cap A$. Since S is a DVR, it is integrally closed in L. Indeed, assume $x \in L$ satisfies an equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_i \in S$. Now $\operatorname{Frac}(S) = L$, and $x \in S$ or $x^{-1} \in S$. In the first case, we are done. If $x^{-1} \in L$, we have

$$-x = a_{n-1} + a_{n-2}x^{-1} + \ldots + a_1 x^{-n+2} + a_0 x^{-n+1}.$$

Now S being integrally closed implies $B \subset S$. We define $\mathfrak{q} := \mathfrak{m} \cap B \subset B$, which is now a prime ideal with $\mathfrak{q} \cap A = \mathfrak{p}$. This proves the proposition. □

Theorem 5.43. *Let A be a Henselian DVR with field of fractions $K = \operatorname{Frac}(R)$, $|\cdot|$ a corresponding absolute value, $L \supset K$ a finite extension, $B = \{x \in L \mid x \text{ integral over } A\}$ the integral closure of A in L. Let $n = [L : K]$. Then the following holds.*

1. *We have $B = \{x \in L \mid N_{L/K}(x) \in A\}$.*
2. *The absolute value $|\cdot|$ has a unique extension to L. This extension is given by*
$$x \mapsto \sqrt[n]{|N_{L/K}(x)|}.$$
3. *The ring B is a DVR.*

Proof. (1) The inclusion $B \subset \{x \in L \mid N_{L/K}(x) \in A\}$ follows from Remark 3.33. So assume we are given $x \in L^\times$ with $N_{L/K}(x) \in A$. We need to show that x is integral over A. Let

$$\mu_x = X^d + a_1 X^{d-1} + \ldots + a_d \in K[X]$$

be its minimal polynomial over K. The Norm is up to a sign the constant term of the characteristic polynomial χ_x of x. Now by Cayley-Hamilton (using the fact that μ_x is irreducible), χ_x is a power of μ_x. We find that $N_{L/K}(x) = \pm a_d^m \in A$ for some $m > 0$. This implies $a_d \in A$. We apply Proposition 5.41 to conclude that $\mu_x \in A[X]$, so x is integral over A, i.e. $x \in B$.

(2) We first prove that $\alpha(x) = \sqrt[n]{|N_{L/K}(x)|}$ is a discrete non-archimedean absolute value on L extending $|\cdot|$ on K. Let $x \in K$. Then, $\sqrt[n]{|N_{L/K}(x)|} = \sqrt[n]{|x|^n} = |x|$, so α extends $|\cdot|$. We check the properties of an absolute value.

First, it is clear that $\alpha(x) = 0$ if and only if $x = 0$. Multiplicativity follows from multiplicativity of the norm $N_{L/K}$. It remains to prove the strong triangle inequality $\alpha(x+y) \leq \max\{\alpha(x), \alpha(y)\}$. Without loss of generality we may assume $\alpha(x) \geq \alpha(y)$ and $x \neq 0$.

It is enough to show that $\alpha(1+y/x) \leq \max\{1, \alpha(y/x)\}$ (we can simply multiply this by $\alpha(x)$). Let $z := y/x$, then $\alpha(z) \leq 1$ and $\max\{1, \alpha(z)\} = 1$. Therefore, we only need to show $\alpha(1+z) \leq 1$. Recall that $A = \{x' \in K \mid |x'| \leq 1\}$. Since $\sqrt[n]{|N_{L/K}(z)|} = \alpha(z) \leq 1$, we have $|N_{L/K}(z)| \leq 1$, so by (1) we have $z \in B$. This implies $z + 1 \in B$, and again by (1) this implies $\alpha(z+1) \leq 1$.

Before proving uniqueness of α, we prove (3). We can write $B = \{x \in L \mid \alpha(x) \leq 1\}$, and since α is an absolute value, we find that B is a DVR. Therefore, B has a unique non-zero prime ideal which is maximal and by Proposition 5.42 α is the unique extension of $|\cdot|$ (extensions are in bijection with prime ideals in B lying over the corresponding prime in A). □

Corollary 5.44. *Let $(K, |\cdot|)$ be a complete valued field, $|\cdot|$ discrete, $L \supset K$ an algebraic extension. Then there exists a unique extension $\|\cdot\|$ of $|\cdot|$ to L. If $L \supset K$ is finite, then $\|\cdot\|$ is discrete and $(L, \|\cdot\|)$ is complete.*

Proof. Every algebraic extension is a union of its finite subextension. Therefore we may assume $L \supset K$ is finite. By Theorem 5.43 there exists a unique $\|\cdot\|$ which is discrete. Now K is complete, and L is a finite-dimensional vector space over K. It is a standard fact that a finite-dimensional vector space over a complete field is complete. □

Example 5.45. Let $A = \mathbb{Z}_p, K = \mathbb{Q}_p$. Consider the extension $L = \mathbb{Q}_p(\sqrt{p})$. Let $|\cdot|_p$ be the p-adic absolute value on $\mathbb{Q}_p$, and B the integral closure of A in L. Let $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ the normalized p-adic valuation. Note that $\sqrt{p} \notin \mathbb{Q}_p$, for otherwise $v_p(\sqrt{p}) = \frac{1}{2} v_p(p) = 1/2$, which is a contradiction.

Now $\mathbb{Z}_p$ is complete, so by Theorem 5.43 and Corollary 5.44 the ring B is a complete DVR. We have $pB = (\sqrt{p})^2$, so $(\sqrt{p})$ lies over pA. Since $[L : K] = 2$, $(\sqrt{p}) \subset B$ has to be the unique prime ideal, and $e_{\sqrt{p}} = 2$, $f_{\sqrt{p}} = 1$. In fact, we can conclude that $B = \mathbb{Z}_p[\sqrt{p}]$ by the description $B = \{x \in L \mid N_{L/K} \in \mathbb{Z}_p\}$.

Exercise 5.46. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$, and $n \geq 1$. Moreover, let ζ be a primitive $(p^n - 1)$-th root of unity, and $L = \mathbb{Q}_p[\zeta]$. Show the following.

(1) We have $[L : K] = n$, and (p) is unramified.
(2) The integral closure of $\mathbb{Z}_p$ in L is $\mathbb{Z}_p[\zeta]$.

We remark that if $L \supset K$ is finite of degree n, and (p) is unramified in L, then $L \cong \mathbb{Q}_p[\zeta]$.

5.6. **Local-global principles.** Assume we are again in Situation 3.15. Moreover, let $K_\mathfrak{p}$ be the completion of K with respect to $|\cdot|_\mathfrak{p}$, and denote the extension of $|\cdot|_\mathfrak{p}$ to $K_\mathfrak{p}$ by the same symbol $|\cdot|_\mathfrak{p}$. Recall that $|K_\mathfrak{p}|_\mathfrak{p} = |K|_\mathfrak{p}$ and similarly for $v_\mathfrak{p}$.

Then $\widehat{A}_\mathfrak{p} := \{x \in K_\mathfrak{p} \mid |x|_\mathfrak{p} \leq 1\} = \lim_n A/\mathfrak{p}^n$ is a complete DVR with $\mathrm{Frac}(\widehat{A}_\mathfrak{p}) = K_\mathfrak{p}$. Let $\widehat{\mathfrak{p}} = \pi\widehat{A}_\mathfrak{p} = \{x \in K_\mathfrak{p} \mid |x|_\mathfrak{p} < 1\}$ be the maximal ideal of $\widehat{A}_\mathfrak{p}$. For $n \geq 1$ we have $\mathfrak{p}^n\widehat{A}_\mathfrak{p} = \widehat{\mathfrak{p}}^n\widehat{A}_\mathfrak{p}$ and moreover $A/\mathfrak{p}^n = A_\mathfrak{p}/\mathfrak{p}^n A_\mathfrak{p} \cong \widehat{A}_\mathfrak{p} / \widehat{\mathfrak{p}}^n\widehat{A}_\mathfrak{p}$.

Theorem 5.47. *In the above notation, let $L \supset K$ be a finite separable field extension, and let B be the integral closure of A in L. Then the following holds.*

(1) For $\mathfrak{q} \in \mathrm{Spec}\ B$ lying over $\mathfrak{p}$ we have $e_\mathfrak{q} = e_{\widehat{\mathfrak{q}}}$, $f_\mathfrak{q} = f_{\widehat{\mathfrak{q}}}$, and
(2) we have $L \otimes_K K_\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

Proof. (1) Let $e := e_\mathfrak{q}$. By Remark 3.28 we have $\mathfrak{p}B_\mathfrak{q} = (\mathfrak{q}B_\mathfrak{q})^e$. Then $\widehat{\mathfrak{p}}\widehat{B}_\mathfrak{q} = \widehat{(\mathfrak{q}B_\mathfrak{q})}^e = \widehat{\mathfrak{q}}^e\widehat{B}_\mathfrak{q}$. This implies $e_{\widehat{\mathfrak{q}}} = e$. Moreover, $f_\mathfrak{q} = [B/\mathfrak{q} : A/\mathfrak{p}] = [\widehat{B}_\mathfrak{q}/\widehat{\mathfrak{q}} : \widehat{A}_\mathfrak{p}/\widehat{\mathfrak{p}}\widehat{A}_\mathfrak{p}] = f_{\widehat{\mathfrak{q}}}$.

(2) By the fundamental equality in Theorem 3.24, we have

$$\dim_{K_\mathfrak{p}}(L \otimes_K K_\mathfrak{p}) = \dim_K(L) = \sum_{\mathfrak{q}|\mathfrak{p}} e_q\ f_q.$$

On the other hand, the right hand side of (2) has dimension $\sum_{\mathfrak{q}|\mathfrak{p}} \dim_{K_\mathfrak{p}}(L_\mathfrak{q})$. By (1), we have $\dim_{K_\mathfrak{p}}(L_\mathfrak{q}) = e_\mathfrak{q} f_\mathfrak{q}$. We find that both sides of (2) are finite-dimensional $K_\mathfrak{p}$-vector spaces of the same dimension. Consider the $K_\mathfrak{p}$-linear map

$$\begin{aligned} \phi : L \otimes_K K_\mathfrak{p} &\to \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q} \\ x \otimes 1 &\mapsto (x, ..., x). \end{aligned}$$

By the Weak Approximation Theorem 5.32, ϕ has dense image. Note that the image of ϕ is a finite-dimensional $K_\mathfrak{p}$-subvector space. Such a subspace is automatically closed by Lemma 5.48 below, hence ϕ is surjective. Therefore ϕ is a surjective map of finite-dimensional vector spaces, and as such is bijective. □

Lemma 5.48. *Let $(K, |\cdot|)$ be a complete valued field, V and W finite-dimensional normed vector spaces. Then every linear map $V \to W$ is continuous. Moreover:*

(1) Let V be a finite dimensional K-vector space, then all norms on V are equivalent. This means there is a unique topology on V coming from a norm with respect to $|\cdot|$ on K.
(2) Subvector spaces of finite dimensional vector spaces are closed.

Proof. Reference is *Bourbaki*, Topological Vector Spaces, Chapter I, §2.3. □

Corollary 5.49. *Let A, K, B and L as in Theorem 5.47. Write $L = K(\theta)$ (this is possible since $L \supset K$ is finite and separable). Denote by $f := \mu_{\theta,K}$ the minimal polynomial of θ. Let $\mathfrak{p} \in \mathrm{Spec}\ A$ be a non-zero prime ideal and let $f = f_1 \cdot ... \cdot f_r$ be the decomposition of f into monic irreducible factors over $K_\mathfrak{p}$. Then the $\mathfrak{q}_i \in \mathrm{Spec}\ B$ lying above $\mathfrak{p}$ correspond bijectively to the f_i and we have $L_{\mathfrak{q}_i} \cong K_\mathfrak{p}[T]/(f_i)$. In particular, $\deg(f_i) = [L_{\mathfrak{q}_i} : K_\mathfrak{p}] = e_{\mathfrak{q}_i} f_{\mathfrak{q}_i}$.*

Proof. Since f is separable, all f_i are distinct. Hence

$$\prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q} \cong L \otimes_K K_\mathfrak{p} \cong K[T]/(f) \otimes_K K_\mathfrak{p} = K_\mathfrak{p}[T]/(f).$$

By the chinese remainder theorem, $K_\mathfrak{p}[T]/(f) \cong \prod_{i=1}^r K_\mathfrak{p}[T]/(f_i)$. The theorem follows from the Lemma below. □

Lemma 5.50. *Let $K_1, ..., K_n$ be fields. Any ideal $I \subset \prod_{i=1}^n K_i$ is a subproduct of $\prod_{i=1}^n K_i$. Moreover, any surjective homomorphism $\phi : \prod_{i=1}^n K_i \to B$ can be identified with the projection onto a subproduct.*

Proof. The projection $p_j : \prod_{i=1}^n K_i \to K_j$ is a surjective ring homomorphism onto K_j. Therefore, $p_j(I) \subset K_j$ is an ideal and as such it is either 0 or K_j. Thus I is the product of K_j for which $p_j(I) \subset K_j \neq 0$. For the second statement, note that $\ker(\phi)$ is an ideal, so it is a subproduct of $\prod_{i=1}^n K_i$. Therefore $\prod_{i=1}^n K_i = \ker\phi \times \mathrm{im}(\phi)$ and $\mathrm{im}(\phi) = B$ is a subproduct. □

Corollary 5.51. *Let A, K, B and L and $\mathfrak{p}$ as in Theorem 5.47. Let $x \in L$, then we have*

(1) $N_{L/K}(x) = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_q|K_\mathfrak{p}}(x)$, *and*
(2) $\mathrm{Tr}_{L/K}(x) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{q}/K_\mathfrak{p}}(x)$.

Exercise 5.52. Prove the above Corollary.

6. Local and global fields

6.1. Locally compact groups.

Definition 6.1. A topological space X is locally compact if it is Hausdorff and every point of X has a compact neighborhood.

Theorem 6.2 (Topological facts)**.** *(1) Let $(K, |\cdot|)$ be a complete valued field, and let V be a normed space over K. Assume that some neighborhood of $0 \in V$ is precompact (i.e. its closure is compact). Then K and V are locally compact and V is finite dimensional.*
(2) Let $(G, +)$ be an abelian group with a metric d such that $d(g, g') = d(g + h, g' + h)$ for all $g, g', h \in G$. If G is locally compact, then G is complete.

Proof. The reference is [Bou02, Chapter I, § 2.4., Theorem 3] and [Bou95, Chapter III, § 3.3, Corollary 1 of Proposition 4]. □

In the following we study some integration theory on locally compact spaces.

Definition 6.3. Let X be locally compact, and $\mathcal{B}$ its Borel σ-algebra. Recall that this is the σ-algebra generated by open subsets of X. A measure $\mu : \mathcal{B} \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is called *Radon measure* if

(a) $\mu(C) < \infty$ for every compact C, and
(b) for all $A \in \mathcal{B}$ we have $\mu(A) = \sup\{\mu(C) \mid C \subset A \text{ compact}\}$ (we say the measure is inner regular).

Let G be a locally compact topological group. A *left Haar measure* μ on G is a non-zero Radon measure on G such that $\mu(gZ) = \mu(Z)$ for all $g \in G$ and all measurable sets Z.

Remark 6.4. In the above situation, we call a Radon measure μ *regular*, if μ is in addition outer regular, which means that $\mu(A) = \inf\{\mu(U) \mid U \supset A \text{ open}\}$. It can be shown that for σ-compact spaces, any Radon measure is regular. Here, σ-compact means that in addition to being locally compact, X can be written as countable union of compact sets. In the cases we are interested in, this will always be satisfied (such as non-discrete locally compact fields for example).

Theorem 6.5. *Let G be a locally compact topological group. Then, a Haar measure μ on G exists. Moreover, if μ' is another Haar measure, then there exists a positive real number $\alpha \in \mathbb{R}_{>0}$ such that $\mu' = \alpha\mu$.*

Proof. This is [Bou04, Chapter II, § 1.2., Theorem 1]. □

Remark 6.6. Let G be a locally compact group, $\alpha : G \to G$ an automorphism of G (which means α is a group homomorphism and a homeomorphism). Choose a Haar measure μ on G. Then the map

$$Z \mapsto \mu(\alpha(Z))$$

for every measurable set Z is again a Haar measure. Indeed, $\mu(\alpha(gZ)) = \mu(\alpha(g)\alpha(Z)) = \mu(\alpha(Z))$. Therefore there is a unique $|\alpha|_G \in \mathbb{R}_{>0}$ satisfying

$$\mu(\alpha(Z)) = |\alpha|_G \mu(Z)$$

for every measurable set Z. It is easy to check that $|\alpha|_G$ is independent of the chosen Haar measure μ. Indeed, let μ' be another Haar measure. Then $\mu' = \lambda\mu$ for some $\lambda \in \mathbb{R}_{>0}$. Assume Z is measurable with $\mu(Z) > 0$. Then $|\alpha|_G = \frac{\mu(\alpha(Z))}{\mu(Z)} = \frac{\mu'(\alpha(Z))}{\mu'(Z)}$.

Moreover, if $\beta : G \to G$ is an automorphism of G, then for every measurable set Z we have

$$\mu(\alpha(\beta(Z))) = |\alpha|_G \mu(\beta(Z)) = |\alpha|_G \, |\beta|_G \mu(Z).$$

Therefore, the map $\mathrm{Aut}(G) \to \mathbb{R}_{>0}$ given by $\alpha \mapsto |\alpha|_G$ is a group homomorphism.

Definition 6.7. The real number $|\alpha|_G$ is called the *modulus of* α.

We need a few more facts and properties about locally compact groups and Haar measures which we state without proofs.

Theorem 6.8. *Let G be an abelian locally compact topological group, and $H \subset G$ a closed subgroup.*

(1) Then H and G/H are locally compact abelian groups.

(2) Let μ_G be a Haar measure on G, μ_H a Haar measure on H. Note that this is not necessarily the restriction of μ_G to $\mathcal{B}(H)$. Then there exists a unique Radon measure $\mu_{G/H}$ on G/H satisfying

$$\int_G f(x) d\mu_G(x) = \int_{G/H} \left(\int_H f(gh) d\mu_H(h) \right) d\mu_{G/H}(gH),$$

for every continuous real-valued function f on G. In addition, the measure $\mu_{G/H}$ is a Haar measure on G/H. For compact $C \subset G$, the above equation implies

$$\mu_G(C) = \int_{G/H} f_C(gH) d\mu_{G/H}(gH)$$

where $f_C : G/H \to \mathbb{R}$ is defined by

$$f_C(gH) = \mu_H(\{h \in H \mid gh \in C\}) = \mu_H(H \cap g^{-1}C).$$

(3) *Let $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha(H) = H$. Then, we have an induced automorphisms $\overline{\alpha} \in \mathrm{Aut}(G/H)$. The modulus satisfies*

$$|\alpha|_G = |\alpha|_H \, |\overline{\alpha}|_{G/H}.$$

Proof. The reference is [Bou04, Chapter VII, § 2]. □

Remark 6.9. Suppose $H \subset G$ is a discrete subgroup, and let μ_H be the counting measure on H. Then $f_C(gH) = \#(H \cap g^{-1}C) = \#(gH \cap C)$. Suppose that the restriction of the natural projection $\pi : G \to G/H$ to C is injective. Then $f_C(gH)$ is the characteristic function of $\pi(C) \subset G/H$, and $\mu_G(C) = \int_{G/H} f_C d\mu_{G/H} = \mu_{G/H}(\pi(C))$.

Example 6.10. Let G a compact topological group. Then G is locally compact and carries a Haar measure μ'. Since G is compact, and μ' is a Radon measure, we have $0 < \mu'(G) < \infty$. Haar measures are unique up to scaling by a positive real number, so there exists a unique Haar measure μ on G with $\mu(G) = 1$. We call this the *normalized Haar measure of G*. Note that for any automorphism $\alpha \in \mathrm{Aut}(G)$ we have $|\alpha|_G = 1$. Indeed, we have

$$1 = \mu(G) = \mu(\alpha(G)) = |\alpha|_G \mu(G) = |\alpha|_G.$$

Exercise 6.11. Let G be a discrete topological group. Show the following.

(1) The group G is locally compact, and the Borel σ-algebra on G is the power set of G.
(2) The counting measure which assigns to $Z \subset G$ its number of elements if Z is finite, or ∞ if Z is infinite, is a Haar measure on G.
(3) For every automorphism $\alpha \in \mathrm{Aut}(G)$ we have $|\alpha|_G = 1$.

6.2. **Local fields.**

Theorem 6.12 (Classification of non-discrete locally compact fields)**.** *Let K be a non-discrete topological field. The following are equivalent.*

(i) The field K is locally compact.
(ii) There exists an absolute value $|\cdot|$ on K inducing the given topology on K such that $(K, |\cdot|)$ is a complete valued field and
  (a) either $|\cdot|$ is archimedean, or
  (b) $|\cdot|$ is discrete and $R/\mathfrak{m}$ is a finite field, where $R = \{x \in K \mid |x| \leq 1\}$ and $\mathfrak{m} = \{x \in K \mid |x| < 1|\}$.
(iii) We are in one of the following cases.
  (a) Archimedean case. We have $K = \mathbb{R}$ or $K = \mathbb{C}$,
  (b) Non-archimedean, $\mathrm{char}(K) = 0$. The field K is a finite extension of $\mathbb{Q}_p$ endowed with the unique topology as a finite dimensional normed $\mathbb{Q}_p$-vector space for some prime number p (with respect to the p-adic absolute value).
  (c) Non-archimedean, $\mathrm{char}(K) > 0$. We have $K = \mathrm{Frac}(\mathbb{F}_q[\![t]\!])$ for some prime power $q = p^r$ with topology induced by the discrete valuation

$$v : \mathbb{F}_q[\![t]\!] \to \mathbb{Z} \cup \{\infty\},$$
$$\sum_{i \geq 0} a_i t^i \mapsto \inf\{m \geq 0 \mid a_m \neq 0\}.$$

In any of these cases the field K is called a local field.

Proof. We will not need every statement of this theorem, only the ones involving characteristic 0 fields. We prove only some statements, and refer to [Wei95, Chapter I] for the rest.

Equivalence of (ii)(a) and (iii)(a) is part of Ostrowski's Theorem 5.17. It is clear that $\mathbb{R}$ and $\mathbb{C}$ are locally compact and non-discrete, so (iii)(a) implies (i).

We show that (iii)(b) implies (ii)(b), and that this implies (i). For the first implication, let $K \supset \mathbb{Q}_p$ be a finite extension. By Corollary 5.44 the p-adic absolute value extends uniquely to an absolute value $\|\cdot\|$ on K, which makes K a normed vector space over $\mathbb{Q}_p$. By Lemma 5.48 all norms are equivalent, and it is a standard fact that K is complete with respect to any of these norms (since $\mathbb{Q}_p$ is complete). The residue field of K is a finite extension of $\mathbb{F}_p$, hence finite.

We prove that (ii)(b) implies (i). Note that the topology is non-discrete, since the absolute value is non-trivial. We need to show that K is locally compact, i.e. every point $x \in K$ has a compact neighborhood. We show that actually every point has a compact open neighborhood. For this, we check that the ring $R = \{x \in K \mid |x| \leq 1\}$ is open in K. Recall that $|\cdot| : K^\times \to \mathbb{R}_{>0}$ is continuous for the discrete topology on $\mathbb{R}_{>0}$. This implies $R^\times = \{x \in K \mid |x| = 1\}$ is open. Moreover, $\mathfrak{m}$ is defined by $|x| < 1$, so it is clearly open, and so is $R = R^\times \cup \mathfrak{m}$. Now it suffices to check that R is compact (because in that case, $x + R$ is a compact neighborhood of $x \in K$ for any K). Since R is complete, we have $R = \lim_n R/\mathfrak{m}^n \subset \prod_n R/\mathfrak{m}^n$. Here, every $R/\mathfrak{m}^n$ carries the discrete topology, so in particular it is Hausdorff, and the inverse limit is closed in the product. It therefore suffices to prove that $\prod_n R/\mathfrak{m}^n$ is compact. This follows from Tychonoff's theorem once we know that each $R/\mathfrak{m}^n$ is compact (which in the discrete case is equivalent to being finite). Thus, we need to show that $R/\mathfrak{m}^n$ is finite for every n. We prove it by induction on n. Let $\mathfrak{m} = (\pi)$. We have an exact sequence

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n \to 0,$$

where $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong R/\mathfrak{m}$ as R-modules via multiplication with π^{-n}. By induction hypothesis, $R/\mathfrak{m}^n$ is finite, and by assumption, $R/\mathfrak{m}$ is finite. We omit the proofs of all other implications. □

Remark 6.13. The above proof implies that $\#R/\mathfrak{m}^n = q^n$ where $q = \#R/\mathfrak{m}$.

Definition 6.14. Let K be a local field and $a \in K^\times$. Then the map $x \mapsto ax$ is a group automorphism of $(K, +)$. Denote by $|a|_K \in \mathbb{R}_{>0}$ its modulus. Recall that this means for any Haar measure μ on K and any measurable set Z we have $\mu(aZ) = |a|_K \mu(Z)$.

In addition, define $|0|_K := 0$ (note that then $\mu(aZ) = |a|_K \mu(Z)$ for all $a \in K$ and all measurable Z). We call $|a|_K$ the *modulus of* a. Note that the modulus is multiplicative, i.e. $|ab|_K = |a|_K |b|_K$.

Proposition 6.15. *(1) For $K = \mathbb{R}$ the modulus $|\cdot|_\mathbb{R}$ is the usual absolute value.*

(2) For $K = \mathbb{C}$ the modulus $|\cdot|_\mathbb{C}$ is the square of the usual absolute value. In particular, since it does not satisfy the triangle inequality, it is not an absolute value on $\mathbb{C}$.

(3) Let K be non-archimedean with corresponding DVR $R \subset K$ and finite residue field k. Let v be the normalized discrete valuation for R. Then for any $a \in K$ we have $|a|_K = q^{-v(a)}$, where $q = \#k$.

Proof. Let $a \in K^\times$.

(1) The Lebesgue measure on $\mathbb{R}$ is a Haar measure. It is normalized such that $\mu([0,1]) = 1$. We use it to compute the modulus. Let $|\cdot|$ be the usual absolute value on $\mathbb{R}$ and $C = [0,1]$. We have $\mu(aC) = |a| = |a|\mu(C)$.

(2) We again use the Lebesgue measure on $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ to compute the modulus. Let $C = [0,1] \times [0,i]$, then $\mu(C) = 1$. The effect of scaling C by $a \in \mathbb{C}^\times$ is rotation by the argument of a and dilation by $|a|$. Therefore

$$\mu(aC) = \mu([0,|a|] \times [0,|a|i]) = |a|^2 = |a|^2\mu(C).$$

(3) Write $a = \frac{b}{c}$ for $b, c \in R \setminus \{0\}$. Then $|a|_K = \frac{|b|_K}{|c|_K}$. Thus, it suffices to show $|a|_K = q^{-v(a)}$ for all $a \in R$. Write $n = v(a) \geq 0$. Then $\#R/aR = q^n$. This means we can write R as a disjoint union of q^n subsets of the form$aR + b$. This means

$$\mu(R) = \sum \mu(aR + b) = \sum \mu(aR) = q^n \mu(aR),$$

where the second equality follows since μ is a Haar measure, hence translation invariant. This implies $|a|_K = q^{-n}$, proving the claim.

□

6.3. **Global fields.**

Definition 6.16. Let K be a field. The equivalence class of a non-trivial absolute value on K is called a *place* of K.

Example 6.17. By Ostrowski's Theorem 5.17, the places of $\mathbb{Q}$ are the p-adic absolute values $|\cdot|_p$ and the archimedean absolute value $|\cdot|_\infty$.

Definition 6.18. A *number field* K is a finite extension of $\mathbb{Q}$. We define $O_K := \{x \in K \mid x \text{ integral over } \mathbb{Z}\}$, which is a Dedekind domain.

Proposition 6.19. *Let K be a number field, $|\cdot|$ a place of K, and $\widehat{K}$ the completion of K with respect to $|\cdot|$. There are two cases.*

(1) If $|\cdot|$ is archimedean, then $\widehat{K} = \mathbb{R}$ or $\widehat{K} = \mathbb{C}$, and there is a $\mathbb{Q}$-linear embedding $\tau : K \hookrightarrow \mathbb{C}$ such that $|\cdot|$ is equivalent to $|\cdot|_\tau$. Here, $|x|_\tau := |\tau(x)|$ for the usual absolute value on $\mathbb{C}$. Moreover, $|\cdot|_\tau$ is equivalent to $|\cdot|_{\tau'}$ if and only if $\tau = \tau'$ or $\tau' = \overline{\tau}$ (the pointwise complex conjugate).

(2) If $|\cdot|$ is non-archimedean, there exists a non-zero prime ideal $\mathfrak{q} \subset O_K$ such that $|\cdot|$ is equivalent to $|\cdot|_\mathfrak{q}$. Moreover, $\widehat{K}$ is a finite extension of $\mathbb{Q}_p$ where p is the prime number generating $\mathfrak{q} \cap \mathbb{Z}$.

In both of these cases, $\widehat{K}$ is a local field.

Proof. (1): Ostrowski's Theorem 5.17 (2) implies that $\widehat{K} = \mathbb{R}$ or $\widehat{K} = \mathbb{C}$. Let τ be the composition

$$K \overset{\iota}{\hookrightarrow} \widehat{K} \hookrightarrow \mathbb{C}$$

where ι is the natural embedding into the completion. For $x \in K$ we have

$$|x| = |\iota(x)| = |\tau(x)|^s$$

for some $s > 0$ (because the extension of the absolute value on $\widehat{K}$ to $\mathbb{C}$ is equivalent to the usual absolute value).

If $\tau' = \overline{\tau}$ it is clear that $|\cdot|_\tau = |\cdot|_{\tau'}$. Vice versa, if $|\cdot|_\tau \sim |\cdot|_{\tau'}$, there exists a positive real number such that $|\cdot|_{\tau'} = |\cdot|_\tau^s$. However, $|\cdot|_\tau$ and $|\cdot|_{\tau'}$ agree on $\mathbb{Q}$, so $s = 1$.

In addition, completing K with respect to $|\cdot|_\tau$ and with respect to $|\cdot|_{\tau'}$ yields the same completion $\widehat{K}$. By the universal property of completion, τ and τ' extend to $\widehat{\tau}, \widehat{\tau}' : \widehat{K} \to \mathbb{C}$.

If $\widehat{K} = \mathbb{R}$, then since $\mathbb{Q} \subset \mathbb{R}$ is dense, we have $\widehat{\tau} = \widehat{\tau}'$, implying $\tau = \tau'$.

If $\widehat{K} = \mathbb{C}$, then define $\alpha := \widehat{\tau} \circ (\widehat{\tau}')^{-1}$. By the above argument, this is a field automorphism of $\mathbb{C}$ fixing $\mathbb{R}$. This implies $\alpha = \mathrm{id}$ or α is complex conjugation.

(2) By Ostrowski's Theorem 5.17 (1), the restriction of $|\cdot|$ to $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for a unique p. By Proposition 5.42, $|\cdot|$ is the $\mathfrak{q}$-adic absolute value for some prime ideal $\mathfrak{q} \subset O_K$ lying over (p). This implies $\widehat{K} = K_\mathfrak{q}$, which is a finite extension of $\mathbb{Q}_p$. □

Definition 6.20. Let K be a number field, v a place of K, and K_v the completion of K with respect to v.

(1) Let v be archimedean with corresponding $\mathbb{Q}$-embedding $\tau : K \hookrightarrow \mathbb{C}$. We call τ *real* if $\tau(K) \subset \mathbb{R}$ (which holds if and only if $K_v = \mathbb{R}$), and we call τ complex if $\tau(K) \not\subset \mathbb{R}$ (which holds if and only if $K_v = \mathbb{C}$). We define

$$|x|_v := \begin{cases} |\tau(x)|_\mathbb{R}, \tau \text{ real} \\ |\tau(x)|_\mathbb{C}, \tau \text{ complex.} \end{cases}$$

Note that $|\cdot|_\mathbb{C}$ denotes the modulus, which is the square of the usual absolute value on $\mathbb{C}$.

(2) Let v be non-archimedean corresponding to the prime ideal $\mathfrak{p} \subset O_K$. Then we define $|\cdot|_v$ to be the modulus on K_v. Recall that for $\widehat{\mathfrak{p}} = \mathfrak{p}O_v$ this means $|x|_v = q^{-v_{\widehat{\mathfrak{p}}}(x)}$ for $q = \#O_K/\mathfrak{p} = p^{f_v}$. Here $f_v = f_\mathfrak{p} = [O_K/\mathfrak{p} : \mathbb{F}_p]$, and the valuation $v_{\widehat{\mathfrak{p}}}$ is the normalized discrete valuation on O_v. Moreover, we denote by $e_v = e_\mathfrak{p}$ the ramification index of $\mathfrak{p}$, i.e. e_v is the largest integer such that $\mathfrak{p}^{e_v}$ divides pO_K.

Lemma 6.21. *Let K be a number field, v a place of K, and let $|\cdot|_p = v|_\mathbb{Q}$ (this means p is a prime number or $p = \infty$). Then $|x|_v = |N_{K_v/\,\mathbb{Q}_p}(x)|_p$.*

Exercise 6.22. Prove the above lemma.

Theorem 6.23 (Product formula)**.** *Let K be a number field, and let $x \in K^\times$. Then $|x|_v = 1$ for almost all places v of K and*

$$\prod_{v \text{ place of } K} |x|_v = 1.$$

Proof. The number of archimedean places is bounded by

$$\#\mathrm{Hom}_\mathbb{Q}(K, \mathbb{C}) = [K : \mathbb{Q}] < \infty.$$

Indeed, by the primitive element theorem $K = \mathbb{Q}(\alpha) = \mathbb{Q}[T]/(f)$ for some $\alpha \in K$ with minimal polynomial f. The polynomial f has $n = [K : \mathbb{Q}]$ distinct roots $\alpha_1, ..., \alpha_n$, and the distinct embeddings $\mathbb{Q}[T]/(f) \hookrightarrow \mathbb{C}$ are given by $T \mapsto \alpha_j$ for some j (the image of T has to be a root of f). For a non-archimedean place v corresponding to $\mathfrak{q} \subset O_K$ we have $|x|_v \neq 1$ if and only if $\mathfrak{q}$ occurs in the prime ideal

factorization of the fractional ideal xO_K. So we find that $|x|_v = 1$ for almost all places v.

We claim that if p is a prime number, or if $p = \infty$, we have $N_{K/\mathbb{Q}}(x) = \prod_{v|p} N_{K_v/\mathbb{Q}_p}(x)$. Here, we write $v|\infty$ to mean that v is archimedean. For finite places we have seen this in Corollary 5.51. For $p = \infty$, we have

$$\begin{aligned} N_{K/\mathbb{Q}}(x) &= \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \tau(x) \\ &= \prod_{\tau \text{ real}} \tau(x) \cdot \prod_{\tau \text{ complex}} \tau(x) \\ &= \prod_{K_v = \mathbb{R}} x \cdot \prod_{K_v = \mathbb{C}} x\overline{x} \\ &= \prod_{v|\infty} N_{K_v/\mathbb{R}}(x), \end{aligned}$$

since for every complex embedding τ, its conjugate $\overline{\tau}$ also appears.

Now we prove the product formula. By Lemma 6.21 we get

$$\prod_{v \text{ place of } K} |x|_v = \prod_{p \text{ place of } \mathbb{Q}} \prod_{v|p} |x|_v = \prod_{p \text{ place of } \mathbb{Q}} \prod_{v|p} |N_{K_v/\mathbb{Q}_p}(x)|_p.$$

By what we proved above we find

$$\prod_{p \text{ place of } \mathbb{Q}} \prod_{v|p} |N_{K_v/\mathbb{Q}_p}(x)|_p = \prod_{p \text{ place of } \mathbb{Q}} |N_{K/\mathbb{Q}}(x)|_p = 1,$$

using the product formula for $\mathbb{Q}$. □

Definition 6.24. A *global field* is a field K together with a set of places satisfying the following conditions.

(a) There exist representatives $|\cdot|_v$ of the given places such that for all $x \in K^\times$ we have $|x|_v = 1$ for almost all places v, and the product formula is satisfied, i.e.

$$\prod_v |x|_v = 1.$$

(b) There exists a place v such that K_v is a local field.

Corollary 6.25. *Number fields are global fields.*

Remark 6.26. One can show that if K is a global field, there are two cases.

(1) Either $\mathrm{char}(K) = 0$, and K is a number field, or
(2) $\mathrm{char}(K) = p > 0$, and K is a finite extension of $\mathbb{F}_p(T)$.

The fields in case (2) arise as function fields of curves over finite fields.

For the proof of this fact we refer to [AW45].

7. Adeles and ideles

In this section, we introduce the notion of adeles and ideles. They give a convenient way of considering all completions of a global field at once, and allow us to study number theory using topological and analytic methods. After introducing adeles and ideles, we will use these objects to prove two classic results in algebraic number theory. For that, recall the fundamental exact sequence

$$1 \to O_K^\times \to K^\times \to \mathrm{Div}(O_K) \to \mathrm{Cl}(O_K) \to 1$$

for a number field K (recall that $\mathrm{Div}(O_K)$ is the group of fractional ideals of O_K). We will prove Dirichlet's unit theorem, which says that $O_K^\times$ is finitely generated, and the number of generators is explicit in terms of real and complex embeddings of K. After that, we will prove finiteness of the class group $\mathrm{Cl}(K)$.

We will often use the terminology *almost all*, meaning all but finitely many.

7.1. **Restricted product.**

Definition 7.1. Let $(X_i)_{i\in I}$ be a family of topological spaces. For almost all $i \in I$ let $O_i \subset X_i$ be an open subspace. Define

$$X := \prod_{i\in I}{}' := \{(x_i) \in \prod_{i\in I} X_i \mid x_i \in O_i \text{ for almost all } i\}.$$

We endow X with a topology by giving a basis for it. The basis consists of those sets $\prod_{i\in I} U_i$ with $U_i \subset X$ open, for which $U_i = O_i$ for almost all $i \in I$. We call X with this topology the *restricted product of the X_i with respect to the O_i*. Often, the O_i will be implicit, and we simply refer to X as the restricted product.

Define $I_f := \{i \in I \mid \text{There exists an } O_i \subset X_i\}$, and $I_\infty = I \setminus I_f$ (which is a finite set). For a finite subset $S \subset I$ with $S \supset I_\infty$ define moreover

$$X_S := \prod_{i\in S} X_i \times \prod_{i\in I\setminus S} O_i \subset X,$$

which is an open subspace in X. For two finite subsets $S \subset S' \subset I$ with $I_\infty \subset S \subset S'$ we have $X_S \subset X_{S'}$ and

$$X = \bigcup_{\substack{S\subset I \text{finite} \\ S\supset I_\infty}} X_S.$$

Proposition 7.2. *Let X_i and O_i be as above. Assume every X_i is locally compact, and every O_i is compact. Then, the restricted product $\prod'_{i\in I} X_i$ is locally compact.*

Proof. For any finite $S \supset I_\infty$, the space X_S is locally compact. This follows from the fact that finite products of locally compact spaces are locally compact. Moreover, every $X_S \subset X$ is open, and ranging over finite S, the X_S cover X. □

Remark 7.3. Let X_i and O_i be as in Proposition 7.2. For each $i \in I$, let μ_i be a Radon measure on X_i, such that for every $i \in I_f$, the measure is normalized by $\mu_i(O_i) = 1$. We can endow $X = \prod'_{i\in I} X_i$ with the product measure μ. This works as follows. The Borel σ-algebra on the product is generated by subsets $\prod_{i\in I} M_i$ where $M_i \subset X_i$ is compact and $M_i = O_i$ for almost all $i \in I$. Then,

$$\mu(\prod_{i\in I} M_i) = \prod_{i\in I} \mu_i(M_i),$$

which is well-defined since $\mu(M_i) = \mu(O_i) = 1$ for almost all $i \in I$. Note that the restriction of μ to $\prod_{i\in I_f} O_i$ is the product probability measure.

Remark 7.4 (Modulus)**.** Suppose $X_i = G_i$ is a locally compact topological group, $O_i \subset G_i$ is an open compact subgroup for $i \in I_f$. Moreover, for each $i \in I$, let $\alpha_i : G_i \xrightarrow{\sim} G_i$ be an automorphism of topological groups which induces an automorphism

$$\alpha_i : O_i \xrightarrow{\sim} O_i$$

for almost all $i \in I_f$. Let $G := \prod'_{i\in I} G_i$. Then,

$$\alpha : G \to G$$
$$(g_i)_{i\in I} \mapsto (\alpha_i(g_i))_{i\in I}$$

is an automorphism of topological groups. If $\alpha_i(O_i) = O_i$, then $|\alpha_i|_{G_i} = 1$ (since $\mu_i(O_i) = \mu_i(\alpha_i(O_i)) = |\alpha_i|_{G_i}\mu_i(O_i)$), and moreover $|\alpha|_G = \prod_{i\in I} |\alpha_i|_{G_i}$. Indeed, let $C_i \in G_i$ be a compact neighborhood of e, and assume $C_i = O_i$ for $i \in I_f$. Then, we have

$$\mu(\alpha(\prod_i C_i)) = \mu(\prod_i \alpha_i(C_i)) = \prod_i \mu_i(\alpha_i(C_i))$$
$$= \prod_i |\alpha_i|_{G_i}\ \mu_i(C_i) = \left(\prod_{i\in I} |\alpha_i|_{G_i}\right) \mu(\prod_i C_i).$$

7.2. **Adeles and ideles.**

Definition 7.5. Let K be a number field, $V := V_K$ its set of places. For $v \in V$ we let K_v be the completion of K with respect to v. Moreover, we let V_f be the set of non-archimedean (also called finite) places, and V_∞ the set of archimedean places. For each $v \in V_f$ let $O_v \subset K_v$ be the corresponding complete DVR. The *ring of adeles of* K is the restricted product

$$\mathbb{A}_K := \prod_{v\in V}{}' K_v$$

with respect to the O_v. It is a topological ring with respect to componentwise addition and multiplication. Moreover, we let

$$\mathbb{A}_{K,f} = \prod_{v\in V_f}{}' K_v$$

be the ring of finite adeles. Note that $\mathbb{A}_K = \mathbb{A}_{K,f} \times \prod_{v\in V_\infty} K_v$, and that $\mathbb{A}_K$ is locally compact.

Exercise 7.6. Prove the following isomorphisms. We have

$$\mathbb{A}_{\mathbb{Q},f} \cong (\prod_{p \text{ prime}} \mathbb{Z}_p) \otimes_{\mathbb{Z}} \mathbb{Q}, \text{ and}$$

$$\mathbb{A}_{\mathbb{Q}} / (\mathbb{R} \times \prod_{p \text{ prime}} \mathbb{Z}_p) \cong \bigoplus_{p \text{ prime}} \mathbb{Q}_p / \mathbb{Z}_p \cong \bigoplus_p \mathbb{Z}[1/p]/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}.$$

Remark 7.7. Let K be a number field. Then the map $K \to \mathbb{A}_K, x \mapsto (x, x, ...)$ is a well-defined injective ring homomorphism. Indeed, we have to show that for $x \in K^\times$ we have $x \in O_v$ for almost all $v \in V_f$. Now xO_K is a fractional ideal, so in its prime ideal decomposition only finitely many different prime ideals appear. This implies $|x|_v = 1$ for almost all $v \in V_f$. For these v we even have $x \in O_v^\times$.

The following is one of the most important properties of the adele ring. It is the one of the main results of this chapter.

Theorem 7.8. *Let K be a number field. Then $K \subset \mathbb{A}_K$ is discrete, and the quotient group $\mathbb{A}_K /K$ is compact. In fact, $\mathbb{A}_K/K$ is the Pontryagin dual of $(K, +)$ endowed with the discrete topology.*

We will postpone the proof until the end of this chapter, and first reap some consequences.

Remark 7.9. Removing even a single place makes the situation completely different. This is the content of the next theorem, for which we introduce some notation first.

Definition 7.10. For $x = (x_v) \in \mathbb{A}_K$, we will write $|x|_v = |x_v|_v$, where $|\cdot|_v$ denotes the modulus on K_v. We define a group homomorphism $|\cdot| : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$ by $(x_v)_{v \in V_K} \mapsto \prod_{v \in V_K} |x|_v$. Note that almost all $|x_v|_v = 1$. Let $\mathbb{A}_K^1 := \ker(|\cdot|) = \{x \in \mathbb{A}_K^\times \mid |x| = 1\}$.

We will also write $|x| = \prod_{v \in V_K} |x|_v$ for any $x \in \mathbb{A}_K$ for the *adelic norm*.

Remark 7.11. For $x \in \mathbb{A}_K$, the adelic norm $|x|$ converges to zero unless $|x|_v = 1$ for almost all places $v \in V_K$. In this case $|x|$ is essentially a finite product. This can be seen as follows. First note that $|x|_v \leq 1$ for almost all v. Moreover, for an infinite product $\prod_{n=1}^\infty x_n$ of real numbers $0 < x_n < 1$ one has $\prod_{n=1}^\infty x_n > 0$ only if the sequence (x_n) converges to 1. However, when v is non-archimedean, and $|x|_v < 1$, then $|x|_v$ is bounded by $1/2$, because $|x|_v$ is of the form p^{-f_v} for some prime number p. So if $|x|_v < 1$ for infinitely many v, then $|x|$ converges to 0 (as the corresponding sequence cannot converge to 1).

Theorem 7.12 (Strong approximation)**.** *Let K be a number field, and let V_K be its set of places. Fix a decomposition $V_K = S \cup T \cup \{w\}$, where S is finite, and the union is disjoint. Given $a_v \in K_v$ and $\varepsilon_v \in \mathbb{R}_{>0}$ for $v \in S$, there exists an $x \in K$ with $|x - a_v|_v < \varepsilon_v$ for all $v \in S$, and $|x|_v \leq 1$ for all $v \in T$.*

We will need the following result for the proof.

Lemma 7.13 (Adelic Blichfeldt-Minkowsi lemma)**.** *Let K be a number field. Then there is a constant $B \in \mathbb{R}_{>0}$ depending only on K, such that for all $a \in \mathbb{A}_K$ with $|a| > B$ there exists a non-zero $x \in K \subset \mathbb{A}_K$ with $|x|_v \leq |a|_v$ for all $v \in V_K$.*

Proof. Denote by μ the product measure on $\mathbb{A}_K$ normalized with respect to each O_v. Let b_0 be the measure of a fundamental region for K in $\mathbb{A}_K$. Since $\mathbb{A}_K/K$ is compact, $b_0 < \infty$. Moreover, define

$$b_1 = \mu(\{z \in \mathbb{A}_K \mid |z|_v \leq 1 \text{ for all } v, |z|_v \leq \frac{1}{4} \text{ for archimedean } v\}).$$

Note that $b_1 \neq 0$, since there are only finitely many archimedean places (if not, the measure may converge to zero). Define $B := b_0/b_1$, and assume $a \in K$ satisfies $|a| > B$. We know that $|a| \leq 1$ for almost all places ν, so $|a| > B_K$ implies $|a|_v = 1$ for almost all ν.

Define $M := \{z \in \mathbb{A}_K \mid |z|_v \leq |a|_v \text{ for all } v, |z|_v \leq \frac{1}{4}|a|_v \text{ for archimedean } v\}$. Then

$$\mu(M) = b_1|a| > b_1 B = b_0,$$

because μ is the normalized product measure. Now $\mu(M) > b_0$, which implies that M is not contained in any fundamental region for $K \subset \mathbb{A}_K$. This means, there exist $z_1, z_2 \in M$ with $z_1 \neq z_2$, and with the same image in $\mathbb{A}_K\ /K$. In other words, $x = z_1 - z_2 \in K^\times\ \subset K \subset \mathbb{A}_K$.

Now, we use the triangle inequalities (strong for non-archimedean places), to conclude that

$$|x|_v\ \leq \begin{cases} \max\{|z_1|_v, |z_2|_v\} \leq |a|_v, v \text{ non-archimedean,} \\ |z_1|_v + |z_2|_v\ \leq 2\ \cdot \frac{1}{4}\ |x|_v \leq \frac{1}{2}\ |a|_v, v \text{ real,} \\ (|z_1 - z_2|_v^{1/2})^2 \leq (|z_1|_v^{1/2} + |z_2|_v^{1/2})^2 \leq (2 \cdot \frac{1}{2}|a|_v^{1/2})^2 = |a|_v, v \text{ complex.} \end{cases}$$

Here, note that for v complex, the square-root of the modulus is the usual absolute value on $\mathbb{C}$. Altogether we find $|x|_v\ \leq |a|_v$ for all $v \in V_K$. □

Proof of the strong approximation theorem. Let $W = \{z \in \mathbb{A}_K\ \mid |z|_v\ \leq 1$ for all $v \in V_K\ \}$. When we prove compactness of $\mathbb{A}_K/K$ we will see a slightly more refined statement. Namely, W contains a complete set of representatives for $K \subset \mathbb{A}_K$ (actually we will see a slight variant, but it is not difficult to conclude the desired statement).

This implies $\mathbb{A}_K = K + W$, and even more, if $u \in K \subset \mathbb{A}_K$ is non-zero, then $\mathbb{A}_K = K + uW$. Indeed, given $c \in \mathbb{A}_K$, we can write $u^{-1}c \in \mathbb{A}_K$ as $u^{-1}c = a + b$ with $a \in K$ and $b \in W$. This implies $c = ua + ub$ with $ua \in K$, and $ub \in uW$.

Let B be as in the Blichfeldt-Minkowski lemma, and choose $z \in \mathbb{A}_K$ satisfying the following properties.

(i) For all $v \in S$, we have $0 < |z|_v < \varepsilon_v$,
(ii) for all $v \in T$ we have $0 < |z|_v \leq 1$,
(iii) and $|z|_w > B \prod_{v \neq w} .|z|_v^{-1}$.

This is clearly possible (simply choose each component of z in a suitable way). Note that at this point, you do not have control over the size of $|z|_w$ anymore. This is the reason we need to remove at least a single place from V_K.

Then $|z|\ > B$, and we can apply the above Lemma, to find a non-zero $u \in K \subset \mathbb{A}_K$ with $|u|_v \leq |z|_v$ for all $v \in V_K$. Now we finish the proof. Let $a = (a_v) \in \mathbb{A}_K$ with $a_v = 0$ for $v \notin S$, and a_v given by the hypothesis of the theorem for $v \in S$. We will find an $x \in K$ satisfying the desired properties.

Note that $\mathbb{A}_K = K + uW$, for the u we just found. Therefore $a = x + y$ with $x \in K$ and $y \in uW$. We claim that this x is the one we are looking for. Indeed, since $u^{-1}y \in W$, we have $|u^{-1}y|\ \leq 1$, and we get

$$|x - a_v|_v = |y|_v \leq |u|_v\ \leq |z|_v \leq \begin{cases} \varepsilon_v, & v\ \in S \\ 1, & v\ \in T. \end{cases}$$

This proves the claim. □

Corollary 7.14. *Let K be a number field, and let w be any place of K. Then $K \subset \prod'_{v \in V_K \setminus \{w\}} K_v$ is dense.*

Exercise 7.15. The strong approximation theorem is a direct generalization of the Chinese remainder theorem for the ring of integers O_K of K. Deduce the Chinese remainder theorem from it.

Definition 7.16. Let K be a number field. The restricted product $\mathbb{A}_K^\times := \prod'_{v \in V_K} K_v^\times$ is called the *idele group of K*.

Remark 7.17. The topology on $\mathbb{A}_K^\times$ is the one coming from its structure as restricted product. Even though $\mathbb{A}_K^\times$ is the group of units of $\mathbb{A}_K$, the topology on it is not the subspace topology.

Exercise 7.18. For $n \geq 1$ define $a_n \in \mathbb{A}_{\mathbb{Q}}^\times$ as follows. Its $\mathbb{R}$-component is 1, and its $\mathbb{Q}_p$-component is $n! + 1$ for every prime number p. Show that $(a_n)_n$ converges to 1 in $\mathbb{A}_{\mathbb{Q}}$, but in $\mathbb{A}_{\mathbb{Q}}^\times$ it does not converge to 1.

Proposition 7.19. *There is a well-defined injective group homomorphism $K^\times \mapsto \mathbb{A}_K^1$, defined by $x \mapsto (x, x, ...)$.*

Proof. This follows from the product formula for K. □

Here is the second main theorem of this chapter, whose proof we also postpone.

Theorem 7.20. *The subspace $K^\times \subset \mathbb{A}_K^1$ is discrete, and $\mathbb{A}_K^1 / K^\times$ is compact.*

Definition 7.21. Let $S \subset V_K$ be a finite set of places containing V_∞. The ring of S-integers is

$$O_S = \{x \in K \mid x \in O_v \text{ for all } v \notin S\} = \cap_{v \in V_K \setminus S} O_{K,\mathfrak{q}_v},$$

with unit group $O_S^\times = \{x \in K^\times \mid x \in O_v^\times \text{ for all } v \notin S\}$.

Example 7.22. (1) Let $S = V_\infty$, then $O_S = O_K$.

(2) Let $K = \mathbb{Q}$, $S = \{\infty, p_1, ..., p_r\}$ for some prime numbers p_i. In this case,

$$O_S = \mathbb{Z}\left[p_1^{-1}, ..., p_r^{-1}\right].$$

Note that this is the set of all $\frac{a}{s}$ with $a \in \mathbb{Z}$, and $s \in \mathbb{Z} \setminus \{0\}$ where the only prime divisors allowed for s are the p_i.

Consider the map $R_S : O_S^\times \to \prod_{v \in S} \mathbb{R}, x \mapsto (\log(|x|_v))_{v \in S}$, which is a group homomorphism. For $x \in O_S^\times$ we have $|x|_v = 1$ for all $v \notin S$, so by the product formula, we have $\prod_{v \in S} |x|_v = 1$.

Therefore, defining $\left(\prod_{v \in S} \mathbb{R}\right)^\circ := \{(c_v)_{v \in S} \in \prod_{v \in S} \mathbb{R} \mid \sum_{v \in S} c_v = 0\}$, we find that $\mathrm{Im}(R_S) \subset \left(\prod_{v \in S} \mathbb{R}\right)^\circ$.

Proposition 7.23. *In the above situation, we have that $R_S(O_S^\times) \subset \left(\prod_{v \in S} \mathbb{R}\right)^\circ$ is discrete, $\ker(R_S)$ is finite, and the quotient $\left(\prod_{v \in S} \mathbb{R}\right)^\circ / R_S(O_S^\times)$ is compact.*

Proof. We omit this proof and refer to [Lan94, Chapter VII, §3]. □

7.3. **Dirichlet's unit theorem.** Assuming the main properties of adeles and ideles in Theorem 7.8, Theorem 7.20, and Proposition 7.23, we can derive Dirichlet's unit theorem without too much work. First, we need a preparatory result.

Lemma 7.24. *Let V be an n-dimensional real vector space, and $\Gamma \subset V$ a discrete subgroup such that V/Γ is compact. Then, there exists a basis $e_1, ..., e_n$ of V such that $\Gamma = \bigoplus_{i=1}^n \mathbb{Z} e_i$.*

Proof. Let V' be the subvector space of V generated by Γ. Then we have a surjective continuous homomorphism $V/\Gamma \to V/V'$. Since V/Γ is compact, so is V/V'. This can only happen if $V = V'$. Therefore, Γ contains a basis $e_1, ..., e_n$ of V. Define $\Gamma' := \bigoplus_{i=1}^n \mathbb{Z} e_i \subset \Gamma$. Then, $V/\Gamma' = \bigoplus_{i=1}^n \mathbb{R}/\mathbb{Z}$ is compact. Note that

$$\Gamma/\Gamma' = \ker(V/\Gamma' \to V/\Gamma) \subset V/\Gamma'$$

is closed in V/Γ', so Γ/Γ' is compact. Since Γ is discrete, the quotient Γ/Γ' has to be finite. This means there exists an integer $m \geq 1$ such that $\Gamma \subset \frac{1}{m}\,\Gamma'$. The claim now follows from the elementary divisor theorem (it implies submodules of free modules over principal ideal domains are free). □

Theorem 7.25. *Let K be a number field, S a finite set of places containing V_∞. Moreover, let $r := \#S - 1$. Then we have*

$$O_S^\times \cong \mathbb{Z}^r \oplus \mu(K),$$

where $\mu(K) = \{\zeta \in K \mid \text{there exists } n \geq 1 : \zeta^n = 1\}$ is a finite group.

Proof. Consider the exact sequence

$$1 \to \ker(R_S) \to O_S^\times \xrightarrow{R_S} \mathrm{Im}(R_S) \to 0.$$

By Proposition 7.23, the subspace $\mathrm{Im}(R_S) \subset \left(\prod_{v\in S} \mathbb{R}\right)^\circ$ is discrete with compact quotient, and $\ker(R_S)$ is finite. Therefore we can apply Lemma 7.24 to conclude that $\mathrm{Im}(R_S) \cong \mathbb{Z}^r$ is free (note that $r = \dim\left(\prod_{v\in S} \mathbb{R}\right)^\circ$). This implies that the above exact sequence splits, so $O_S^\times \cong \mathbb{Z}^r \oplus \ker(R_S)$. It only remains to show that $\ker(R_S) = \mu(K)$. For this, we check that $\mu(K) \subset \ker(R_S)$. Indeed, $\mu(K) \subset O_K^\times \subset O_S^\times$ is clear. If $\zeta \in \mu(K)$ with $\zeta^n = 1$, then we have

$$0 = R_S(\zeta^n) = nR_S(\zeta)$$

inside a real vector space, implying $R_S(\zeta) = 0$. Vice versa, $z \in \ker(R_S)$ if and only if $|z|_v = 1$ for all $v \in S$. So for any integer m, if $z \in \ker(R_S)$, we have $z^m \in \ker(R_S)$. Since $\ker(R_S)$ is finite, there exists an m with $z^m = 1$. □

Corollary 7.26 (Dirichlet's unit theorem)**.** *Let K be a number field. Then*

$$O_K^\times \cong \mathbb{Z}^m \oplus \mu(K),$$

where $m = \#V_\infty - 1 = r + s - 1$ with r equal to the number of real embeddings $K \hookrightarrow \mathbb{C}$, and s equal to half the number of complex embeddings $K \hookrightarrow \mathbb{C}$, and $\mu(K)$ is a finite group of units in K.

Example 7.27. (1) We have $\mathbb{Z}^\times = \mu(\mathbb{Q}) = \{\pm 1\}$.

(2) Let $K = \mathbb{Q}[\sqrt{d}]$ for $d \in \mathbb{Z}$ square-free. Then we have two cases.
   (a) If $d > 0$, then the $\mathbb{Q}$-embeddings $K \to \mathbb{C}$ given by $\sqrt{d} \mapsto \pm\sqrt{d}$ are real. Therefore, K has two archimedean places, given by $|x|_1 = |a + b\sqrt{d}|$ and $|x|_2 = |a - b\sqrt{d}|$. This implies $O_K^\times = \mathbb{Z} \oplus \mu(K)$.
   (b) If $d < 0$, then the $\mathbb{Q}$-embeddings $K \to \mathbb{C}$ are complex. Therefore K has a single archimedean place, and $O_K^\times$ is finite. E.g. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

(3) Let $K = \mathbb{Q}$, $S = \{\infty, p\}$ for a prime number p. In this case, we have $O_S = \mathbb{Z}[\frac{1}{p}]$, and $O_S^\times = \{\pm p^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mu(K)$.

Exercise 7.28. (1) Let K be a number field. Show

$$O_K^\times = \{x \in O_K \mid N_{K/\mathbb{Q}}(x) \in \{\pm 1\} = \mathbb{Z}^\times\}.$$

(2) Give an elementary proof that $O_K^\times$ is finite for $K = \mathbb{Q}[\sqrt{d}]$ with $d \in \mathbb{Z}, d < 0$ square-free.

7.4. **Finiteness of the class group.**

Definition 7.29. Let K be a number field. The group $\mathrm{Cl}(K) = \mathrm{Div}(O_K)/\mathrm{PrincDiv}(O_K)$ is called the *class group of* K. The number $h_K := \#\mathrm{Pic}(O_K)$ is called the *class number of* K.

Remark 7.30. Recall that $h_K = 1$ if and only if O_K is a principal ideal domain. Since O_K is a Dedekind domain, this is also equivalent to O_K being a unique factorization domain.

Before proving finiteness of the class number h_K, let us explain the relation to ideles. Let K be a number field, and consider the open subspace

$$U = \prod_{v \in V_\infty} K_v^\times \times \prod_{v \in V_f} O_v^\times \ \subset \mathbb{A}_K^\times.$$

The normalized valuation on K_v induces an isomorphism $K_v^\times/O_v^\times \xrightarrow{\sim} \mathbb{Z}$. This gives an isomorphism

$$\mathbb{A}_K^\times/U = \bigoplus_{v \in V_f} K_v^\times/O_v^\times \cong \bigoplus_{v \in V_f} \mathbb{Z} \cong \mathrm{Div}(O_K).$$

Definition 7.31. We call $C_K := \mathbb{A}_K^\times/K^\times$ be the *idele class group*.

Remark 7.32. We now have

$$\begin{aligned}\mathrm{Cl}(K) &= \mathrm{coker}(K^\times \to \mathrm{Div}(O_K)) \cong \mathrm{coker}(K^\times \to \mathbb{A}_K^\times/U) \\ &\cong \mathbb{A}_K^\times/(U \cdot K^\times) \cong C_K/\overline{U},\end{aligned}$$

where $\overline{U}$ is the image of U in C_K. Let I be a fractional ideal. We describe its image in $C_K/\overline{U}$ under the above isomomorphism. For each $v \in V_f$, let x_v be a generator of $I_v = I \otimes_{O_K} O_v$, which is a fractional ideal of O_v. For $v \in V_\infty$, choose x_v arbitrary. Then I is mapped to the class of $(x_v) \in \mathbb{A}_K^\times$.

Theorem 7.33. *Let K be a number field. The class group $\mathrm{Cl}(K)$ is finite.*

Proof. Since $\mathrm{Cl}(K) \cong C_K/\overline{U}$, it suffices to show that the latter is discrete and compact.

First we show that $C_K/\overline{U}$ is discrete. For this recall the following general facts.

Lemma 7.34. *Let G be a topological group, and $H \subset G$ a subgroup. Then the projection $G \to G/H$ is open, and $H \subset G$ is open if and only if G/H is discrete. Moreover, G/H is Hausdorff if and only if H is closed in G.*

Projections being open maps implies that $\overline{U} \ \subset C_K$ is open (since $U \subset \mathbb{A}_K^\times$ is open). Further, $\overline{U} \subset C_K$ being open implies that the quotient is discrete.

Now we show that $C_K/\overline{U}$ is compact. By Theorem 7.20, the quotient $\mathbb{A}_K^1/K^\times$ is compact. Therefore it suffices to show that the map

$$f : \mathbb{A}_K^1/K^\times \hookrightarrow C_K \ \twoheadrightarrow C_K/\overline{U} = \mathbb{A}_K^\times/(K^\times U)$$

is surjective (because in that case $C_K/\overline{U}$ is the image of a compact space under a continuous map). For this we need to show that $U\mathbb{A}_K^1 = \mathbb{A}_K^\times$.

Let v be an archimedean place of K. For $a \in \mathbb{A}_K^\times$ choose $b \in K_v^\times$ with $|b|_{K_v} = |a| \in \mathbb{R}_{>0}$. You can think of b as an element of $\mathbb{A}_K^\times$ with v'-component equal to 1 for every $v' \neq v$. Then $|b| = |a|$ and $b \in U$. Thus, $a = (ab^{-1})b$ with $ab^{-1} \in \mathbb{A}_K^1$ and $b \in U$. $\square$

Remark 7.35. Note that in the above proof we had to choose an archimedean place of K. We could only do this because K is number field. For a global field of positive characteristic, i.e. a finite extension of $\mathbb{F}_p(T)$ we could not have found an archimedean place.

Remark 7.36. Class numbers are still not well understood. Here is a selection of open problems.

(1) Do there exist infinitely many square-free $d > 1$ with $\mu_{\mathbb{Q}[\sqrt{d}]} = 1$? Conjecturally, the answer is yes, and about 75% of them should have class number equal to 1. This sometimes goes by the name *Cohen-Lenstra heuristics*, see [CL84].
(2) Do there exist infinitely many primes p such that $p \nmid h_{\mathbb{Q}[\zeta_p]}$, where $\zeta_p = \exp(2\pi i/p)$ is a primitive p-th root of unity? Such a prime is sometimes called a *regular prime*.

7.5. **Proof of the main theorems.** In the previous sections, we saw that the main input in proving the Dirichlet unit theorem, and finiteness of the class group, were Theorem 7.8, Theorem 7.20, and Proposition 7.23. In this section, we will prove this results.

Proof of Theorem 7.8. The rough idea is to prove the theorem first for $K = \mathbb{Q}$, and deduce it for general K from this version. So assume $K = \mathbb{Q}$. We prove that $\mathbb{Q} \subset \mathbb{A}_\mathbb{Q}$ is discrete. For this, it suffices to find an open neighborhood $U \subset \mathbb{A}_\mathbb{Q}$ of 0 for which $U \cap \mathbb{Q} = \{0\}$ (in that case, 0 is open in $\mathbb{Q}$, and we can translate to prove the same for every $x \in \mathbb{Q}$).

Consider the open subspace $U = (-1/2, 1/2) \times \prod_{p \text{ prime}} \mathbb{Z}_p \subset \mathbb{A}_\mathbb{Q}$. If $x \in \mathbb{Q} \cap U$, then considered as element in $\mathbb{Q}_p$ we have $x \in \mathbb{Z}_p$ for every prime. This means no prime appears with a negative exponent in the prime decomposition of x, hence $x \in \mathbb{Z}$. But since $x \in (-1/2, 1/2)$ we need to have $x = 0$.

We now prove that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact. Let $J := [-1/2, 1/2] \subset \mathbb{R}$. We claim that in $\mathbb{A}_\mathbb{Q}$ we have

$$\left(J \times \prod_{p \text{ prime}} \mathbb{Z}_p \right) + \mathbb{Q} = \mathbb{A}_\mathbb{Q},$$

where $\mathbb{Q}$ is diagonally embedded. From Exercise 7.6 we know that

$$\mathbb{A}_\mathbb{Q}/(\mathbb{R} \times \prod_p \mathbb{Z}_p) = \mathbb{Q}/\mathbb{Z}.$$

This implies $\mathbb{Q} + (\mathbb{R} \times \prod_p \mathbb{Z}_p) = \mathbb{A}_\mathbb{Q}$. So let $x \in \mathbb{A}_\mathbb{Q}$ with $x = (q + r, (y_p + q)_p)$ for some $q \in \mathbb{Q}, r \in \mathbb{R}, y_p \in \mathbb{Z}_p$. We can choose $n \in \mathbb{Z}$ with $r - n \in J$. Then $x = ((q+n) + (r-n), (y_p - n + q + n)_p)$, where $q + n \in \mathbb{Q}$, $r - n \in J$, $y_p - n \in \mathbb{Z}_p$, and $q + n \in \mathbb{Q}$.

We go on to prove the claim for a general number field K. We will use the following statement.

Proposition 7.37. *Let $L \supset K$ be an extension of number fields. Then the map defined by*

$$\begin{aligned} \mathbb{A}_K \otimes_K L &\to \mathbb{A}_L \\ (x_v) \otimes y &\mapsto (z_w) \end{aligned}$$

with $z_w = x_v y$ for $w \mid v$ is an isomorphism of topological rings.

Proof. We have

$$\mathbb{A}_K \otimes_K L \cong \prod\nolimits'_{v \in V_K} (K_v \otimes_K L)$$

where the restricted product is taken with respect to the compact open subgroups $O_v \otimes_{O_K} O_L$, and the map is given by $(x_v) \otimes y \mapsto (x_v \otimes y)$. Moreover, we have $\mathbb{A}_L = \prod'_{w \in V_L} L_w$, taken with respect to the open compact subgroups O_w.

We have seen in Theorem 5.47 that $K_v \otimes_K L \cong \prod_{w|v} L_w$ for each non-archimedean place v. For an archimedean place v this follows from Proposition 6.19. Therefore, the proof follows from the next result. □

Proposition 7.38. *Let A be a Dedekind domain, $\mathfrak{p} \in \operatorname{Spec} A$ a non-zero prime ideal, $L \supset K = \operatorname{Frac}(A)$ a finite separable extension, B the integral closure of A in L. Then, we have an isomorphism*

$$\widehat{A}_\mathfrak{p} \otimes_A B \cong \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}.$$

Proof. Let $n = [L : K]$, then B is a finitely generated projective A-module of rank n. This implies that after extension of scalars, $\widehat{A}_\mathfrak{p} \otimes_A B$ is a finitely generated free $\widehat{A}_\mathfrak{p}$-module of rank n (since $\widehat{A}_\mathfrak{p}$ is a principal ideal domain, projective implies free).

We have seen before that $n = \sum_{\mathfrak{q}|\mathfrak{p}} [L_\mathfrak{q} : K_\mathfrak{p}]$, so that $\prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}$ is a free $\widehat{A}_\mathfrak{p}$-module of rank n. It therefore suffices to show that the natural map $\widehat{A}_\mathfrak{p} \otimes_A B \to \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}$ is surjective.

Applying Nakayama's lemma to the cokernel of this map (if it vanishes modulo the maximal ideal, then it is zero), it suffices to prove this after modding out the maximal ideal $\widehat{\mathfrak{p}} \subset \widehat{A}_\mathfrak{p}$. This puts us in the following situation. Since $\widehat{A}_\mathfrak{p}/\widehat{\mathfrak{p}} = A/\mathfrak{p}$, we have

$$\widehat{A}_\mathfrak{p}/\widehat{\mathfrak{p}} \otimes_{\widehat{A}_\mathfrak{p}} \widehat{A}_\mathfrak{p} \otimes_A B = A/\mathfrak{p} \otimes_A B = B/\mathfrak{p}B.$$

Morever, we also have by the Chinese remainder theorem that

$$B/\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}/\widehat{\mathfrak{q}}^{e_{\widehat{\mathfrak{q}}}} = \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}/\widehat{\mathfrak{p}}\widehat{B}_\mathfrak{q} = \widehat{A}_\mathfrak{p}/\widehat{\mathfrak{p}} \otimes_{\widehat{A}_\mathfrak{p}} \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}.$$

This proves the claim. □

With this in hand, we can prove that $\mathbb{A}_K/K$ is compact. Let $m := [K : \mathbb{Q}]$. By Proposition 7.37, we find that $\mathbb{A}_\mathbb{Q}^m \cong \mathbb{A}_K$ as topological $\mathbb{A}_\mathbb{Q}$-modules, where the isomorphism restricts to the identification $\mathbb{Q}^m \cong K$. We conclude that

$$\mathbb{A}_K/K \cong (\mathbb{A}_\mathbb{Q}/\mathbb{Q})^m.$$

Since we know that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact by the first part of the proof, we conclude that $\mathbb{A}_K/K$ is compact. □

Remark 7.39. We can now give an alternative and very short proof of the product formula for the number field K. Let $a \in K^\times$. Then multiplication with a is an isomorphism $\mathbb{A}_K \xrightarrow{\sim} \mathbb{A}_K$ which induces an isomorphism $K \xrightarrow{\sim} K$. Therefore, by Remark 7.4 we have

$$\prod_{v \in V_K} |a|_\nu = |a|_{\mathbb{A}_K} = |a|_K |a|_{\mathbb{A}_K/K} = 1,$$

where the second equality follows from Theorem 6.8, $|a|_{\mathbb{A}_K/K} = 1$, because the quotient is compact (see Example 6.10), and $|a|_K = 1$, because $K \subset \mathbb{A}_K$ is discrete (see Exercise 6.11)

The next goal is to prove Theorem 7.20, which says that $\mathbb{A}_K^1/K^\times$ is compact, and $K^\times \subset \mathbb{A}_K^1$ is discrete.

Lemma 7.40. *Let K be a number field, $b, c \in \mathbb{R}_{>0}$ with $b \geq c > 0$. Then the following holds.*

(1) The subspace $\{x \in \mathbb{A}_K^\times \mid |x| \geq c\} \subset \mathbb{A}_K^\times$ is closed in $\mathbb{A}_K$, and the subspace topologies as a subset of $\mathbb{A}_K$ and as a subset of $\mathbb{A}_K^\times$ coincide.

(2) The subspace $\{x \in \mathbb{A}_K^\times \mid b \geq |x| \geq c\}$ is closed in $\mathbb{A}_K$.

Proof. First we show that (1) implies (2). The modulus $\mathbb{A}_K^\times \to \mathbb{R}_{>0}$, mapping $x \to |x|$ is continuous. This is a general fact for locally compact groups. Note however that $\mathbb{A}_K \to \mathbb{R}_{\geq 0}, x \mapsto |x|$ ist not continuous, only the map $x \mapsto |x_v|_v$ is continuous for all $v \in V_K$.

This immediately implies that $\{x \in \mathbb{A}_K^\times \mid b \geq |x| \geq c\} = |\cdot|^{-1}([b,c]) \subset \mathbb{A}_K^\times$ is closed. Note that $|x| \geq b^{-1}$ if and only if $|x^{-1}| \leq b$, so the subspace topology for $\{x \in \mathbb{A}_K^\times \mid b \geq |x| \geq c\}$ as subsets of $\mathbb{A}_K$ and of $\mathbb{A}_K^\times$ agrees. This implies $\{x \in \mathbb{A}_K^\times \mid b \geq |x| \geq c\}$ is closed in $\mathbb{A}_K$.

We now prove (1). First we check that $\{x \in \mathbb{A}_K^\times \mid |x| \geq c\}$ is closed in $\mathbb{A}_K$ by proving that its complement is open. Let $a = (a_v)_{v \in V_K} \in \mathbb{A}_K$ with $|a| < c$. We need to find an open neighborhood $U \subset \mathbb{A}_K$ of a with $|x| < c$ for all $x \in U$.

Let $S \subset V_K$ be a finite subset such that $V_\infty \subset S$, for all $v \notin S$ we have $a_v \in O_v$ and moreover $\prod_{v \in S} |a_v|_v < c$ (this works because $|a|_v = 1$ for all $v \notin S$). Then, since

$$\begin{aligned} \mathbb{A}_K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto \prod_{v \in S} |x|_v \end{aligned}$$

is continuous, the preimage U' of $[0, a)$ is open. Letting U be the intersection of U' and the open set $\prod_{v \in S} K_\nu \times \prod_{v \notin S} O_v$, by construction we have $a \in U$, and for all $x \in U$ we have $\prod_{v \in S} |x|_v < c$, and $x_v \in O_v$ for all $v \notin S$. This implies $|x| \leq \prod_{v \in S} < c$, as required.

Now we check that $\mathbb{A}_K$ and $\mathbb{A}_K^\times$ induce the same topology on $\{x \in \mathbb{A}_K^\times \mid |x| \geq c\}$. For this we need to check that for any open subset W' of $\{x \in \mathbb{A}_K^\times \mid |x| \geq c\}$, there is an open subset W of $\mathbb{A}_K$ with $W' = \{x \in \mathbb{A}_K^\times \mid |x| \geq c\} \cap W$. Here, W' is open for the subspace topology induced from $\mathbb{A}_K^\times$. Let $S \subset V$ be a finite set of places containing V_∞. Then the space

$$G(S) = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} O_v^\times$$

carries the product topology as subset of $\mathbb{A}_K$ but also as subset of $\mathbb{A}_K^\times$ (because S is finite). Therefore it suffices to show the following. For any $a \in \mathbb{A}_K^\times$ with $|a| \geq c$ there exists an neighborhood $U \subset \mathbb{A}_K$ of a such that we have

$$\{x \in \mathbb{A}_K^\times \mid |x| \geq c\} \cap U \subset G(S)$$

for some finite set of places as above.

First, let $S' = V_\infty \cup \{v \in V_f \mid a_v \notin O_v\}$. Choose a real number r satsifying $r > \prod_{v \in S'} |a|_v$ and let U be an open neighborhood of a in $\mathbb{A}_K$ such that for all $x \in U$ we have $\prod_{v \in S'} |x|_v < r$, and $x_v \in O_v$ for $v \notin S'$.

Define $S := S' \cup \{v \in V_f \mid p^{f_v} < rc^{-1}, p \text{ prime with } \mathfrak{q}_v \mid (p)\}$. Note that this is a finite set, since there are only finitely many primes p for which p^{f_v} is bounded by a given number.

We now show that U and S do the job. Let $x \in \mathbb{A}_K^\times \cap U$ with $|x| \geq c$, and let $v \notin S$ (this means that $p^{-f_v} \leq cr^{-1}$). We need to prove that $x \in O_v^\times$.

Note that

$$c \leq |x| \leq |x|_v \prod_{v' \in S'} |x|_{v'} < |x|_v r.$$

Since $x_v \in O_v$, this implies that $1 \geq |x|_v > cr^{-1} \geq p^{-f_v} = |\pi_v|_v$ where $\pi_v \in O_v$ is a uniformizer. Since $|\pi_v|_v$ is the largest value below 1 that $|\cdot|_v$ can attain, we conclude $|x|_v = 1$, so $x_v \in O_v^\times$. □

Proof of Theorem 7.20. First we prove that $K^\times \subset \mathbb{A}_K^1$ is discrete. By Lemma 7.40, the topologies induced on $\mathbb{A}_K^1$ by $\mathbb{A}_K^\times$ and $\mathbb{A}_K$ agrees. Since $K \subset \mathbb{A}_K$ is discrete, so is $K^\times \subset \mathbb{A}_K^1$.

Next we check that $\mathbb{A}_K^1/K^\times$ is compact. It suffices to find a compact subset $C \subset \mathbb{A}_K^1$ for which the natural projection $C \to \mathbb{A}^1/K^\times$ is surjective. This is equivalent to asking that $CK^\times = \mathbb{A}_K^1$.

Let μ' be the quotient Haar measure on $\mathbb{A}_K/K$ with respect to the counting measure on the discrete subspace K. Since $\mathbb{A}_K/K$ is compact, $\mu'(\mathbb{A}_K/K)$ is finite. On the other hand, $\mathbb{A}_K$ is not compact. We will use the following basic fact on Haar measures.

Lemma 7.41. *Let G be a locally compact, but not compact, topological group, $c \in \mathbb{R}$, and μ a Haar measure on G. Then there exists a compact $C \subset G$ such that $\mu(C) > c$.*

Proof. We refer to [Bou04, Chapter VII]. □

We apply this result to $G = \mathbb{A}_K$ and $c = \mu'(\mathbb{A}_K/K)$. We can therefore find a compact subset $C_0 \subset \mathbb{A}_K$ with $\mu(C_0) > c = \mu'(\mathbb{A}_K/K)$. Define $C_1 := \{y - z \mid y, z \in C_0\}$ and let $C := C_1 \cap \mathbb{A}_K^1$. We claim that C is the set we are looking for.

First we check that $CK^\times = \mathbb{A}_K^1$. So let $x \in \mathbb{A}_K^1$. Then $\mu(x^{-1}C_0) = |x|^{-1}\,\mu(C_0) = \mu(C_0) > \mu'(\mathbb{A}_K/K)$. Let Y be the image of $x^{-1}C_0$ in $\mathbb{A}_K/K$. Recall that by Remark 6.9, the measure μ' satisfies $\mu'(\pi(C')) = \mu(C')$ for the natural projection π, and a compact $C' \subset \mathbb{A}_K$ for which $\pi|_{C'}$ is injective. Therefore, since $\mu'(Y) \leq \mu'(\mathbb{A}_K/K) < \mu(x^{-1}C_0)$, the quotient map $x^{-1}C_0 \to Y$ cannot be injective. As a consequence, there exist $y, z \in C_0$ for which $x^{-1}y$ and $x^{-1}z$ have the same image mod K, i.e. such that $u := x^{-1}y - x^{-1}z \in K^\times$. Then $xu = y - z \in C_1$, and since $x \in \mathbb{A}_K^1$, so is xu. This implies $xu \in C$, so we can write $x = (xu)u^{-1} \in CK^\times$.

It remains to prove compactness of C. First note that C_0 is compact, and C_1 is compact, because it is the image of the continuous map

$$\begin{aligned} C_0 \times C_0 &\to \mathbb{A}_K \\ (y, z) &\mapsto y - z. \end{aligned}$$

By Lemma 7.40 (2), the subspace $\mathbb{A}_K^1 \subset \mathbb{A}_K$ is closed. Moreover, C_1 is compact, hence closed (as $\mathbb{A}_K$ is Hausdorff). Therefore $C = C_1 \cap \mathbb{A}_K^1 \subset C_1$ is a closed subspace of a compact space, thus it is compact. □

8. First steps in class field theory

8.1. **Introduction.** This section closely follows notes by Oron Propp for a lecture by Sam Raskin, see [Ras16]. Class field theory studies abelian extensions of number fields. Let us give some motivation.

Question 8.1. When can an algebraic number in $\overline{\mathbb{Q}}$ be expressed using any combination of taking n-th roots, $+, -, \cdot, /$ on rational numbers? More precisely, given a separable polynomial $f \in K[X]$, K a number field, when can the equation $f(x) = 0$ be solved by radicals?

The answer is given by Galois theory.

Theorem 8.2 (Galois' theorem)**.** *The polynomial f can be solved by radicals if and only if the Galois group of its splitting field is solvable.*

Recall that a finite group G is *solvable* if there exists a chain of subgroups

$$1 \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_k = G$$

such that $G_j \subset G_{j+1}$ is normal, and the quotient G_{j+1}/G_j is abelian. A Galois extension L/K is *solvable*, if $G = \mathrm{Gal}(L/K)$ is solvable, and it is *abelian* if its Galois group is. More precisely this means that L/K can be written as a successive extension of abelian Galois extensions. An example is

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_3, \sqrt[3]{2}).$$

Here, $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is the splitting field of $X^3 - 2$. As such, its Galois group G over $\mathbb{Q}$ is a subgroup of the symmetric group S_3, and since the degree of the extension is 6, we have $G = S_3$. This is non-abelian, but each individual extension above is abelian (even cyclic). The upshot is that to understand solvability by radicals, we are reduced to understanding abelian extensions. For general number fields, they are not completely understood, but for $K = \mathbb{Q}$ we have the following.

Theorem 8.3 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$ for some integer n, where ζ_n is a primitive n-th root of unity.*

Recall here that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ is Euler's totient function, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. This group acts on roots of unity by $m : \zeta_n \mapsto \zeta_n^m$ for $m \in (\mathbb{Z}/n\mathbb{Z})^\times$. In the original sense, class field theory is the search for a generalization of the Kronecker-Weber theorem to an arbitrary number field. In other words, one wants to describe all abelian extensions of a number field K in some way.

Abelian extensions are also interesting because they predict identities between algebraic numbers. For instance we have the following equalities

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \overline{\zeta}_8 = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}}.$$

These identities are perhaps not so surprising once you know the Kronecker-Weber theorem. Indeed, as $\mathbb{Q}(\sqrt{2})$ is abelian, it is contained in a cyclotomic extension (which in this case turns out to be $\mathbb{Q}(\zeta_8)$), so necessarily we have to be able to express $\sqrt{2}$ using algebraic operations on ζ_8.

One particular instance of abelian extensions are quadratic extensions, which we are going to study in more detail. They are related to questions about solvability of quadratic equations. A classic result is the Hasse-Minkowski theorem.

Theorem 8.4. *Let K be a number field, and let $q(x_1, ..., x_n) = \sum_{i>j} a_{ij}x_ix_j + \sum_{i=1}^n a_ix_i^2$ be a quadratic form with coefficients $a_{ij}, a_i \in K$. Then for any $y \in K$, the equation*

$$q(x_1, ..., x_n) = y$$

has a (non-trivial) solution in K if and only if it has a solution in every completion K_v.

We will introduce a map related to class field theory, which helps us to solve quadratic equations in non-archimedean K_v, by reducing the question to elementary congruence problems. Moreover, as an example, consider the case $K = \mathbb{Q}$. Here, we can reformulate instances of this solvability question to asking whether $z \in \mathbb{Q}$ is a norm in a quadratic extension. More explicitly, for the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d})$, and norm given by $N(x + y\sqrt{d}) = x^2 - dy^2$, it is clear that this is related to solving the quadratic equation $x_1^2 - dx_2^2 = z$.

8.2. **Main statements.** Note that for any field K with separable closure K^{sep} and two abelian Galois extensions $K_j \supset K$ with $K_j \subset K^{\text{sep}}$ for $j = 1, 2$, the compositum of $K_1 \cdot K_2$ is a again an abelian extension (because its Galois group over K is a subgroup of the direct product of Galois groups of K_1 and K_2).

Definition 8.5. Let K be a field with separable closure K^{sep}. The *maximal abelian extension* K^{ab}/K is the compositum of all abelian extensions of K. The Galois group $Gal(K^{\text{ab}}/K)$ is the abelianization of $\text{Gal}(K^{\text{sep}}/K)$.

Recall that $G_K = \text{Gal}(K^{\text{sep}}/K)$ is a *profinite* group. This means it is endowed with a topology making it a topological group which is Hausdorff, compact and totally disconnected. An equivalent characterization is saying that a topological group G is profinite if and only if it is an inverse limit of discrete finite groups. In our situation, G_K (resp. G_K^{ab}) is an inverse limit of Galois groups of finite (abelian) Galois extensions of K, where the transition maps are the restriction maps. On the other hand, given any group G, there is a universal way to construct a profinite group out of it.

Definition 8.6. Let G be a group. Then the topological group

$$\widehat{G} := \lim G/H$$

with the limit running over finite index normal subgroups H of G is called the *profinite completion* of G.

Theorem 8.7 (Local class field theory)**.** *Let $K/\mathbb{Q}_p$ be a finite extension. Then there is a canonical isomorphism*

$$\theta_K : \widehat{K^\times} \xrightarrow{\sim} G_K^{\text{ab}}$$

of profinite groups called the local reciprocity map.

Moreover, this isomorphism satisfies a certain compatibility which we describe in the following. We have a short exact sequence

$$1 \to O_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where v is the normalized discrete valuation with respect to the maximal ideal $\mathfrak{p}_K \subset O_K$. We have seen that $O_K^\times \subset K^\times$ is open. Note that $O_K^\times = \lim_n O_K^\times/(1+\mathfrak{p}_K^n)$, so $O_K^\times$ is profinite. Applying profinite completion, we obtain an exact sequence

$$1 \to O_K^\times \to \widehat{K^\times} \xrightarrow{\widehat{v}} \widehat{\mathbb{Z}} \to 0.$$

Note that this is not automatic in general, as profinite completion is only right exact, but it is true in this situation that injectivity is preserved.

On the other hand, let L/K be a finite Galois extension. We denote by k_K and k_L the residue fields, which are finite fields, say $k_K = \mathbb{F}_q$ and $k_L = \mathbb{F}_{q^n}$. Recall that there is a surjective map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) \cong \mathbb{Z}/n\mathbb{Z}$, and this map is an isomorphism if and only if L/K is unramified. The group $\mathrm{Gal}(k_L/k_K)$ is generated by the Frobenius autom orphism $\mathrm{Frob} : x \mapsto x^q$. We can take an inverse limit over all finite extensions L/K to obtain a homomorphism

$$G_K \to \mathrm{Gal}(\overline{k}/k) = \widehat{\mathbb{Z}}.$$

Since the target $\widehat{\mathbb{Z}}$ is abelian, this map factors through a homomorphism $G_K^{\mathrm{ab}} \to \widehat{\mathbb{Z}}$. The local reciprocity map makes the diagram

$$\begin{array}{ccc} \widehat{K^\times} & \xrightarrow{\widehat{v}} & \widehat{\mathbb{Z}} \\ \downarrow{\scriptstyle \theta_K} & \nearrow & \\ G_K^{\mathrm{ab}} & & \end{array}$$

commute.

In the end we will be interested in abelian extension of number fields, meaning we need a global version of the reciprocity map. This is formulated using adeles. Recall that the ideles class group of a number field K is the quotient $C_K = \mathbb{A}_K^\times/K^\times$.

Theorem 8.8 (Global class field theory)**.** *For any number field K there is a canonical isomorphism*

$$\Theta_K : \widehat{C_K} \xrightarrow{\sim} G_K^{\mathrm{ab}}$$

of profinite groups, called the global reciprocity map.

The global reciprocity map is compatible with the local ones at the places $v \in V_K$ in the following sense. Let $\overline{K}$ be an algebraic closure of K. We have a commuting diagram of embeddings

$$\begin{array}{ccc} K & \longrightarrow & K_v \\ \downarrow & & \downarrow \\ \overline{K} & \longrightarrow & \overline{K_v}, \end{array}$$

and these maps induce injective homomorphisms $G_{K_v} \to G_K$ and $G_{K_v}^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$. The local and global reciprocity maps make the diagram

$$\begin{array}{ccc} K_v^\times & \longrightarrow & C_K \\ \downarrow{\scriptstyle \theta_{K_v}} & & \downarrow{\scriptstyle \Theta_K} \\ G_{K_v}^{\mathrm{ab}} & \longrightarrow & G_K^{\mathrm{ab}}, \end{array}$$

commute, where the upper horizontal arrow is the map sending $x \in K_v^\times$ to the class of the idele whose v-coordinate is x and whose v'-coordinate is 1 for all places $v' \neq v$.

The proof of local and even more of global class field theory is out of the scope of this lecture. We remark though that class field theory can be understood as the simplest instance of the Langlands correspondence. This correspondence relates *automorphic representations* for $\mathrm{GL}_n(\mathbb{A}_K)$ and *Galois representations* of G_K of rank n. For GL_1, an automorphic representation is a continuous character

$$\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times.$$

On the other hand, a Galois representation of G_K of rank 1 is a continuous character

$$\rho : G_K^{\mathrm{ab}} \to \mathbb{C}^\times.$$

Note that because $\mathbb{C}^\times$ is abelian, ρ factors through G_K^{ab}. The global reciprocity map induces an isomorphism only after profinite completion, and the character χ only extends to $\widehat{C_K}$ if it has finite image. Indeed, if $\chi : C_K \to \mathbb{C}^\times$ has finite image, then its kernel N' is a closed and normal subgroup of finite index. Moreover, χ factors through C_K/N'. Thus, the natural map $\widehat{C_K} = \lim C_K/N \to C_K/N'$ induces a character $\chi : \widehat{C_K} \to \mathbb{C}^\times$ by composition. Vice versa, we have the following result.

Proposition 8.9. *Let G be a profinite group and $\chi : G^{\mathrm{ab}} \to \mathbb{C}^\times$ a continuous character. Then the image of χ is finite.*

Proof. There is an open neighborhood $U \subset \mathbb{C}^\times$ of 1 not containing any non-trivial subgroup of $\mathbb{C}^\times$. To see this, let W be a bounded convex neighborhood of $0 \in \mathbb{C}$ such that $\exp : W \to \exp(W)$ is a diffeomorphism. Let $W_1 = \frac{1}{2}W$, and assume $H \subset \exp(W_1)$ is a subgroup. Let $y \in H$ and write $y = \exp(x)$, where we assume $x \neq 0$. Since W is bounded, there exists a maximal $k \in \mathbb{Z}_{\geq 0}$ with $kx \in W_1$. Then $y^{k+1} = \exp((k+1)x) \in H \subset \exp(W_1)$. This implies there is $x' \in W_1$ with $\exp(x') = \exp((k+1)x)$ by convexity. Note that $\frac{k+1}{2} \leq k$, so $(k+1)x \in 2W_1 = W$. Since exp is injective on W, we conclude that $x' = (k+1)x \in W_1$, which contradicts the maximality of k. This implies that $x = 0$, so $y = 1$ and H has to be trivial.

Back to χ, the preimage of $\chi^{-1}(U)$ is an open neighborhood of the neutral element $e \in G^{\mathrm{ab}}$, so there is an open subgroup $e \in V \subset \chi^{-1}(U)$. The image $\chi(V)$ is a subgroup of $\mathbb{C}^\times$ contained in U, so it is trivial. This implies $V \subset \ker(\chi)$, so χ descends to a map $\chi : G^{\mathrm{ab}}/U \to \mathbb{C}^\times$. Since U is open, the quotient G^{ab}/U is finite. □

In this way, the global reciprocity map induces a correspondence between characters $\rho : G_K^{\mathrm{ab}} \to \mathbb{C}^\times$ and characters $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$ with finite image.

8.3. **Quadratic extensions and the Hilbert symbol.** From now on, we will focus on quadratic extensions, and explain how in this case the reciprocity map can be constructed explicitly using the so-called *Hilbert symbol*. Until the end of this chapter, if it is not explicitly said otherwise, by a local field we mean a local field of characteristic not equal to 2. Note that this includes in particular every completion of a number field.

First off, let K be a field with $\mathrm{char}(K) \neq 2$, and let G_K be the absolute Galois group of K. Let $G_{K,2} = G_K/\langle \sigma^2 \mid \sigma \in G_K \rangle$, i.e. it is the maximal quotient of G_K in which $\sigma^2 = 1$ for all $\sigma \in G_K$. It is necessarily abelian, because $xy = (xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in G_K$. Therefore it is a $\mathbb{Z}/2$-module, i.e. an $\mathbb{F}_2$-vector space. Moreover, denote by $(K^\times)^2$ the subgroup of squares of $K^\times$. Then $K^\times/(K^\times)^2$ is an abelian 2-torsion group, so also an $\mathbb{F}_2$-vector space. Denote its dual space by $(K^\times/(K^\times)^2)^\vee = \mathrm{Hom}(K^\times/(K^\times)^2), \mathbb{F}_2)$

Proposition 8.10. *There is a canonical isomorphism*

$$G_{K,2} \xrightarrow{\sim} (K^\times/(K^\times)^2)^\vee$$

of $\mathbb{F}_2$-vector spaces.

Proof. Given $\sigma \in G_{K,2}$ we define $\chi_\sigma : K^\times/(K^\times)^2 \to \mathbb{F}_2$ by

$$\chi_\sigma(d) = \begin{cases} 0, \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ 1, \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases}$$

Let us check that this defines a group homomorphism. We need to see that for $\sigma_1, \sigma_2 \in G_{2,K}$ we have $\chi_{\sigma_1\sigma_2} = \chi_{\sigma_1} + \chi_{\sigma_2}$. This is clear since $(\sigma_1\sigma_2)(\sqrt{d}\ ) = (-1)^{\chi_{\sigma_1}}(-1)^{\chi_{\sigma_2}}\sqrt{d} = (-1)^{\chi_{\sigma_1}+\chi_{\sigma_2}}\sqrt{d}$.

Since both groups are profinite 2-torsion groups, it suffices to prove that both groups are isomorphic after taking continuous duals. We have

$$\mathrm{Hom}_{\mathrm{cts}}((K^\times/(K^\times)^2)^\vee, \mathbb{F}_2) = K^\times/(K^\times)^2.$$

Moreover, a continuous map $G_{K,2} \to \mathbb{F}_2$ is the same as a quadratic extension of K. Indeed, given a quadratic extension $K^{\mathrm{sep}} \supset L \supset K$, we obtain a normal subgroup $\mathrm{Gal}(K^{\mathrm{sep}}/L) \subset G_K$ with image $G_{L,2}$ in $G_{K,2}$, and satisfying $G_K/G_L = G_{K,2}/G_{L,2} = \mathrm{Gal}(L/K) = \mathbb{F}_2$. The map $G_{K,2} \to \mathbb{F}_2$ is the projection. Vice versa, by Galois theory the kernel of a map $G_{K,2} \to \mathbb{F}_2$ comes as a quotient from the Galois group of a quadratic extension. A quadratic extension is necessarily of the form $K(\sqrt{d})$, and $d \in K^\times$ is unique up to multiplying by a square. □

Example 8.11. For $K = \mathbb{Q}$, the above proposition tells us that

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_p \mathbb{Z}/2\mathbb{Z}$$

On the other hand, global class field theory predicts that we can compare this to

$$(\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{A}_{\mathbb{Q}}^\times)^2)^\wedge.$$

The local reciprocity map induces an isomorphism $K^\times/(K^\times)^2 \xrightarrow{\sim} G_{K,2}$ and hence it predicts the existence of a non-degenerate pairing

$$(\cdot,\cdot) : K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \mathbb{F}_2 = \{\pm 1\}.$$

We will construct it in the following.

Definition 8.12. The pairing

$$(\cdot,\cdot) : K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{\pm 1\}$$
$$(a,b) = \begin{cases} 1, & \text{if there exist } x,y \in K \text{ with } ax^2+by^2=1 \\ -1, & \text{else} \end{cases}$$

is called the *Hilbert symbol*.

Remark 8.13. The Hilbert symbol is well-defined. If $a = a'd^2$, then $ax^2+by^2 = 1$ if and only if $a'(dx)^2+by^2 = 1$, and similarly for b. Moreover it is clearly symmetric.

Proposition 8.14. *The Hilbert symbol is*

(1) bimultiplicative, i.e. for all $a,b,c \in K^\times$ we have

$$(a,bc) = (a,b)(a,c), \text{ and}$$

(2) non-degenerate, i.e. for all $a \in K^\times$, if $(a,b) = 1$ for all $b \in K^\times$, then a is a square.

Here, note that bimultiplicativity says the following. The equation $ax^2+bcy^2 = 1$ has a solution if and only if $ax^2+by^2 = 1$ and $ax^2+cy^2 = 1$ both have a solution or if both cannot be solved. It is not clear at all that this is true, and in fact in general this holds only for local fields.

Example 8.15. Let's check that the proposition holds for $K = \mathbb{R}$. In this case the equation $ax^2+by^2 = 1$ is not solvable only if $a < 0$ and $b < 0$. Indeed, if say $a > 0$, then $x = 1/\sqrt{a}$ and $y = 0$ is a solution. From this description it is easy to see that bimultiplicativity holds. Moreover, the squares in $\mathbb{R}^\times$ are precisely the positive real numbers $\mathbb{R}_{>0}$, so that $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \mathbb{R}^\times/\mathbb{R}_{>0} = \{\pm 1\}$. Therefore, if $(a,b) = 1$ for all b, we can pick $b < 0$, implying that $a > 0$, hence a is a square. If you identify $\mathbb{F}_2 = \{\pm 1\}$ the pairing becomes the natural multiplication pairing

$$\mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$$
$$(x,y) \mapsto xy.$$

To better understand the Hilbert symbol we need to understand squares in $K^\times$. We have seen $K = \mathbb{R}$ above, and when $K = \mathbb{C}$, every element has a square root.

Lemma 8.16. *Let K be non-archimedean, with ring of integers O_K, maximal ideal $\mathfrak{p} \subset O_K$ and residue field $k = O_K/\mathfrak{p}$. Assume that $\mathrm{char}(k)$ is odd. Let $x \in K^\times$ and write $x = \pi^{v(x)}y$ where π is a uniformizer and $y \in O_K^\times$. Then the following are equivalent:*

(1) x is a square,
(2) $v(x)$ is even and y is a square,
(3) $v(x)$ is even y is a square mod $\mathfrak{p}$.

Proof. The only thing which is not immediately clear is that (3) implies (1). We can reduce to $x \in O_K^\times$. Assume $x \mod \mathfrak{p}$ is a square, i.e. $\overline{x} = \overline{u}^2$, where $\overline{x}$ denotes the image in $k = O_K/\mathfrak{p}$. This is equivalent to saying that $f = T^2 - x \in O_K[T]$ has a root $\overline{u} \mod \mathfrak{p}$. We can apply Hensel's lemma provided we can show that this root occurs with multiplicity 1. For that we need to show that $\overline{f}'(\overline{u}) \neq 0$, but this is clear since $f' = 2T$ and $\overline{u}$ is non-zero (as $x \in O_K^\times$ we have $\overline{x} \neq 0$). □

Corollary 8.17. *In the above situation, we have $K^\times/(K^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. We have $K^\times = O_K^\times \times \mathbb{Z}$. By the Lemma, $(K^\times)^2 = (O_K^\times)^2 \times 2\mathbb{Z}$. Moreover, the reduction map $O_K^\times \to k^\times$ induces an isomorphism $O_K^\times/(O_K^\times)^2 \to k^\times/(k^\times)^2$. Indeed, the map $O_K^\times \to k^\times/(k^\times)^2$ is clearly surjective, so it suffices to show that its kernel is $(O_K^\times)^2$. This is precisely (3) in the Lemma. For a finite field, it is easy to see that $(k^\times)^2$ has index 2 in $k^\times$. Either use the fact that $k^\times$ is cyclic, or check that the kernel of the squaring map is $\{\pm 1\}$. □

8.4. **Relation to norms.** Assume $a \in K^\times$ is not a square, so that $K(\sqrt{a}) \supset K$ is an extension of degree 2.

Lemma 8.18. *For $b \in K^\times$ we have $(a, b) = 1$ if and only if b is a norm for the extension $K(\sqrt{a}) \supset K$.*

Proof. Assume b is a norm, so there exists $\alpha, \beta \in K$ with

$$b = N(\alpha + \beta\sqrt{a}) = \alpha^2 - \beta^2 a.$$

Note that this implies $\alpha^2 = a\beta^2 + b$. If $\alpha \neq 0$, we see that

$$1 = a\,\frac{\beta^2}{\alpha^2} + b\frac{1}{\alpha^2},$$

so we have found a solution. If $\alpha = 0$, then $b + \beta^2 a = 0$. You can check that $x = \frac{1}{2}(1 + \frac{1}{a})$ and $y = \frac{1}{2\beta}(1 - \frac{1}{a})$ is a solution in this case. The other implication follows from reversing the above argument. □

Our next goal will be to prove the following main result on the Hilbert symbol.

Theorem 8.19. *Let K be a local field, and $L \supset K$ a quadratic extension. Then, the norm $N : L^\times \to K^\times$ is a homomorphism, and $N(K^\times) \subset L^\times$ is a subgroup of index 2.*

Assuming this theorem, we get the desired properties for the Hilbert symbol.

Lemma 8.20. *The Hilbert symbol for K is bimultiplicative and non-degenerate if and only if for all quadratic extensions L of K the image $N(K^\times) \subset L^\times$ is a subgroup of index 2.*

Proof. Assume that $N(K^\times) \subset L^\times$ is a subgroup of index 2 for all quadratic extension L. Let $a \in K^\times$. By symmetric, bimultiplicativity of the Hilbert symbol is equivalent to $(a, -) : K^\times \to \{\pm 1\}$ being a homomorphism. So this is what we have to show.

If a is a square, then $ax^2 + by^2 = 1$ is solvable for any b (e.g. by $(\frac{1}{\sqrt{a}}, 0)$), so the map $b \mapsto (a, b)$ is the trivial homomorphism.

If a is not a square, we let $L = K(\sqrt{a})$. By Lemma 8.18 we know that $(a, b) = 1$ if and only if $b \in N(L^\times)$. This implies that we have a factorization (as maps)

$$\begin{array}{ccc} K^\times & \xrightarrow{(a,-)} & \{\pm 1\}. \\ \downarrow & \nearrow & \\ K^\times/N(L^\times) & & \end{array}$$

Indeed, if $b, c \in K^\times$ mapping to the same class in $K^\times/N(L^\times)$, then $b = cd$ for some $d \in N(L^\times)$. Note that $(a, b) = 1$ if and only if b is a norm, and this is now true if and only if c is a norm, which in turn holds if and only if $(a, c) = 1$.

The projection $K^\times \to K^\times/N(L^\times)$ is trivially a homomorphism, and since $N(L^\times)$ is an order 2 subgroup, the map $K^\times/N(L^\times) \to \{\pm 1\}$ is necessarily an isomorphism of groups (since 1 is mapped to 1).

We now show non-degeneracy by proving the contrapositive. Let $a \notin (K^\times)^2$, and let $L = K(\sqrt{a})$. Then since $N(L^\times) \subset K^\times$ is a proper subgroup, there exists a $b \in K^\times$ which is not a norm for L. This is true if and only if $(a, b) = -1$, proving non-degeneracy.

For the converse, note that for a non-square $a \in K^\times$, the map $(a, -) : K^\times \to \{\pm 1\}$ is surjective by non-degeneracy, and a homomorphism by bimultiplicativity. Therefore we have an isomorphism $K^\times/N(K(\sqrt{a})^\times) \cong \{\pm 1\}$, because $N(K(\sqrt{a})^\times)$ is the kernel of $(a, -)$. This implies that is has index 2. □

Example 8.21. When $K = \mathbb{R}$, there is a unique quadratic extension $L = \mathbb{C}$. The norm is $N(x + iy) = x^2 + y^2$, so we have $N(\mathbb{C}^\times) = \mathbb{R}_{>0} = (\mathbb{R}^\times)^2$.

Assuming Theorem 8.19, we obtain the following.

Corollary 8.22. *The Hilbert symbol is bimultiplicative and non-degenerate.*

We omit the proof of Theorem 8.19. Instead, we give some ideas on the global situation.

Exercise 8.23.
(1) Give an explicit description of the Hilbert symbol for $\mathbb{Q}$ using the Hasse-Minkowski theorem.
(2) Use the first part to find $a_1, a_2 \in \mathbb{Q}^\times$ such that $(a_1 a_2, b) \neq (a_1, b)(a_2, b)$.

8.5. **Global class field theory and quadratic reciprocity.** Recall that for a number field K, global class field theory predicts an isomorphism

$$\Theta_K : \widehat{C_K} \xrightarrow{\sim} G_K^{\mathrm{ab}},$$

where $C_K = \mathbb{A}_K^\times / K^\times$. We will focus on the case $K = \mathbb{Q}$. Recall that we have the following identification

$$G_{\mathbb{Q}}^{\mathrm{ab}} / \langle \sigma^2 \rangle \cong \mathrm{Hom}(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \{\pm 1\}) \cong \mathrm{Hom}(\mathbb{Q}^\times, \{\pm 1\})$$

Combining these facts, we expect that $\mathrm{Hom}(\mathbb{Q}^\times, \{\pm 1\}) \cong \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / (\mathbb{A}_{\mathbb{Q}}^\times)^2$. This predicts a pairing which factors as follows:

$$\begin{array}{ccc} \mathbb{A}_{\mathbb{Q}}^\times \times \mathbb{Q}^\times & \longrightarrow & \{\pm 1\} \\ \downarrow & \nearrow & \\ \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / (\mathbb{A}_{\mathbb{Q}}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & & \end{array}$$

The pairing should be non-degenerate in the sense that it induces the isomorphism

$$\mathrm{Hom}(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \{\pm 1\}) \cong \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / (\mathbb{A}_{\mathbb{Q}}^\times)^2$$

above.

Definition 8.24. Let $V = V_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$. We define the following pairing

$$\begin{aligned} \mathbb{A}_{\mathbb{Q}}^\times \times \mathbb{Q}^\times &\to \{\pm 1\} \\ ((x_p), z) &\mapsto \prod_{p \in V} (x_p, z)_p, \end{aligned}$$

where we consider $y \in \mathbb{Q}^\times \subset \mathbb{A}_\mathbb{Q}^\times$, and $(-,-)_p$ denotes the Hilbert pairing on $\mathbb{Q}_p$ and on $\mathbb{R}$ (if $p = \infty$).

Proposition 8.25. *We have $(x_p, z) = 1$ for all but finitely many $p \in V$, so the above product is well-defined.*

Proof. The set of finite places for which $x_p \notin \mathbb{Z}_p^\times$ is finite, and so is the set of finite places for which $z \notin \mathbb{Z}_p$. Thus it suffices to show that when $p \neq 2$, and $x_p \in \mathbb{Z}_p$ and $z \in \mathbb{Z}_p$, then $(x_p, z) = 1$. This will follow from the lemma below. □

Lemma 8.26. *Let p be an odd prime, and let $a, b, c \in \mathbb{Z}_p^\times$. Then there exist $x, y \in \mathbb{Z}_p$ such that*

$$ax^2 + by^2 = c.$$

Proof. First off, we show that we can solve $ax^2 + by^2 = c \bmod p$. Including 0, there are $(p+1)/2$ squares in $\mathbb{Z}/p\mathbb{Z}$. This means ax^2 takes $(p+1)/2$ values mod p, and so does $c - by^2$. Since $(p+1)/2 + (p+1)/2 = p + 1 > p$, there has to be a common value. This implies there are $x, y \in \mathbb{Z}/p\mathbb{Z}$ with $ax^2 + by^2 = c \bmod p$ and not both 0 (because $c \neq 0$).

Without loss of generality assume $x \neq 0 \bmod p$. Then $(c - by^2)/a = x^2 \bmod p$, and using Hensel's lemma we can lift this root of $(c - by^2)/a \bmod p$ to a root in $\mathbb{Z}_p$. □

Note that $((x_p), z) \mapsto \prod_{p \in V} (x_p, z)_p$ is clearly bimultiplicative, and factors through $(\mathbb{A}_\mathbb{Q}^\times)^2$. However, we need to show that it factors through the diagonally embedded $\mathbb{Q}^\times$. This amounts to proving the following Proposition, which we will see to be essentially equivalent to the quadratic reciprocity law.

Proposition 8.27. *For all $x, y \in \mathbb{Q}$ we have $\prod_p (x, y)_p = 1$.*

Proof. Since the pairing is invariant under multiplication by squares, we can assume $x = \pm p_1 \cdots p_r$ and $y = \pm q_1 \cdots q_s$ for prime numbers p_i and q_j. Moreover, by bimultiplicativity, we may assume $x \in \{-1, 2, p\}$ and $y \in \{-1, 2, q\}$ for two distinct odd primes p and q.

Let's consider the case (p, q). We need to show that

$$(p, q)_\infty \cdot \prod_\ell (p, q)_\ell = 1.$$

Here $(p, q)_\infty = 1$ because $p, q > 0$ (actually $p > 0$ or $q > 0$ would suffice). Moreover, for any odd prime $\ell' \neq p, q$ we have that p and q are ℓ'-adic units, so the Hilbert symbol is trivial there. It remains to show that

$$(p, q)_2 (p, q)_p (p, q)_q = 1.$$

Recall that for n prime to p, the Legendre symbol is

$$\left(\frac{n}{p}\right) = \begin{cases} 1, & n \text{ is a square mod } p \\ -1, & \text{else.} \end{cases}$$

Exercise 8.28. Let p be an odd prime, and $a, b \in \mathbb{Q}_p$. Write $a = p^\alpha u$, $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^\times$. Let $\varepsilon : \mathbb{Z}_2^\times \to \mathbb{Z}/2\mathbb{Z}$ be defined by $\varepsilon(z) = (z-1)/2 \bmod 2$. Show that

$$(a, b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

From the exercise, it follows that $(p,q)_p = (\frac{q}{p})$ and $(p,q)_q = (\frac{p}{q})$. Moreover, for $p = 2$ we freely use the fact that $(p,q)_2 = (-1)^{\varepsilon(p)\varepsilon(q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. For a proof (which is similar to $p \neq 2$, but more tedious), we refer to [Ser78, Chapter III]. This is equal to 1 unless $p \equiv q \equiv 3 \bmod 4$. Now the product formula $(p,q)_2(p,q)_p(p,q)_q = 1$ is equivalent to

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

which is precisely the quadratic reciprocity law.

From the remaining cases, we only check that $\prod_p (2,\ell)_p = 1$ and omit the rest (which can be tedious). We also omit some detail, for which we refer to [Ser78, Chapter III, Theorem 3]. As before we have $(2,\ell)_p = 1$ for $p \neq 2, \ell$, and

$$(2,\ell)_\ell = \left(\frac{2}{\ell}\right)$$

We again freely use a fact about the $p = 2$ case, namely $(2,\ell)_2 = (-1)^{\theta(\ell)}$ where

$$(-1)^{\theta(\ell)} = \begin{cases} 1, & \ell \equiv 1, -1 \mod 8 \\ -1, & \ell \equiv 3, -3 \mod 8. \end{cases}$$

Thus we need to show that

$$\left(\frac{2}{\ell}\right) = (-1)^{\theta(\ell)},$$

i.e. we need to understand when 2 is a square mod ℓ. Recall that $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, where $\zeta_8 = \exp(\pi i/4)$ is a primitive 8-th root of unity. Here is a short proof of this fact. We have

$$(\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = \zeta_4 + 2 + \zeta_4^{-1}.$$

Since $\zeta_4 = i$, the latter is equal to 2, implying the desired identity. Therefore, $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$, and the restriction map $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ gives a character

$$\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\},$$

by identifying $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \{\pm 1\}$. Here, an element $n \in (\mathbb{Z}/8\mathbb{Z})^\times$ acts via $\zeta_8 \mapsto \zeta_8^n$. The claim now is that

$$\left(\frac{2}{n}\right) = \chi(n) = (-1)^{\theta(n)}$$

for $n \in (\mathbb{Z}/8\mathbb{Z})^\times$. By definition, we have $\ker((-1)^{\theta(-)}) = \{\pm 1\}$, and an element $n \in (\mathbb{Z}/8\mathbb{Z})^\times$ is in $\ker(\chi)$ if and only if it fixes $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. This in turn is equivalent to

$$\zeta_8^n + \zeta_8^{-n} = \zeta_8 + \zeta_8^{-1}.$$

This happens if and only if $n = 1, -1$ (either both summands are fixed, or they are switched). This implies that the kernel of all maps agree, which implies that they are the same (the target has just two elements). □

The only thing that remains to check is non-degeneracy. This is the content of the next result.

Proposition 8.29. *The map*

$$\chi : \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 \to \mathrm{Hom}(\mathbb{Q}^\times, \{\pm 1\}) \cong G_{\mathbb{Q},2}$$

induced by the pairing

$$\begin{aligned} \mathbb{A}_\mathbb{Q}^\times \times \mathbb{Q}^\times &\to \{\pm 1\} \\ ((x_p), z) &\mapsto \prod_{p \in V} (x_p, z)_p \end{aligned}$$

is an isomorphism. Note that $\mathrm{Hom}(\mathbb{Q}^\times, \{\pm 1\}) = \mathrm{Hom}(\mathbb{Q}^\times / (\mathbb{Q}^\times)^2, \{\pm 1\})$.

Proof. First, note that $\mathbb{Q}_p^\times = \langle p \rangle \times \mathbb{Z}_p^\times$ via p-adic valuation. Identifying $\mathbb{Z} \cong \langle p \rangle$ we have

$$\mathbb{A}_\mathbb{Q}^\times \cong \mathbb{R}^\times \times \prod_p{}' \mathbb{Q}_p^\times \cong \{\pm 1\} \times \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times \times \bigoplus_p \mathbb{Z}$$

Now, the diagonally embedded $\mathbb{Q}^\times$ can be canonically identified with $\{\pm 1\} \times \bigoplus_p \mathbb{Z}$ via the composition

$$\mathbb{Q}^\times \hookrightarrow \mathbb{A}_\mathbb{Q}^\times \to \{\pm 1\} \times \bigoplus_p \mathbb{Z},$$

where the latter map is the projection. This implies that we obtain an identification

$$\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 \cong \prod_p \mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2.$$

We have seen that for odd primes p, the quotient $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2$ has order two, and is generated by any quadratic non-residue. One can show moreover (cf. [Ser78, Chapter II]) that

$$\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times,$$

which is of order 4 and generated by the classes of -1 and 5 (this implies that $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as abelian groups). Therefore we have

$$\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \prod_{p \neq 2} \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, recall that

$$\mathbb{Q}^\times / (\mathbb{Q}^\times)^2 = \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z},$$

where the first copy of $\mathbb{Z}/2\mathbb{Z}$ corresponds to the sign. The goal now is to show that after dualizing, the copies of $\mathbb{Z}/2\mathbb{Z}$ occurring in the source and target of χ match up (dualizing turns direct sums into products). For that, consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \prod_{p \neq 2} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker(\mathrm{ev}_{-1}) & \longrightarrow & \mathrm{Hom}(\mathbb{Q}^\times, \{\pm 1\}) & \xrightarrow{\mathrm{ev}_{-1}} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

The first copy of $\mathbb{Z}/2\mathbb{Z}$ comes from $p = 2$ and is generated by the adele $(5, 1, ..., 1)$. The rightmost copy of $\mathbb{Z}/2\mathbb{Z}$ is generated by $(-1, 1, ..., 1)$. The other copies corresponding to odd primes are generated by any quadratic non-residue r mod p. The rows are exact, and the left two vertical arrows are given by χ, whereas the rightmost vertical arrow is the induced map on the quotient. The map ev_{-1} is defined

by $\mathrm{ev}_{-1}(\varphi) = \varphi(-1)$. We want to show that χ is an isomorphism. By exactness it suffices to prove that the two outer vertical arrows are isomorphisms.

Let p be an odd prime. One checks by computation that for a quadratic non-residue r mod p, we have

$$(\chi(r)(\pm q))_p = \begin{cases} 1, & q \neq p \\ -1, & q = p, \end{cases}$$

where $(-)_p$ denotes restriction to the p-factor in $\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2$. Moreover $\chi(r)(-1) = 1$. A similar computation at $p = 2$ shows that

$$\chi(5, 1, ..., 1)(q) = 1, \chi(5, 1, ..., 1)(-1) = 1, \text{ and } \chi(5, 1, ..., 1)(2) = -1.$$

This shows that the left vertical arrow is well-defined and injective. On the other hand, a map $\varphi : \mathbb{Q}^\times \to \{\pm 1\}$ is determined by its restriction to each summand in $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2 = \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z}$, and by the above calculation we can choose an element in $\mathbb{Z}/2\mathbb{Z} \times \prod_{p \neq 2} \mathbb{Z}/2\mathbb{Z}$ accordingly. This shows surjectivity. Moreover, since $\chi(-1, 1, 1, ...) = -1$, the rightmost map is non-trivial, hence an isomorphism. This proves the claim.

□

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.1 Spectrum of a ring
§A.2 Radical of ideals
§A.3 Cayley–Hamilton
§A.4 Nakayama's lemma
§A.5 Tensor products
§A.6 Base change

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 $T = (t_{ij}) \in \mathrm{Mat}_{s\times r}(A)$.

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 $\mathrm{Mat}_{s\times r}(A)$ 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 $T \in \mathrm{Mat}_{r\times r}(A)$ 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

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

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

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

where $I_r \in \mathrm{Mat}_{r\times r}(A)$ denotes the identity matrix. Namely, take $S = (s_{ij})$ with $s_{ij} = \det(T_{ji})$ where $T_{ji} \in \mathrm{Mat}_{(r-1)\times(r-1)}(A)$ 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

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

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

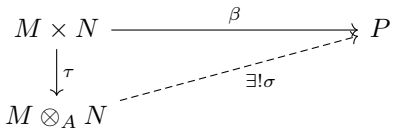
Exercise A.25. Let A be a ring and M a finitely generated A-module. Let I be an ideal in A with $I \subset \operatorname{Jac}(A)$. If $M = IM$, then $M = 0$.

Corollary A.26. *For every finitely generated A-module and prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$, 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

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

where $m \otimes n$ are formal symbols, $\operatorname{Free}_A\{-\}$ is the free A-module generated on these symbols and $\operatorname{Span}_A\{-\}$ 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

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

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 $\mathrm{supp}(\mathbb{Z}/m\mathbb{Z})\cap \mathrm{supp}(\mathbb{Z}/n\mathbb{Z}) = \varnothing$, 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 $\mathrm{rank}_A(M) := \#I$ 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

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

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. □

Appendix B. Solutions to some exercises

Exercise 1.4. The inverse is given by $\infty \mapsto (-1, 0)$ and $\mathbb{Q} \ni t \mapsto (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$.

Exercise 1.6. If x^2+y^2 odd, then either x^2 or y^2 is odd and the other one is even. So, without loss of generality x^2 is even and y^2 is odd, which implies $x = 2x'$ and $y = 2y' + 1$ for some $x', y' \in \mathbb{Z}$. We get $x^2 + y^2 = 4x'^2 + 4y'^2 + 4y' + 1 \equiv 1 \mod 4$.

Exercise 1.8. An element $x \in \mathbb{Z}[i]$ is invertible if and only if $|x| = 1$. This leads to the four cases $x = \pm 1, \pm i$. Now, let $a \in \mathbb{Z}[i]$ such that $|a|$ is prime. If $a = bc$ for some $b, c \in \mathbb{Z}[i]$, then either $|b| = 1$ or $|c| = 1$, i.e., either b or c is a unit and so a is prime.

Exercise 1.10. Follows from the fact that the group $\mathbb{F}_p^\times$ is cyclic of order $p - 1$, which is an even number by our assumption on p being odd.

Exercise 2.6. The ring $R_{(p)}$ is a domain as a subring of $\mathrm{Frac}(R)$. By construction, it is local with maximal ideal $pR_{(p)}$.

Exercise 2.14. (1): The map identifies with the localization $M \to M[(R\backslash\{0\})^{-1}]$. For $m \in M$, one has $\frac{m}{1} = 0$ if and only if there exists some $r \in R\backslash\{0\}$ with $rm = 0$.
(2): Omitted.
(3): The "if" directions follow from (2). The final direction is [Sta18, 0AUT].

Exercise 2.17. Replace R by $R_\mathfrak{p}$ for $\mathfrak{p} \subset R$ prime ideal. So, we can assume R to be local. We claim $I = Ry$ for some $y \in K := \mathrm{Frac}(R)$. Since $I^{-1}I = R$ there exist $x_i \in I^{-1}$, $y_i \in I$ with $\sum x_i y_i = 1$. Note $x_i y_i \in R$ for all i by definition of being invertible. At least one summand, say xy, does not belong to the maximal of R and hence $u := xy \in R^\times$. Replacing y by $u^{-1}y$ we obtain $xy = 1$ with $x \in I^{-1}$, $y \in I$. Then, $I = Ry$ since for $z \in I$ one has $z = (zx)y$ and $zx \in R$ as $x \in I^{-1}$.

Exercise 3.40. By Exercise 3.14 we have $B = \mathbb{Z}[\sqrt{d}]$, which is a free $\mathbb{Z}$-module with basis $1, \sqrt{d}$. The associated trace matrix is given by

$$\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Thus, $\Delta(1, \sqrt{d}) = 4d$ and $\Delta_{B/\mathbb{Z}} = (4d)$.

Exercise 3.41. Let $n \in \mathbb{N}$ be the $\mathbb{Z}$-rank of B. The base change matrix between two $\mathbb{Z}$-bases of B is some invertible matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. Hence, we have $\det(A) \in \mathbb{Z}^\times = \{\pm 1\}$. We conclude $\det(A)^2 = 1$ and the exercise follows from Remark 3.38(2).

Exercise 3.57.

Exercise 3.58. By Exercises 3.14 and 3.40 we have $B = \mathbb{Z}[\sqrt{d}]$ and $\Delta_{B/\mathbb{Z}} = (4d)$. Thus, p is unramified in $L = \mathbb{Q}[\sqrt{d}]$ if and only if $p \nmid 4d$. Since $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2$ is abelian, the element $\mathrm{Frob}_p \in \mathrm{Gal}(L/K)$ is defined for all odd primes p with $p \nmid d$. In this case, we have $\mathrm{Frob}_p = 1$ if and only if p is completely decomposed in L if and only if $T^2 - \bar{d} \in \mathbb{F}_p[T]$ has a zero if and only if $\bar{d} \in \mathbb{F}_p$ is a square if and only if $d^{\frac{p-1}{2}} \equiv 1 \mod p$.

Exercise 4.14. One has

$$\left(\frac{7600}{4049}\right) = \left(\frac{7600 - 4049}{4049}\right) = \left(\frac{3551}{4049}\right) = \left(\frac{53}{4049}\right)\left(\frac{67}{4049}\right).$$

As $4049 \equiv 1 \mod 4$ this is the same as

$$\left(\frac{4049}{53}\right)\left(\frac{4049}{67}\right) = \left(\frac{21}{53}\right)\left(\frac{29}{67}\right) = \left(\frac{3}{53}\right)\left(\frac{7}{53}\right)\left(\frac{29}{67}\right).$$

Using again quadratic reciprocity

$$\left(\frac{53}{3}\right)\left(\frac{53}{7}\right)\left(\frac{67}{29}\right) = \left(\frac{2}{3}\right)\left(\frac{4}{7}\right)\left(\frac{9}{29}\right) = -1,$$

since 4 and 9 are square modulo 7 and 29, but 2 modulo 3 is not.

Exercise A.2. (1): Preimages of ideals under ring maps are ideals and so is $\varphi^{-1}(\mathfrak{q})$. Let $a, b \in A$ with $ab \in \varphi^{-1}(\mathfrak{q})$. Then, $\varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{q}$ and so $\varphi(a) \in \mathfrak{q}$ or $\varphi(b) \in \mathfrak{q}$ (or both) using that $\mathfrak{q}$ is a prime ideal. This shows $a \in \varphi^{-1}(\mathfrak{q})$ or $b \in \varphi^{-1}(\mathfrak{q})$.

(2): Since φ is surjective, we have $\varphi(\varphi^{-1}(\mathfrak{q})) = \mathfrak{q}$ for all subsets $\mathfrak{q} \subset A/I$. This implies injectivity. The description of the image of $\mathrm{Spec}(\varphi)$ is left to the reader.

Exercise A.3. For a prime ideal $\mathfrak{q} \subset A_{\mathfrak{p}}$, we have $\mathfrak{q} = (\mathfrak{q} \cap A)A_{\mathfrak{p}}$ where $\mathfrak{q} \cap A$ denotes the preimage of $\mathfrak{q}$ under $A \to A_{\mathfrak{p}}$. This implies injectivity. The description of the image is left to the reader.

Exercise A.5. One has $f \in A^\times$ if and only if $A/fA = 0$ if and only if $\mathrm{Spec}(A/fA) = \varnothing$ if and only if $f \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ if and only if $f(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$.

Exercise A.7. One has $\mathrm{Spec}(k[T]) = \{(f) \mid f \in k[T]\backslash k \text{ irreducible, normed}\} \cup \{(0)\}$. The localizations at (f) and (0) are $k[T]_{(f)} = \{\frac{a}{b} \in k(T) \mid f \nmid b\}$ and $k(T)$ respectively. The residue fields are finite extensions of k and $k(T)$ respectively. If k is algebraically closed, all normed and irreducible polynomials of degree ≥ 1 are of the form $T - \lambda$ for $\lambda \in k$. All residue fields are isomorphic to k in this case.

Exercise A.11. (1): Let $e = \max\{e_i \mid i = 1, \ldots, r\}$ and $q := p_1 \cdot \ldots \cdot p_r$. Then, $q^e \in (a)$ and hence $q \in \sqrt{(a)}$, i.e., $(q) \subset \sqrt{(a)}$. On the other hand, $\sqrt{(a)} = (q')$ for some $q' \in A$ because A is a principal ideal domain. By definition, there exists $e' \geq 1$ such that $(q')^{e'} \in (a)$. Since all $e_i \geq 1$ we get $p_i \mid (q')^{e'}$ and so $p_i \mid q'$ using that all p_i are prime. This shows $q \mid q'$, and so $(q) \supset (q') = \sqrt{(a)}$ holds as well.

(2): Since A is noetherian, we have $\sqrt{I} = (f_1, \ldots, f_r)$ for some $f_i \in A$. Let $m_i \geq 1$ with $f_i^{m_i} \in I$ and put $m := r \cdot \max\{m_i\}$. Then, $(\sqrt{I})^m \subset I$.

Exercise A.19. For $I = (X)$ one has $M = u(M) = XM = IM$ where the first equality holds because u is surjective. By Corollary A.18, there exists some $f \in 1+I$ with $fM = 0$. Writing $f = 1+(-X \cdot g)$ for some $g \in A[X]$ we see that u is invertible with inverse $g(u)$.

The final question has a negative answer: for all $n \in \mathbb{Z}\backslash\{0, \pm 1\}$, the map $\mathbb{Z} \to \mathbb{Z}, m \mapsto n \cdot m$ is an injective $\mathbb{Z}$-module endomorphism but not surjective.

Exercise A.22. The image of a unit under any ring map is a unit. Conversely, assume that $\varphi(a) = a \mod I$ is a unit in A/I. Then, there exists $b \in A$ such that $ab \equiv 1 \mod I$, i.e., $ab \in 1 + I$. By Proposition A.21, the element ab is a unit in A and so must be a.

If A is local, then $\mathfrak{m} = \mathrm{Jac}(A)$ and $(A/\mathfrak{m})^\times = (A/\mathfrak{m})\backslash\{0\}$. Using the above with $I = \mathfrak{m}$, we get

$$A^\times = \varphi^{-1}\big((A/\mathfrak{m})\backslash\{0\}\big).$$

The latter set is equal to $A\backslash\mathfrak{m}$ by an elementary calculation.

Exercise A.23. Assume $\varphi(f)$ is a unit. Then, $\varphi(f) \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(B)$, so $f \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(B)$ Since $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective, this implies $f \notin$

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.)

Exercise A.25. Apply Lemma A.24 to the unique map $0 = N \to M$ from the zero module.

Exercise A.34. (1): One has $u \otimes v = (u \otimes \mathrm{id}_N) \circ (\mathrm{id}_{M'} \otimes v)$, which is a composition of surjective maps by Corollary A.32(2). The description of the kernel follows from the same corollary. The final statement is the special case where $u = \mathrm{id}_M$ is the identity on a module M and $v\colon A \to A/I, a \mapsto a \mod I$.

(2): Consider the exact sequence $0 \to I \to A \to A/I \to 0$ and apply $(-) \otimes_A A/J$. By Corollary A.32(1) and Lemma A.30(3), we get an exact sequence

$$I \otimes_A A/J \to A/J \xrightarrow{\pi} A/I \otimes_A A/J \to 0.$$

By (1), $\ker(\pi)$ is the submodule of A/J generated by the image of $I \subset A \to A/J$. Hence, $A/(I + J) = (A/J)/\ker(\pi) = A/I \otimes_A A/J$.

In the example, we compute $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\gcd(m, n)\mathbb{Z}$ since $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$ as ideals in $\mathbb{Z}$. Hence, this ring is zero if and only if $\gcd(m, n)\mathbb{Z} = \mathbb{Z}$ if and only if m, n are coprime.

Exercise A.36. (1): Choose isomorphisms $M = \oplus_{i \in I} A$ and $N = \oplus_{j \in J} A$. Then, one has $A^{(I)} \otimes_A A^{(J)} := (\oplus_{i \in I} A) \otimes_A (\oplus_{j \in J} A) = \oplus_{i \in I, j \in J}(A \otimes_A A) = A^{(I \times J)}$ by Corollary A.32(1) and Lemma A.30(3). In particular, if $r = \#I$ and $s = \#J$ are finite, then $A^r \otimes_A A^s = A^{rs}$.

(2): If M and N are direct summands of the free A-modules E and F respectively, then $M \otimes_A N$ is a direct summand of the A-module $E \otimes_A F$, which is free by the proof of (1).

(3): Choose surjections $A^r \to M$ and $A^s \to N$ for some $r, s \in \mathbb{N}$. Then, the induced map $A^r \otimes_A A^s \to M \otimes_A N$ is surjective by Exercise A.34(1) and $A^r \otimes_A A^s \cong A^{rs}$ is free by (1).

Exercise A.40. One has $\mathbb{Z}[T]/(T^2-d) \cong \mathbb{Z}[\sqrt{d}], T \mapsto \sqrt{d}$ as rings.

(1): Applying $\mathbb{Q} \otimes_{\mathbb{Z}} (-)$, we get $\mathbb{Q}[T]/(T^2-d) \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{d}]$, which is a field since $T^2 - d \in \mathbb{Q}[T]$ is irreducible (because it is quadratic and has no root in $\mathbb{Q}$).

(2): Applying $\mathbb{F}_p \otimes_{\mathbb{Z}} (-)$, we get $\mathbb{F}_p[T]/(T^2-\bar{d}) \cong \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{d}]$. This is a field if and only if $\bar{d}$ is not a square in $\mathbb{F}_p$.

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. 74, 79

[AW45] Emil Artin and George Whaples. Axiomatic characterization of fields by the product formula for valuations. *Bulletin of the American Mathematical Society*, 51(7):469 – 492, 1945. 51

[Bou95] N. Bourbaki. *General Topology*. Springer Berlin, Heidelberg, 1995. Chapters 1-4. 37, 45

[Bou98] N. Bourbaki. *Commutative Algebra*. Springer Berlin, Heidelberg, 1998. Chapters 1-7. 35

[Bou02] N. Bourbaki. *Topological Vector Spaces*. Springer Berlin, Heidelberg, 2002. Chapters 1-5. 45

[Bou04] N. Bourbaki. *Integration II*. Springer Berlin, Heidelberg, 2004. Chapters 7-9. 46, 47, 62

[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. 2

[CL84] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In Hendrik Jager, editor, *Number Theory Noordwijkerhout 1983*, pages 33–62, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg. 59

[Con] Keith Conrad. The splitting field of $x^3 - 2$ over $\mathbb{Q}$. 22

[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

[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. 2

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994. 2, 56

[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. 2

[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

[Ras16] Sam Raskin. Lectures on cohomological class field theory. https://gauss.math.yale.edu/~sr2532/cft/notes.pdf, 2016. Notes by Oron Propp. 63

[Ser78] J.-P. Serre. *A Course in Arithmetic*. Springer New York, NY, 1978. 72, 73

[Sta18] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018. 7, 8, 9, 11, 16, 18, 20, 23, 24, 29, 39, 41, 74, 77, 84

[Wei95] A. Weil. *Basic Number Theory*. Springer Berlin, Heidelberg, 1995. 48

[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]. 2