Algebraic Number Theory

RWTH Aachen, WS 2023

Jürgen Müller

Contents

I Introduction

1 Gaussian integers

(1.1) Primes as sums of two squares. Let $p \in \mathbb{Z}$ be an odd prime.

For $x \in \mathbb{Z}$, we have either $x \equiv 0 \pmod 2$ and hence $x^2 \equiv 0 \pmod 4$, or $x \equiv \pm 1 \pmod 4$ and hence $x^2 \equiv 1 \pmod 4$. Thus, if there are $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$, then precisely one of a or b is odd, and hence we have $p \equiv 1 \pmod 4$. In other words, if $p \equiv -1 \pmod 4$, then p cannot be written as a sum of two squares in $\mathbb{Z}$. (For $p = 2$ we have the representation $2 = 1^2 + 1^2$.)

The question arises what happens in the case $p \equiv 1 \pmod 4$: Looking at a few examples, see Table 1, we are led to conjecture that there always is a representation of p as a sum of two squares in $\mathbb{Z}$, and this representation is unique, up to signs and order. Moreover, if this holds actually true, we wonder whether a and b can possibly be computed algorithmically. To this end we place ourselves into a broader context:

(1.2) Gaussian numbers. Let $\mathbb{Q} \subseteq \mathbb{R}$ be the fields of **rational** and **real numbers**, respectively; let $K \in \{\mathbb{Q}, \mathbb{R}\}$. Then the polynomial $X^2 + 1 \in K[X]$ is irreducible. Hence the quotient K-algebra $L := K[X]/(X^2+1)$ of $K[X]$ with respect to the principal ideal $(X^2+1) \trianglelefteq K[X]$ is a field, being called the field of **Gaussian numbers** if $K = \mathbb{Q}$, and the field of **complex numbers** if $K = \mathbb{R}$; in the latter case we also write $L = \mathbb{C}$.

Letting $i := \overline{X}$ be the **imaginary unit**, where $\overline{\ }\colon K[X] \to L$ is the natural map, the set $\{1, i\} \subseteq L$ is a K-basis, thus any $z \in L$ can be written uniquely as $z = x + iy \in L$ for some $x, y \in K$. By construction we have $i^2 = -1$, thus we also write $i = \sqrt{-1}$ and $L = K(i) = K(\sqrt{-1})$; but note that i is merely a choice of one of the two square roots of -1 in L.

We have $X^2 + 1 = (X - i)(X + i) \in L[X]$. Thus, being the splitting field of a separable polynomial, the field extension $K \subseteq L$ is finite Galois such that $\mathrm{Aut}_K(L) = \{\mathrm{id}, \kappa\}$, where $\kappa\colon L \to L\colon z = x + iy \mapsto \overline{z} = x - iy$ is called **(complex) conjugation**.

Let $N = N_{L/K}\colon L \to K\colon z = x + iy \mapsto z\overline{z} = (x + iy)(x - iy) = x^2 + y^2$ be the associated **norm map**. It is multiplicative in the sense that $N(zz') = N(z)N(z')$ for $z, z' \in L$, and we have $z^{-1} = \frac{\overline{z}}{N(z)} \in L$ for $z \in L^* = L \setminus \{0\}$.

For $z \in \mathbb{C}$ we have $N(z) \geq 0$, where $N(z) = 0$ if and only if $z = 0$. Hence let $|z| := \sqrt{N(z)} \in \mathbb{R}$ be the complex **absolute value**. This defines a metric on $\mathbb{C}$, so that both $\mathbb{R}$ and $\mathbb{C}$ (but not $\mathbb{Q}$ and $\mathbb{Q}(i)$) become complete topological fields.

(1.3) Gaussian integers. We consider the subring $\mathbb{Z}[i] := \{a + bi \in \mathbb{C}; a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}$, being called the ring of **Gaussian integers**; being a subring of a field it is an integral domain. Moreover, conjugation restricts to a ring

automorphism of $\mathbb{Z}[i]$, and we have $N\colon \mathbb{Z}[i] \to \mathbb{Z}$. We collect a few immediate facts about the structure of $\mathbb{Z}[i]$:

Theorem. The group of units of $\mathbb{Z}[i]$ is given as $\mathbb{Z}[i]^* = \{\pm 1, \pm i\} = \langle i \rangle \cong C_4$.

Proof. Let $\mathcal{O} := \mathbb{Z}[i]$. We show that $\mathcal{O}^* = N^{-1}(\{1\}) \subseteq \mathcal{O}$: Since N is multiplicative such that $N(1) = 1$, we get the group homomorphism $N(\mathcal{O}^*) \subseteq \{\pm 1\} = \mathbb{Z}^*$. This implies $\mathcal{O}^* \subseteq N^{-1}(\{1\})$. Conversely, if $z \in \mathcal{O}$ such that $N(z) = z\overline{z} = 1$, then $z^{-1} = \overline{z} \in \mathcal{O} \subseteq \mathbb{Q}(i)$, hence $z \in \mathcal{O}^*$.

Finally, for $z = a + bi \in \mathcal{O}$ we have $N(z) = a^2 + b^2 = 1$ if and only if $a \in \{\pm 1\}$ and $b = 0$, or $a = 0$ and $b \in \{\pm 1\}$. ♯

Theorem. The ring $\mathbb{Z}[i]$ is Euclidean with respect to the degree map N.

Hence $\mathbb{Z}[i]$ is a principal ideal domain, and thus is factorial, where greatest common divisors (not only exist, but) can be computed by the Euclidean algorithm.

Proof. Recall that an integral domain R is called Euclidean, if there is a degree map $\delta\colon R \setminus \{0\} \to \mathbb{N}_0$ such that for all $a \in R$ and $b \in R \setminus \{0\}$ the following is fulfilled: **i)** There are (not necessarily unique) $q, r \in R$ such that $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$, and **ii)** if $a \mid b$ then $\delta(a) \leq \delta(b)$. (Actually, the latter condition can be dispensed of.)

Let now $\mathcal{O} := \mathbb{Z}[i]$. Since monotonicity follows from multiplicativity of N, we only have to show that quotients and remainders exist: Let $u, v \in \mathcal{O}$ such that $v \neq 0$, let $uv^{-1} = s + it \in \mathbb{Q}(i)$ for some $s, t \in \mathbb{Q}$, let $x, y \in \mathbb{Z}$ such that $|s - x| \leq \frac{1}{2}$ and $|t - y| \leq \frac{1}{2}$, and let $q := x + iy \in \mathcal{O}$ and $r := u - qv \in \mathcal{O}$.

Then $r = v(uv^{-1} - q)$, where $uv^{-1} - q = (s - x) + i(t - y)$. From $N(uv^{-1} - q) = (s - x)^2 + (t - y)^2 \leq \frac{1}{2}$ we get $N(r) = N(v)N(uv^{-1} - q) \leq \frac{1}{2}N(v)$. ♯

(1.4) Gaussian primes. We proceed to describe the primes of the factorial domain $\mathcal{O} := \mathbb{Z}[i]$. This is achieved by relating them to the primes of $\mathbb{Z}$, also called **rational primes**; let $\mathcal{P}_\mathbb{Z} \subseteq \mathbb{Z}$ be the set of positive rational primes.

Lemma. Let $\pi \in \mathcal{O}$ be a prime. Then there is a unique $p \in \mathcal{P}_\mathbb{Z}$ such that $\pi \mid p \in \mathcal{O}$, and we have $N(\pi) \in \{p, p^2\}$.

Proof. We have $N(\pi) \in \mathbb{Z}$ such that $N(\pi) > 1$. Hence we consider the factorization of $N(\pi)$ in $\mathbb{Z}$. From $\pi \mid N(\pi) = \pi\overline{\pi} \in \mathcal{O}$, and $\pi \in \mathcal{O}$ being a prime, we infer that there is a prime divisor $p \mid N(\pi) \in \mathbb{Z}$ such that $\pi \mid p \in \mathcal{O}$.

Hence we get $N(\pi) \mid N(p) = p^2 \in \mathbb{Z}$, thus $N(\pi) \in \{p, p^2\}$. This also shows that $p \in \mathcal{P}_\mathbb{Z}$ such that $\pi \mid p \in \mathcal{O}$ is uniquely determined. ♯

Theorem. Let $\pi \in \mathcal{O}$ be a prime, and let $p \in \mathcal{P}_{\mathbb{Z}}$ such that $\pi \mid p \in \mathcal{O}$.

i) If $p = 2$, then we have $2 \sim (1+i)^2$, in other words $\pi \in \{\pm 1 \pm i\}$ are the prime divisors of 2 in $\mathcal{O}$; the rational prime 2 is called **ramified** in $\mathcal{O}$.

ii) If $p \equiv -1 \pmod 4$, then we have $\pi \sim p$, in other words $\pi \in \{\pm p, \pm ip\}$ are the prime divisors of p in $\mathcal{O}$; the rational prime p is called **non-split** in $\mathcal{O}$.

iii) If $p \equiv 1 \pmod 4$, then we have $p \sim \pi\overline{\pi}$, where $\pi \not\sim \overline{\pi}$, in other words $\{\pm\pi, \pm i\pi, \pm\overline{\pi}, \pm i\overline{\pi}\}$ are the prime divisors of p in $\mathcal{O}$; the rational prime p is called **split** in $\mathcal{O}$.

Proof. i) Let $p = 2$. From $N(1+i) = 2$ we infer that $1+i \in \mathcal{O}$ is a prime. We get the factorization $(1+i)^2 \sim (1+i)(1-i) = 2 \in \mathcal{O}$, implying $\pi \sim 1+i$.

ii) Let $p \equiv -1 \pmod 4$. Assume that $N(\pi) = p$, then writing $\pi = a + ib$ for some $a, b \in \mathbb{Z}$, we get $p = a^2 + b^2 \equiv \{0, 1\} \pmod 4$, a contradiction. Hence we have $N(\pi) = p^2 = N(p)$, which since $\pi \mid p$ entails $\pi \sim p$.

iii) Let $p \equiv 1 \pmod 4$. Then by **Artin's Theorem** we have $(\mathbb{Z}/(p))^* \cong C_{p-1}$, thus $(\mathbb{Z}/(p))^*$ has an element of order 4. Hence the quadratic congruence $X^2 + 1 \equiv 0 \pmod p$ is solvable in $\mathbb{Z}$; let $x \in \mathbb{Z}$ such that $p \mid x^2 + 1 \in \mathbb{Z}$. Hence we have $p \mid (x+i)(x-i) \in \mathcal{O}$, but since $\frac{1}{p}(x \pm i) \in \mathbb{Q}(i) \setminus \mathcal{O}$ we have $p \nmid (x \pm i)$, implying that $p \in \mathcal{O}$ is not a prime.

We have $\pi \mid p \mid (x+i)(x-i)$, so that (up to conjugation) we may assume that $\pi \mid (x+i)$. Assume that $\pi \sim \overline{\pi}$; then $\pi \sim \overline{\pi} \mid \overline{x+i} = x - i$, hence $\pi \mid \big((x+i) - (x-i)\big) = 2i$, implying $p = N(\pi) \mid N(2i) = 4$, a contradiction. Hence we have $\pi \not\sim \overline{\pi}$. From $\overline{\pi} \mid \overline{p} = p$ we get $\pi\overline{\pi} \mid p$. Thus from $N(\pi\overline{\pi}) = p^2 = N(p)$ we infer $\pi\overline{\pi} \sim p$. ♯

The above proof also shows that in case iii) the factorization of $p \equiv 1 \pmod 4$ can be found algorithmically as follows:

• We determine $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$: Actually **Wilson's Theorem [1770]**, see Exercise (14.1), says that $x \in \{\pm(\frac{p-1}{2})! \pmod p\}$; instead we may just run through $x \in \{0, \ldots, p-1\}$ incrementally, and check whether $x^2 \equiv -1 \pmod p$; or we may pick $y \in \{0, \ldots, p-1\}$ randomly, and check whether $y^{\frac{p-1}{2}} \equiv 1 \pmod p$, if not then $y^{\frac{p-1}{2}} \equiv -1 \pmod p$ implies that $x \in \{\pm y^{\frac{p-1}{4}} \pmod p\}$. (Note that both deterministic methods need $O(p)$ multiplications modulo p, thus run in exponential time; the randomized method finds a non-square modulo p with probability $\frac{p-1}{2p} \sim \frac{1}{2}$, while taking powers needs $O(\ln p)$ multiplications modulo p, so that this runs in linear time.)

• Now note that $\pi \nmid (x-i)$, that is $\overline{\pi} \nmid (x+i)$, hence $\pi \in \gcd(p, x+i) \subseteq \mathcal{O}$. Thus we just compute $\pi = a + bi \in \gcd(p, x+i) \subseteq \mathcal{O}$ using the Euclidean algorithm, where (up to associates) we may assume that $0 \le a \le b$. (It is well-known that the Euclidean algorithm over $\mathbb{Z}$, and thus over $\mathcal{O}$, runs in polynomial time.)

Table 1: Primes as sums of two squares.

p		a		b	p		a		b	p		a		b
5	=	1^2	+	2^2	113	=	7^2	+	8^2	277	=	9^2	+	14^2
13	=	2^2	+	3^2	137	=	4^2	+	11^2	281	=	5^2	+	16^2
17	=	1^2	+	4^2	149	=	7^2	+	10^2	293	=	2^2	+	17^2
29	=	2^2	+	5^2	157	=	6^2	+	11^2	313	=	12^2	+	13^2
37	=	1^2	+	6^2	173	=	2^2	+	13^2	317	=	11^2	+	14^2
41	=	4^2	+	5^2	181	=	9^2	+	10^2	337	=	9^2	+	16^2
53	=	2^2	+	7^2	193	=	7^2	+	12^2	349	=	5^2	+	18^2
61	=	5^2	+	6^2	197	=	1^2	+	14^2	353	=	8^2	+	17^2
73	=	3^2	+	8^2	229	=	2^2	+	15^2	373	=	7^2	+	18^2
89	=	5^2	+	8^2	233	=	8^2	+	13^2	389	=	10^2	+	17^2
97	=	4^2	+	9^2	241	=	4^2	+	15^2	397	=	6^2	+	19^2
101	=	1^2	+	10^2	257	=	1^2	+	16^2	401	=	1^2	+	20^2
109	=	3^2	+	10^2	269	=	10^2	+	13^2	409	=	3^2	+	20^2

(1.5) Corollary: Primes as sums of two squares [Fermat, 1640]**.**
A prime $p \in \mathcal{P}_{\mathbb{Z}}$ is a sum of two squares in $\mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$, in which case there is a unique representation $p = a^2 + b^2$, where $a, b \in \mathbb{N}$ such that $a \leq b$.

Proof. We may assume that $p \equiv 1 \pmod 4$. We show that the decompositions of p coincide with the solutions of the norm equation $N(\cdot) = p$ in $\mathcal{O} := \mathbb{Z}[i]$: Letting $\pi = a+bi \in \mathcal{O}$ be a prime divisor of p, then we have $p = N(\pi) = a^2+b^2$; conversely, if $p = a^2 + b^2$, then letting $\pi := a + bi \in \mathcal{O}$ we have $\pi\overline{\pi} = N(\pi) = p$, implying that π is a prime divisor of p. Finally, uniqueness follows from the fact that the prime divisors of p are given as $\{\pm a \pm ib, \pm b \pm ia\}$. ♯

Example. i) For $p = 5$ we get $x = 2$ and $\pi \sim 2 + i$, hence $p = 1^2 + 2^2$.
ii) For $p = 13$ we get $x = 5$ and $\pi \sim 2 + 3i$, hence $p = 2^2 + 3^2$.
iii) For $p = 313$ we get $x = 25$ and $\pi \sim 12 + 13i$, hence $p = 12^2 + 13^2$.
iv) For $p = 317$ we get $x = 114$ and $\pi \sim 11 + 14i$, hence $p = 11^2 + 14^2$.

(1.6) Theorem: Two-squares Theorem [Euler, 1754]**.**
Let $n = 2^c \cdot \prod_{k=1}^{r} p_k^{a_k} \cdot \prod_{l=1}^{s} q_l^{b_l} \in \mathbb{N}$, where $p_k, q_l \in \mathcal{P}_{\mathbb{Z}}$ are pairwise distinct odd primes, such that $p_k \equiv 1 \pmod 4$ and $q_l \equiv -1 \pmod 4$, and where $c \in \mathbb{N}_0$ and $a_k, b_l \in \mathbb{N}$ for some $r, s \in \mathbb{N}_0$.

i) Then n is a sum of two squares in $\mathbb{Z}$ if and only if $b_1, \ldots, b_s$ are all even.

ii) There is a **primitive** representation $n = a^2+b^2$, that is $a, b \in \mathbb{Z}$ are coprime, if and only if $c \in \{0, 1\}$ and $s = 0$. In this case, for $r = 0$ we have $1 = 0^2 + 1^2$

and $2 = 1^2 + 1^2$, and for $r \geq 1$ there are precisely 2^{r-1} primitive representations such that $a, b \in \mathbb{N}$ such that $a \leq b$.

Proof. i) If $n = a^2 + b^2 = N(a + bi) = (a + bi)(a - bi)$, where $a, b \in \mathbb{Z}$, then we have the factorization $a + bi \sim (1 + i)^c \cdot \prod_{k=1}^{r} (\pi_k^{\alpha_k} \overline{\pi}_k^{a_k - \alpha_k}) \cdot \prod_{l=1}^{s} q_l^{\frac{b_l}{2}} \in \mathbb{Z}[i]$, where $p_k \sim \pi_k \overline{\pi}_k \in \mathbb{Z}[i]$ and $\alpha_k \in \{0, \ldots, a_k\}$. Hence the b_l are all even.

Conversely, if the latter holds, then any element of $\mathbb{Z}[i]$ having a factorization as above gives rise to a decomposition of n as a sum of two squares in $\mathbb{Z}$.

ii) If n has a primitive representation, then from $2^{\lfloor \frac{c}{2} \rfloor} \cdot \prod_{l=1}^{s} q_l^{\frac{b_l}{2}} \mid \gcd(a, b) \in \mathbb{Z}$ we get $c \leq 1$ and $s = 0$. Hence let conversely $a+bi \sim (1+i)^c \cdot \prod_{k=1}^{r} (\pi_k^{\alpha_k} \overline{\pi}_k^{a_k - \alpha_k})$, where $c \in \{0, 1\}$. The case $r = 0$ being immediate, we may assume that $r \geq 1$.

Then a and b are not coprime, if and only if there is a prime $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \mid a + bi \in \mathbb{Z}[i]$. From the factorization of $a + bi$ we infer that this is equivalent to having $\pi_k \overline{\pi}_k \sim p_k \mid a + bi$ for some k, which in turn amounts to say that $\alpha_k \notin \{0, a_k\}$. In other words, the primitive representations are given by choosing $\alpha_k \in \{0, a_k\}$ for all k, so that there are 2^r choices in total. ♯

Example. For $n := 65 = 5 \cdot 13$, up to conjugation we get $a+bi \sim (2+i)(3+2i) = 4 + 7i$ and $a + bi \sim (2 + i)(3 - 2i) = 8 - i$, hence $65 = 4^2 + 7^2 = 1^2 + 8^2$.

(1.7) Remark. Recall (an easy special case of) the theorem on primes in coprime residue classes [Dirichlet, 1837], in particular saying that there are both infinitely many positive rational primes congruent to 1 (mod 4) and congruent to -1 (mod 4), see Exercise (14.2). Thus there are infinitely many primes (or likewise integers) which can be written as a sum of two squares in $\mathbb{Z}$, and infinitely many positive primes (or likewise positive integers) which cannot.

Hence we may ask how 'dense' the set of integers which are a sum of two squares in $\mathbb{Z}$ is, as a subset of all positive integers [Landau, 1909]: Letting $\sigma_2(x) := |\{n \in \mathbb{N}; n \leq x, n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}|$, for $x \in \mathbb{R}_{>0}$, we have $\lim_{x \to \infty} \left(\sigma_2(x) \cdot \frac{\sqrt{\ln(x)}}{x}\right) = c > 0$, hence $\lim_{x \to \infty} \frac{\sigma_2(x)}{x} = 0$.

2 Galois theory

We recall some notions and facts from Galois theory needed in the sequel.

(2.1) Field extensions. Let K be a field, let $\overline{K}$ be a (fixed field containing) an algebraic closure of K, and let $K \subseteq L$ be a finite (hence algebraic) field extension, where we may assume that $L \subseteq \overline{K}$. The extension $K \subseteq L$ is called **simple**, if there is a **primitive element** $a \in L$ such that $L = K(a)$.

Let $\mathrm{Inj}_K(L) = \mathrm{Hom}_{K\text{-algebra}}(L, \overline{K})$ be the set of all K-algebra homomorphisms from L into $\overline{K}$; in particular, these restrict to the identity on K, and thus are embeddings. We have $\mathrm{Aut}_K(L) \subseteq \mathrm{Inj}_K(L)$, where the group $\mathrm{Aut}_K(L)$ of K-algebra automorphisms of L is called the **Galois group** of L over K.

Theorem: [KRONECKER]**.** Let $f \in K[X]$ be irreducible, and $a \in \overline{K}$ such that $f(a) = 0$. Then for $x \in \overline{K}$ there is a (unique) K-algebra (iso)morphism $\varphi\colon K(a) \to K(x)$ such that $a^\varphi = x$, if and only if $f(x) = 0$.

Proof: (idea). Letting $X \mapsto a$ induces an isomorphism $K[X]/(f) \to K(a)$. ♯

(2.2) Normality. Let K be a field, let $\overline{K}$ be an algebraic closure of K, and let $K \subseteq L$ be a finite field extension, where we assume that $L \subseteq \overline{K}$. The extension $K \subseteq L$ is called **normal**, if any irreducible polynomial in $K[X]$ having a root in L already splits in $L[X]$.

If $f \in K[X]$ is non-constant such that $n := \deg(f) \in \mathbb{N}$, and splits over $\overline{K}$ as $f = a \cdot \prod_{i=1}^{n}(X - a_i) \in \overline{K}[X]$, then $M := K(a_1, \ldots, a_n) \subseteq \overline{K}$ is called the **splitting field** of f in $\overline{K}$; the extension $K \subseteq M$ is finite of degree $[M\colon K] \mid n!$.

Theorem. The extension $K \subseteq L$ is normal, if and only if L is the splitting field of some non-constant polynomial in $K[X]$. ♯

(2.3) Separability. Let K be a field, let $\overline{K}$ be an algebraic closure of K, and let $K \subseteq L$ be a finite field extension, where we assume that $L \subseteq \overline{K}$.

An irreducible polynomial in $K[X]$ is called **separable**, if it has only simple roots in $\overline{K}$, or equivalently (by Kronecker's Theorem) if it has a simple root in $\overline{K}$. A non-constant polynomial in $K[X]$ is called **separable**, if all its irreducible divisors are separable. (Note that we do not require that the polynomial in question is square-free, as is sometimes done in the literature.)

Separability can actually be checked without referring to $\overline{K}$: Letting $\partial = \partial_X \in \mathrm{End}_K(K[X])$ be the **(formal) derivative** with respect to X, given by $\partial(1) = 0$ and $\partial(X^d) = dX^{d-1}$ for $d \in \mathbb{N}$. Then an irreducible polynomial in $f \in K[X]$ is separable if and only if f and $\partial(f)$ are coprime.

The field K is called **perfect** if all irreducible polynomials in $K[X]$ are separable. In particular, a consideration of derivatives shows that fields of characteristic 0 and finite fields are perfect.

An element $a \in L$ is called **separable** over K, if its (irreducible) minimum polynomial $\mu_a \in K[X]$ over K is separable. The extension $K \subseteq L$ is called **separable** if any element of L is separable over K; this holds if and only if L is generated by separable elements (which follows from the general main theorem of Galois theory). In particular, any finite extension of a perfect field is separable.

Theorem: Existence of primitive elements. Let $c_1, \ldots, c_r \in \overline{K}$ be separable over K, where $r \in \mathbb{N}$, and $b \in \overline{K}$. Then $K \subseteq K(c_1, \ldots, c_r, b)$ is simple.

Proof. Letting $a := c_1$, by induction over r it suffices to show that $K \subseteq K(a, b)$ is simple, where we may assume that $a \notin K$. If K is finite, then $K(a, b)$ is finite as well, thus $K(a, b)^*$ is cyclic, hence $K \subseteq K(a, b)$ is simple. Hence we may assume that K is infinite.

Let $\mu_a, \mu_b \in K[X]$ be the minimum polynomials of a and b over K, respectively. We have $\mu_a = \prod_{i=1}^{n}(X - a_i) \in \overline{K}[X]$, where the a_i are pairwise distinct, for some $n \geq 2$, and $a = a_1$ (say), and $\mu_b = \prod_{j=1}^{m}(X - b_j) \in \overline{K}[X]$, for some $m \geq 1$ and $b = b_1$ (say). Let $d \in K \setminus \{\frac{b_j - b}{a - a_i} \in L; i \in \{2, \ldots, n\}, j \in \{1, \ldots, m\}\}$, which since K is infinite is a non-empty set, and let $c := da + b \in K(a, b)$. In order to show that $K(a, b) = K(c)$, it suffices to show that $a \in K(c)$:

Let $f \in \gcd(\mu_a(X), \mu_b(c - dX)) \subseteq K(c)[X]$. Since $\mu_a(a) = 0$ and $\mu_b(c - da) = \mu_b(b) = 0$ we have $X - a \mid f$. Since $f \mid \mu_a$, we conclude that its roots are amongst the a_i. Assume that $\mu_b(c - da_i) = 0$ for some $i \in \{2, \ldots, n\}$, then for some $j \in \{1, \ldots, m\}$ we have $b_j = c - da_i = d(a - a_i) + b$, implying $d = \frac{b_j - b}{a - a_i}$, a contradiction. Thus we have $X - a_i \nmid \mu_b(c - dX)$ for all $i \in \{2, \ldots, n\}$, implying that $X - a_i \nmid f$. This entails that $f \sim X - a \in K(c)[X]$, thus $a \in K(c)$. ♯

Proposition. Let $K \subseteq L$ be separable, and let $K \subseteq M \subseteq L$ be an intermediate field. Then any K-embedding of M into $\overline{K}$ has precisely $[L\colon M]$ extensions to K-embeddings of L into $\overline{K}$. In particular, $|\mathrm{Aut}_K(L)| \leq |\mathrm{Inj}_K(L)| = [L\colon K]$.

Proof. Let $\sigma \in \mathrm{Inj}_K(M)$. Since we may assume that $M \subseteq L$ is simple, by Kronecker's Theorem there is an extension $\widehat{\sigma} \in \mathrm{Inj}_K(L)$ of σ. Then, if $\widetilde{\sigma} \in \mathrm{Inj}_K(L)$ also is an extension of σ, considering $\widehat{\sigma}^{-1}\widetilde{\sigma}\colon L^{\widehat{\sigma}} \to L^{\widetilde{\sigma}}$ shows that the set of all extensions is in bijection with $\mathrm{Inj}_{M^\sigma}(L^{\widehat{\sigma}})$, which by Kronecker's Theorem again has cardinality $[L^{\widehat{\sigma}}\colon M^\sigma] = [L\colon M]$. ♯

(2.4) Galois extensions. Let K be a field, let $\overline{K}$ be an algebraic closure of K, and let $K \subseteq L$ be a separable finite extension, where we assume that $L \subseteq \overline{K}$. For $S \subseteq \mathrm{Aut}_K(L)$ let $K \subseteq \mathrm{Fix}_L(S) \subseteq L$ be the associated **fixed field**. Then the extension $K \subseteq L$ is called **Galois** if $\mathrm{Fix}_L(\mathrm{Aut}_K(L)) = K$. The key observation (which actually holds for any finite field extension) now is a follows:

Theorem: [Artin]**.** For any $H \leq \mathrm{Aut}_K(L)$ we have $[L\colon \mathrm{Fix}_L(H)] = |H|$.

In particular, $K \subseteq L$ is Galois if and only if $|\mathrm{Aut}_K(L)| = [L\colon K]$. ♯

Theorem: Main theorem of Galois theory. The extension $K \subseteq L$ is Galois if and only if it is normal.

Proof: (idea). Considering the minimum polynomial of a primitive element, this follows from Kronecker's Theorem. ♯

Theorem: Galois correspondence. Let $K \subseteq L$ be a Galois extension, and let $G := \mathrm{Aut}_K(L)$. Then the following holds:

i) The following maps are mutually inverse inclusion-reversing bijections:

$$\mathcal{F}\colon \{H \leq G \text{ subgroup}\} \to \{K \subseteq M \subseteq L \text{ intermediate field}\}\colon H \mapsto \mathrm{Fix}_L(H)$$

$$\mathcal{G}\colon \{K \subseteq M \subseteq L \text{ intermediate field}\} \to \{H \leq G \text{ subgroup}\}\colon M \mapsto \mathrm{Aut}_M(L)$$

ii) For a subgroup $H \leq G$ we have $[L\colon \mathrm{Fix}_L(H)] = |H|$, and for an intermediate field $K \subseteq M \subseteq L$ we have $[M\colon K] = [G\colon \mathrm{Aut}_M(L)]$.

iii) For an intermediate field $K \subseteq M \subseteq L$ the extension $K \subseteq M$ is Galois if and only if $M^\sigma = M$ for all $\sigma \in G$, which holds if and only if $\mathrm{Aut}_M(L) \trianglelefteq G$ is a normal subgroup. In this case we have $G/\mathrm{Aut}_M(L) \cong \mathrm{Aut}_K(M)$. ♯

II Algebra

3 Algebraic integers

(3.1) Norm, trace, and discriminant. a) Let $K \subseteq L$ be a finite field extension of degree $n := [L\colon K] = \dim_K(L) \in \mathbb{N}$, and let $\rho = \rho_{L/K}\colon L \to \mathrm{End}_K(L) \cong K^{n\times n}\colon z \mapsto (y \mapsto yz)$ be the (right) regular action of L.

For $z \in L$ let $\chi_z = \chi_{z,L/K} = \chi_{\rho(z)} \in K[X]$ be the characteristic polynomial of $\rho(z)$, also being called the **field polynomial** of z in L/K. Moreover, $N(z) = N_{L/K}(z) := \det(\rho(z)) \in K$ and $T(z) = T_{L/K}(z) := \mathrm{Tr}(\rho(z)) \in K$ are called the **norm** and the **trace** of $z \in L$ over K, respectively. (Recall that $(-1)^n N(z)$ and $-T(z)$ are the constant and second leading coefficients of χ_z, respectively.

From $\rho(az) = a\rho(z)$, for $z \in L$ and $a \in K$, we get $T(az) = aT(z)$ and $N(az) = a^n N(z)$. From $\rho(z)+\rho(y) = \rho(z+y)$ and $\rho(z)\rho(y) = \rho(zy)$, for $z, y \in L$, we infer that $T\colon L \to K$ is K-linear, and that $N\colon L^* \to K^*$ is a group homomorphism.

The symmetric K-bilinear **trace form** of L over K is defined as $L \times L \to K\colon [x, y] \mapsto T(xy) =: \langle x, y\rangle$. Letting $\mathcal{B} := \{y_1, \ldots, y_n\} \subseteq L$ be a K-basis we get the associated Gram matrix $\Gamma_\mathcal{B} := [\langle y_i, y_j\rangle]_{ij} = [T(y_i y_j)]_{ij} \in K^{n\times n}$, and the **discriminant** of $\mathcal{B}$ is defined as the Gram determinant $\mathrm{disc}(\mathcal{B}) := \det(\Gamma_\mathcal{B}) \in K$.

Proposition. For $z \in L$ we have $\chi_z = \mu_z^l$, where $l := [L\colon K(z)]$, as well as $N(z) = (N_{K(z)/K}(z))^l \in K$ and $T(z) = l \cdot T_{K(z)/K}(z) \in K$.

Proof. We consider the extension $K \subseteq K(z) \subseteq L$; recall that the minimum polynomial $\mu_z \in K[X]$ of z over K does not depend on L. We have the K-basis $\mathcal{B} := \{1, z, \ldots, z^{d-1}\} \subseteq K(z)$, where $d := \deg(\mu_z) = [K(z)\colon K]$, and $\rho_{K(z)/K}(z) \in K^{d\times d}$ is the companion matrix associated with μ_z.

Let $\mathcal{C} := \{y_1, \ldots, y_l\} \subseteq L$ be a $K(z)$-basis, where $l = \frac{n}{d}$. Then $\mathcal{C} \cdot \mathcal{B} := \{y_1, y_1 z, \ldots, y_1 z^{d-1}; y_2, y_2 z, \ldots, y_2 z^{d-1}; \ldots\} \subseteq L$ is a K-basis, with respect to which the action of z is given by a block diagonal matrix, all of whose l blocks of size $d \times d$ coincide with the companion matrix $\rho_{K(z)/K}(z)$. Hence we have $\chi_z = \mu_z^l$, as well as $\det(\rho(z)) = \det(\rho_{K(z)/K}(z))^l$ and $\mathrm{Tr}(\rho(z)) = l \cdot \mathrm{Tr}(\rho_{K(z)/K}(z))$. ♯

(3.2) Field embeddings. a) The above notions are closely related to Galois theory: Let $K \subseteq L$ be a separable finite extension of degree $n := [L\colon K]$, let $\overline{K}$ be (a field containing) an algebraic closure of K, where we assume that $L \subseteq \overline{K}$, and let $I := \mathrm{Inj}_K(L)$. For $z \in L$, the elements $z^\sigma \in \overline{K}$, for $\sigma \in I$, are called its **(algebraic) conjugates**. We first consider norms and traces:

Proposition. For $z \in L$ we have $\chi_z = \prod_{\sigma\in I}(X - z^\sigma) \in \overline{K}[X]$; in particular we have $N(z) = \prod_{\sigma\in I} z^\sigma \in \overline{K}$ and $T(z) = \sum_{\sigma\in I} z^\sigma \in \overline{K}$.

Proof. $\chi_{z,K(z)/K} = \mu_z = \prod_{\sigma\in I_z}(X - z^\sigma) \in \overline{K}[X]$, where $I_z := \mathrm{Inj}_K(K(z))$. Since any K-embedding of $K(z)$ into $\overline{K}$ extends to $l := [L\colon K(z)]$ embeddings of L, we get $\chi_z = \mu_z^l = \prod_{\sigma\in I_z}(X - z^\sigma)^l = \prod_{\sigma\in I}(X - z^\sigma) \in \overline{K}[X]$. ♯

Proposition. Let $K \subseteq M \subseteq L$ be an intermediate field. Then we have **transitivity**, saying that $N_{M/K} \circ N_{L/M} = N_{L/K}$ and $T_{M/K} \circ T_{L/M} = T_{L/K}$.

Proof. Let $\{\sigma_1, \ldots, \sigma_m\} \subseteq I$ such that $\mathrm{Inj}_K(M) = \{\sigma_1|_M, \ldots, \sigma_m|_M\}$, where $m = [M\colon K]$. For $i \in \{1, \ldots, m\}$ let $\mathrm{Inj}_{M^{\sigma_i}}(L^{\sigma_i}) = \{\tau_{i,1}, \ldots, \tau_{i,l}\}$, where $l = [L\colon M]$. Thus from $I = \{\sigma_i\tau_{i,j}; i \in \{1, \ldots, m\}, j \in \{1, \ldots, l\}\}$ we get $N_{L/K}(z) = \prod_{\sigma\in I} z^\sigma = \prod_{i=1}^l \prod_{j=1}^m (z^{\sigma_i})^{\tau_{i,j}} = \prod_{i=1}^l N_{L^{\sigma_i}/M^{\sigma_i}}(z^{\sigma_i}) = \prod_{i=1}^l N_{L/M}(z)^{\sigma_i} = N_{M/K}(N_{L/M}(z))$, and similarly $T_{L/K}(z) = \sum_{\sigma\in I} z^\sigma = \sum_{i=1}^l \sum_{j=1}^m (z^{\sigma_i})^{\tau_{i,j}} = \sum_{i=1}^l T_{L^{\sigma_i}/M^{\sigma_i}}(z^{\sigma_i}) = \sum_{i=1}^l T_{L/M}(z)^{\sigma_i} = T_{M/K}(T_{L/M}(z))$ ♯

b) Now we turn to discriminants: Letting $\mathcal{B} := \{y_1, \ldots, y_n\} \subseteq L$ be a K-basis, and $I = \{\sigma_1, \ldots, \sigma_n\}$, we have $T(y_i y_j) = \sum_{k=1}^n (y_i y_j)^{\sigma_k} = \sum_{k=1}^n y_i^{\sigma_k} y_j^{\sigma_k}$, hence letting $\Delta_\mathcal{B} := [y_j^{\sigma_i}]_{ij} \in \overline{K}^{n\times n}$ we get $\Gamma_\mathcal{B} = \Delta_\mathcal{B}^{\mathrm{tr}} \cdot \Delta_\mathcal{B}$, so that $\mathrm{disc}(\mathcal{B}) = \det(\Delta_\mathcal{B})^2$.

Proposition. The trace form $\langle \cdot, \cdot \rangle$ is non-degenerate, or equivalently for any K-basis $\mathcal{B} \subseteq L$ we have $\mathrm{disc}(\mathcal{B}) \neq 0$.

(Conversely, non-degeneracy of the trace form implies separability of the field extension; but we will neither need nor prove this fact here.)

Proof. There is a primitive element $z \in L$ such that $L = K(z)$. Hence letting $z_i := z^{\sigma_i} \in \overline{K}$, the z_i are pairwise distinct. For the K-basis $\mathcal{B} := \{1, z, , \ldots, z^{n-1}\} \subseteq L$ we have $\Delta_{\mathcal{B}} = [(z^{j-1})^{\sigma_i}]_{ij} = [z_i^{j-1}]_{ij}$, which is the **Vandermonde matrix** associated with $\{z_1, \ldots, z_n\}$. From this we get $\operatorname{disc}(\mathcal{B}) = \det(\Delta_{\mathcal{B}}) = \prod_{1 \le i < j \le n}(z_i - z_j)^2 = (-1)^{\binom{n}{2}} \cdot \prod_{i,j \in \{1,\ldots,n\}, i \ne j}(z_i - z_j) \ne 0$. ♯

For z as above, having minimum polynomial $\mu_z \in K[X]$, the element $\operatorname{disc}(z) = \operatorname{disc}(\mu_z) := \operatorname{disc}(\mathcal{B}) \in K^*$ is also called the **discriminant** of z and of μ_z.

Corollary. We have $\operatorname{disc}(z) = (-1)^{\binom{n}{2}} \cdot N_{L/K}((\partial\mu_z)(z))$.

Proof. We have $\partial\mu_z = \sum_{i=1}^n \big(\prod_{j \ne i}(X - z_j)\big) \in \overline{K}[X]$. Hence for $z = z_1$, say, we get $(\partial\mu_z)(z_1) = \prod_{j=2}^n (z_1 - z_j)$, thus $N_{L/K}((\partial\mu_z)(z_1)) = \prod_{i=1}^n \big(\prod_{j \ne i}(z_i - z_j)\big) = \prod_{i,j \in \{1,\ldots,n\}, i \ne j}(z_i - z_j) = (-1)^{\binom{n}{2}} \cdot \prod_{1 \le i < j \le n}(z_i - z_j)^2 = (-1)^{\binom{n}{2}} \cdot \operatorname{disc}(z)$. ♯

Example. We consider the Gaussian numbers $\mathbb{Q}(i)$, see (1.2). Then $\mathbb{Q} \subseteq \mathbb{Q}(i)$ is Galois such that $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(i)) = \{\mathrm{id}, \kappa\}$, where $\kappa\colon z = x + iy \mapsto \overline{z} = x - iy$ is conjugation. Thus we have $T(z) = z + \overline{z} = 2x$ and $N(z) = z\overline{z} = x^2 + y^2$.

Moreover, $\mathbb{Q}(i)$ has $\mathbb{Q}$-basis $\mathcal{B} := \{1, i\}$. This yields $\Gamma_{\mathcal{B}} = \begin{bmatrix} T(1) & T(i) \\ T(i) & T(-1) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$ and $\Delta_{\mathcal{B}} = \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$, hence $\operatorname{disc}(\mathcal{B}) = \det(\Gamma_{\mathcal{B}}) = \det(\Delta_{\mathcal{B}})^2 = -4$.

(3.3) Integral extensions. Let R be a commutative (unital) ring, and let $R \subseteq S$ be an **extension** of commutative rings, that is S is a commutative (unital) ring and we have $1_R = 1_S$. (Note that, for example, $R \to R \oplus \{0\} \subseteq R \oplus R = S$ does not qualify.) In other words, S is an R-algebra with structure homomorphism being the identity on R.

An element $s \in S$ is called **integral** over R, if there is $0 \ne f \in R[X]$ monic, such that $f(s) = 0 \in S$; note that in particular $R \ne \{0\}$, that f is necessarily non-constant, and that evaluating f at s refers to the universal property of $R[X]$. The extension $R \subseteq S$ is called **integral**, and S is called **integral** over R, if each element of S is integral over R.

Theorem. An element $s \in S$ is integral over R, if and only if there is an R-subalgebra of S containing s which is finitely generated as an R-module.

Proof. For $s \in S$ let $R \subseteq R[s] := \sum_{i \ge 0} s^i R \subseteq S$ be the smallest R-subalgebra of S containing s. Let now s be integral, and let $f = X^d + \sum_{i=0}^{d-1} f_i X^i \in R[X]$, where $d \ge 1$, such that $f(s) = 0$. Then we have $s^d = -\sum_{i=0}^{d-1} f_i s^i$, so that $R[s] = \sum_{i=0}^{d-1} s^i R$ is generated by $\{1, s, s^2 \ldots s^{d-1}\}$ as an R-module.

Let conversely $R \subseteq R[s] \subseteq T \subseteq S$, where T is an R-subalgebra which is finitely generated by $\{t_1, \ldots, t_k\}$ as an R-module, where $k \in \mathbb{N}$. Then for $j \in \{1, \ldots, k\}$ we have $t_j s = \sum_{i=1}^{k} t_i a_{ij}$, for some $a_{ij} \in R$. Let $A := XE_k - [a_{ij}] \in R[X]^{k \times k}$ be the characteristic matrix associated with $[a_{ij}] \in R^{k \times k}$. Thus $\det(A) \in R[X]$ is monic of degree $k \geq 1$. We show that $\det(A)(s) = \det(A(s)) = 0$, entailing that s is integral over R:

We have $[t_1, \ldots, t_k] \cdot A(s) = 0 \in T^k$. Hence by Cramer's Rule we have $0 = [t_1, \ldots, t_k] \cdot A(s) \cdot \mathrm{adj}(A(s)) = [t_1, \ldots, t_k] \cdot \det(A(s)) \in T^k$, thus $t_i \cdot \det(A(s)) = 0$, for all $i \in \{1, \ldots, k\}$. Thus since $1 \in T$ is an R-linear combination of $\{t_1, \ldots, t_k\}$, we infer that $\det(A(s)) = 0$. ♯

Corollary. i) The extension $R \subseteq S$ is integral if and only if S is generated as an R-algebra by integral elements.

ii) Given extensions $R \subseteq S \subseteq T$, then $R \subseteq T$ is integral if and only if both $R \subseteq S$ and $S \subseteq T$ are integral.

Proof. i) We may assume that $S = R[\mathcal{T}]$, where $\mathcal{T}$ is integral over R. Picking $s \in S$, there are $\{t_1, \ldots, t_k\} \subseteq \mathcal{T}$, where $k \in \mathbb{N}_0$, such that $s \in R[t_1, \ldots, t_k]$. Since t_i is integral over $R[t_1, \ldots, t_{i-1}]$, we conclude that $R[t_1, \ldots, t_i]$ is a finitely generated $R[t_1, \ldots, t_{i-1}]$-module, for all $i \in \{1, \ldots, k\}$. Hence by induction over k we infer that $R[t_1, \ldots, t_k]$ is a finitely generated R-module.

ii) We may assume that $R \subseteq S$ and $S \subseteq T$ are integral. Picking $t \in T$, there is $0 \neq f = X^d + \sum_{i=0}^{d-1} s_i X^i \in S[X]$, where $d \geq 1$, such that $f(t) = 0$. Hence $S' := R[s_1, \ldots, s_{d-1}]$ is a finitely generated R-module, $S'[t]$ is a finitely generated S'-module, so that $S'[t]$ is a finitely generated R-module. ♯

The extension $R \subseteq S$ is called **finite**, if S is a finitely generated integral R-algebra (where it suffices to assume that some generating set is integral), or equivalently if S is a finitely generated R-module.

(3.4) Integral closure. Let $R \subseteq S$ be a ring extension. The subset $R \subseteq \overline{R} = \overline{R}^S := \{s \in S; s \text{ is integral over } R\} \subseteq S$ is a subring of S, being called the **integral closure** or **normalization** of R in S. We have $\overline{\overline{R}} = \overline{R}$, so that taking the integral closure is a closure operator indeed.

In particular, if $\overline{R}^S = R$ then R is called **integrally closed** or **normal** in S. And even more specifically, if R is a domain and R is integrally closed in its field of fractions $\mathrm{Q}(R)$, then R is just called **integrally closed** or **normal**.

Proposition. If R is factorial then it is integrally closed.

Proof. Let $s = \frac{a}{b} \in \mathrm{Q}(R)$, where $a, b \in R \setminus \{0\}$ are coprime, be integral over R, and let $0 \neq f = X^d + \sum_{i=0}^{d-1} r_i X^i \in R[X]$, where $d \geq 1$, such that $f(s) = 0$. This

yields $a^d = -\sum_{i=0}^{d-1} r_i a^i b^{d-i} \in R$. Thus any prime of R dividing b also divides a. By the coprimeness of a and b, this implies $b \in R^*$, so that $s = \frac{a}{b} \in R$. ♯

(3.5) Integrality in field extensions. Let R be an integrally closed domain, let $K := \mathrm{Q}(R)$ be its field of fractions, and let $\overline{K}$ be an algebraic closure of K. Moreover, let $K \subseteq L$ be a finite field extension, where we assume that $L \subseteq \overline{K}$, and let $S := \overline{R}^L$ be the integral closure of R in L. Hence we have $S \cap K = R$.

Proposition. i) For $z \in L$, let $\mu_z \in K[X]$ be its (monic) minimum polynomial over K. Then we have $z \in S$ if and only if $\mu_z \in R[X]$.

ii) For any $z \in L$ there is $0 \neq r \in R$ such that $rz \in S$. In particular, we have $L = \mathrm{Q}(S)$, so that S is an integrally closed domain as well.

iii) Let $z \in S$. Then we have $N(z) \in R$ and $T(z) \in R$. Moreover, we have $z \mid N(z) \in S$, so that in particular $z \in S^*$ if and only if $N(z) \in R^*$.

Proof. i) We may assume that $z \in S$. Then we have $\mu_z = \prod_{i=1}^{d}(X - z_i) \in M[X]$, where $d \geq 1$ and $K \subseteq M$ is the splitting field of μ_z in $\overline{K}$; note that the z_i are not necessarily pairwise distinct. Let $0 \neq f \in R[X]$ monic such that $f(s) = 0$. Then we have $\mu_z \mid f \in K[X]$. Thus $f(z_i) = 0$, saying that z_i is integral over R. Hence $\{z_1, \ldots, z_d\} \subseteq T := \overline{R}^M$ implies that $\mu_z \in T[X] \cap K[X] = R[X]$.

ii) Multiplying μ_z with a suitable element of R we get $f = \sum_{i=0}^{d} r_i X^i \in R[X]$, where $d \geq 1$ and $r_d \neq 0$, such that $f(z) = 0$. Hence $r_d^{d-1} f = (r_d X^d)^d + \sum_{i=0}^{d-1} r_i r_d^{d-i-1} (r_d X)^i \in R[X]$ shows that $r_d z \in L$ is integral over R.

iii) Since $\rho(z)$ can be chosen as a block diagonal matrix, whose blocks are companion matrices associated with $\mu_z \in R[X]$, we infer that $N(z) = \det(\rho(z)) \in R$ and $T(z) = \mathrm{Tr}(\rho(z)) \in R$.

From $N(z) = (\prod_{i=1}^{d} z_i)^m$, where $m := [L\colon K(z)]$ and the z_i are as above, we conclude $z \mid N(z) \in T$, where $\frac{N(z)}{z} \in T \cap L \subseteq S$. In particular, if $N(z) \in R^* \subseteq S^*$, then we have $z \in S^*$ as well; conversely, if $zz' = 1 \in S$ for some $z' \in S$, then we have $N(z)N(z') = N(zz') = N(1) = 1 \in R$, hence $N(z) \in R^*$. ♯

(3.6) Integral bases. a) Let R be a principal ideal domain, let $K := \mathrm{Q}(R)$ be its field of fractions, and let $\overline{K}$ be an algebraic closure of K. Moreover, let $K \subseteq L$ be a separable finite extension of degree $n := [L\colon K]$, where we assume that $L \subseteq \overline{K}$, and let $S := \overline{R}^L$ be the integral closure of R in L.

Theorem. Any ideal $\{0\} \neq I \trianglelefteq S$ is R-free of rank n.

Hence in particular S is R-free of rank n. An R-basis of S is called an **integral basis** of L over K, which by (3.5) indeed is a K-basis of L.

Proof. Let $\mathcal{B} := \{\alpha_1, \ldots, \alpha_n\} \subseteq L$ be a K-basis. Then, by (3.5), by multiplying $\mathcal{B}$ with a suitable element of $R \setminus \{0\}$, we may assume that $\mathcal{B} \subseteq S$. Let $\delta := \operatorname{disc}(\mathcal{B}) = \det(\Gamma_{\mathcal{B}}) \in R$, where by the separability of $K \subseteq L$ we have $\delta \neq 0$.

Then we have $\delta S \subseteq \langle \mathcal{B} \rangle_R$: Letting $\alpha \in S$, there are (unique) $x_j \in K$ such that $\alpha = \sum_{j=1}^n x_j \alpha_j$; then we have $[x_1, \ldots, x_n] \cdot \Gamma_{\mathcal{B}} = [\sum_{j=1}^n x_j T(\alpha_j \alpha_i)]_i = [T(\alpha \alpha_i)]_i \in R^n$. Hence by Cramer's Rule we get $[x_1, \ldots, x_n] \cdot \Gamma_{\mathcal{B}} \cdot \operatorname{adj}(\Gamma_{\mathcal{B}}) = \delta \cdot [x_1, \ldots, x_n] \in R^n$, thus $x_j \in \frac{1}{\delta} \cdot R$ for all $j \in \{1, \ldots, n\}$, so that $S \subseteq \frac{1}{\delta} \cdot \langle \mathcal{B} \rangle_R$.

Hence we have $\delta I \subseteq \delta S \subseteq \langle \mathcal{B} \rangle_R \subseteq S$. Since $\langle \mathcal{B} \rangle_R$ is a finitely generated free module over the principal ideal domain R, it follows that I and S are finitely generated free R-modules as well. Moreover, from $\operatorname{rk}_R(S) = \operatorname{rk}_R(\delta S) \leq \operatorname{rk}_R(\langle \mathcal{B} \rangle_R) \leq \operatorname{rk}_R(S)$ we get $\operatorname{rk}_R(S) = n$.

Since L does not contain any zero-divisors, for any $0 \neq u \in I$ the homomorphism of S-modules $S \to I \colon \alpha \mapsto u\alpha$ is injective. Hence we have $n = \operatorname{rk}_R(S) \leq \operatorname{rk}_R(I)$. Thus we get $n \leq \operatorname{rk}_R(I) = \operatorname{rk}_R(\delta I) \leq \operatorname{rk}_R(\langle \mathcal{B} \rangle_R) = n$, hence $\operatorname{rk}_R(I) = n$. ♯

Corollary. Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\} \subseteq L$ be a K-basis contained in S. Then for $\alpha \in S$ we have $\alpha = \frac{1}{\delta} \cdot \sum_{j=1}^n r_j \alpha_j$, where $r_j \in R$ such that $\delta := \operatorname{disc}(\mathcal{B}) \mid r_j^2$.

Proof. Let $K \subseteq M \subseteq \overline{K}$ be the **normal closure** of L in $\overline{K}$, that is the splitting field of the minimum polynomial of a primitive element of L over K, let $T := \overline{R}^M$, and let $\operatorname{Inj}_K(L) = \{\sigma_1, \ldots, \sigma_n\}$. Then we have $\Delta_{\mathcal{B}} = [\alpha_j^{\sigma_i}]_{ij} \in T^{n \times n}$. Letting $\alpha = \sum_{j=1}^n x_j \alpha_j$ as above, where $x_j := \frac{r_j}{\delta} \in K$, we get $[x_1, \ldots, x_n] \cdot \Delta_{\mathcal{B}}^{\mathrm{tr}} = [\sum_{j=1}^n x_j \alpha_j^{\sigma_i}]_i = [\alpha^{\sigma_i}]_i \in T^n$. Hence by Cramer's Rule we have $[x_1, \ldots, x_n] \cdot \Delta_{\mathcal{B}}^{\mathrm{tr}} \cdot \operatorname{adj}(\Delta_{\mathcal{B}}^{\mathrm{tr}}) = \det(\Delta_{\mathcal{B}}) \cdot [x_1, \ldots, x_n] \in T^n$, hence $x_j \in \frac{1}{\det(\Delta_{\mathcal{B}})} \cdot T$, for all $j \in \{1, \ldots, n\}$. Thus recalling that $\delta = \det(\Delta_{\mathcal{B}})^2$ we get $\delta x_j^2 \in \frac{\delta}{\det(\Delta_{\mathcal{B}})^2} \cdot T = T$. Since $\delta x_j^2 = \frac{r_j^2}{\delta} \in K$ we finally get $\frac{r_j^2}{\delta} \in T \cap K = R$. ♯

b) We consider discriminants: To this end let $\mathcal{B} \subseteq S$ be an R-basis.

Let $U \subseteq S$ be a (finitely generated free) R-submodule of (maximal) rank n, and let $\mathcal{C} \subseteq U$ be an R-basis. Hence S/U is a torsion R-module, so that for any $\alpha \in L$ there is $0 \neq r \in R$ such that $r\alpha \in U$ (not only in S). This entails that $\mathcal{C} \subseteq L$ is a K-basis, so that $\operatorname{disc}(\mathcal{C}) = \det(\Gamma_{\mathcal{C}}) \in R \setminus \{0\}$.

There is $A \in \mathrm{GL}_n(K) \cap R^{n \times n}$ such that $\mathcal{C} = \mathcal{B} \cdot A$, implying $\operatorname{disc}(\mathcal{C}) = \det(\Gamma_{\mathcal{C}}) = \det(A^{\mathrm{tr}} \Gamma_{\mathcal{B}} A) = \det(\Gamma_{\mathcal{B}}) \det(A)^2 = \det(A)^2 \cdot \operatorname{disc}(\mathcal{B})$. More specifically, taking Smith normal forms, we conclude that there are R-bases $\mathcal{B}' \subseteq S$ and $\mathcal{C}' \subseteq U$ such that $\mathcal{C}' = \mathcal{B}' \cdot \operatorname{diag}[m_1, \ldots, m_n]$, where $m_1 \mid m_2 \mid \cdots \mid m_n \in R$, so that $\operatorname{disc}(\mathcal{C}') = (\prod_{i=1}^n m_i)^2 \cdot \operatorname{disc}(\mathcal{B}')$.

In particular, we have $U = S$ if and only if $A \in \mathrm{GL}_n(R)$, or equivalently $\det(A) \sim \prod_{i=1}^n m_i \in R^*$, which holds if and only if $m_n \in R^*$. More generally, the **annihilator** $\operatorname{ann}_R(S/U) := \{a \in R; aS \subseteq U\} \trianglelefteq R$ of S/U is given as $\operatorname{ann}_R(S/U) = (m_n)$, so that m_n is also called the **exponent** of S/U.

Moreover, we let $\operatorname{disc}(U) := \operatorname{disc}(\mathcal{C}) \in (R \setminus \{0\})/(R^*)^2$, where the latter is a quotient of commutative monoids, being called the **discriminant** of U; in particular $\operatorname{disc}_K(L) := \operatorname{disc}(S)$ is also called the **discriminant** of L over K.

(3.7) Algebraic integers. The most important case of the above construction is as follows: The integers $\mathbb{Z}$ are factorial and hence are integrally closed. Thus letting K be an **algebraic number field**, that is a finite extension of $\mathbb{Q}$ of degree $n := [K\colon \mathbb{Q}]$, we let $\mathcal{O} = \mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, being called the **ring of (algebraic) integers** of K (where we typically omit to say that this refers to integrality over $\mathbb{Z}$).

Then $\mathcal{O}$ is an integrally closed domain such that $\mathcal{O} \cap \mathbb{Q} = \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Moreover, $\mathcal{O}$ is a free $\mathbb{Z}$-module, that is a free Abelian group, of rank n; thus let $\mathcal{B} \subseteq \mathcal{O}$ be a $\mathbb{Z}$-basis, that is an integral basis of K (over $\mathbb{Q}$). Then, since $(\mathbb{Z}^*)^2 = \{1\}$, the discriminant $\operatorname{disc}(K) = \operatorname{disc}(\mathcal{O}) := \operatorname{disc}(\mathcal{B}) \in \mathbb{Z} \setminus \{0\}$ is uniquely defined.

Example. Letting $K := \mathbb{Q}(i)$, we show that $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, saying that the Gaussian integers indeed are the integers in the Gaussian number field:

Being a root of $X^2 + 1 \in \mathbb{Q}[X]$, we have $i \in \mathcal{O}$, and thus $\mathbb{Z}[i] \subseteq \mathcal{O}$. Conversely, let $z = x + yi \in \mathcal{O}$, where $x, y \in \mathbb{Q}$. Hence we have $-iz = y - xi \in \mathcal{O}$ as well. We may assume that $x, y \neq 0$. Then we have $\mu_z = (X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} = X^2 - 2xX + (x^2 + y^2)$ and $\mu_{-iz} = (X + iz)(X - i\overline{z}) = X^2 + i(z - \overline{z})X + z\overline{z} = X^2 - 2yX + (x^2 + y^2)$. Thus we have $2x, 2y \in \mathbb{Z}$ and $x^2 + y^2 \in \mathbb{Z}$. Hence we have $x = \frac{a}{2}$ and $y = \frac{b}{2}$, for some $a, b \in \mathbb{Z}$. This yields $a^2 + b^2 \equiv 0 \pmod 4$, implying that a and b are even. ♯

In particular, this implies that $\mathbb{Z}[i]$ is integrally closed, without using the fact that $\mathbb{Z}[i]$ is factorial. Moreover, $\mathcal{B} := \{1, i\}$ is an integral basis, so that we have $\operatorname{disc}(\mathbb{Q}(i)) = \operatorname{disc}(\mathbb{Z}[i]) = \operatorname{disc}(\mathcal{B}) = -4$; see (3.2).

(3.8) Composite fields. Let K and L be algebraic number fields, let $n := [K\colon \mathbb{Q}]$ and $m := [L\colon \mathbb{Q}]$, let $\mathcal{O} := \mathcal{O}_K$ and $\widetilde{\mathcal{O}} := \mathcal{O}_L$, let $\delta := \operatorname{disc}(\mathcal{O})$ and $\widetilde{\delta} := \operatorname{disc}(\widetilde{\mathcal{O}})$, let KL be the **composite field**, and let $\widehat{\mathcal{O}} := \mathcal{O}_{KL}$.

Letting $M := K \cap L$, we have a natural M-algebra epimorphism $K \otimes_M L \to KL$, hence $[KL\colon \mathbb{Q}] \leq [K\colon M] \cdot [L\colon M] \cdot [M\colon \mathbb{Q}] = \frac{n}{[M\colon \mathbb{Q}]} \cdot \frac{m}{[M\colon \mathbb{Q}]} \cdot [M\colon \mathbb{Q}] = \frac{nm}{[M\colon \mathbb{Q}]}$. Thus, if $[KL\colon \mathbb{Q}] = nm$, then we have $M = \mathbb{Q}$, so that $KL \cong K \otimes_{\mathbb{Q}} L$.

Conversely, if both K and L are Galois such that $K \cap L = \mathbb{Q}$, then KL is Galois as well, and we have $\operatorname{Aut}_{\mathbb{Q}}(KL) \cong \operatorname{Aut}_{\mathbb{Q}}(K) \times \operatorname{Aut}_{\mathbb{Q}}(L)$, so that $[KL\colon \mathbb{Q}] = mn$.

Proposition. Assume that $[KL\colon \mathbb{Q}] = nm$, and let $d \in \gcd(\delta, \widetilde{\delta})$.
i) Then we have $\mathcal{O}\widetilde{\mathcal{O}} \subseteq \widehat{\mathcal{O}} \subseteq \frac{1}{d} \cdot \mathcal{O}\widetilde{\mathcal{O}}$; in particular equality holds if $d \in \{\pm 1\}$.
ii) We have $\operatorname{disc}(\widehat{\mathcal{O}}) \mid \delta^m \widetilde{\delta}^n$, where equality holds if $d \in \{\pm 1\}$.

Proof. i) Let $\mathcal{A} := \{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{O}$ and $\mathcal{B} := \{\beta_1, \dots, \beta_m\} \subseteq \widetilde{\mathcal{O}}$ be $\mathbb{Z}$-bases. Then $\mathcal{A} \subseteq K$ and $\mathcal{B} \subseteq L$ are $\mathbb{Q}$-bases, thus $\mathcal{C} := \{\alpha_i\beta_j \in KL; i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\} \subseteq KL$ is a $\mathbb{Q}$-basis, which we assume to be ordered lexicographically. Then for any $\omega \in \widehat{\mathcal{O}}$ we have $\omega = \frac{1}{c} \cdot \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij}\alpha_i\beta_j$, where $c_{ij} \in \mathbb{Z}$ and $0 \neq c \in \mathbb{Z}$, and where we may assume that c and the c_{ij} are coprime. We show that $c \mid \delta$; then by symmetry $c \mid \widetilde{\delta}$ as well, so that $c \mid d$:

We first observe that, given embeddings $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)$ and $\tau \in \mathrm{Inj}_{\mathbb{Q}}(L)$, then there is a unique embedding of KL restricting to σ on K and to τ on L: Since $nm = [KL\colon \mathbb{Q}] = [KL\colon K] \cdot [K\colon \mathbb{Q}] = [KL\colon K] \cdot n$, we have $[KL\colon K] = m$, thus there are precisely m extensions of σ to KL. Since L generates KL, the latter are pairwise distinct on L, hence precisely one of them restricts to τ on L.

For $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)$ let $\widehat{\sigma} \in \mathrm{Inj}_{\mathbb{Q}}(KL)$ be the extension restricting to id_L. Letting $\gamma_i := \frac{1}{c} \cdot \sum_{j=1}^{m} c_{ij}\beta_j \in L$, for $i \in \{1, \dots, n\}$, we have $\omega^{\widehat{\sigma}} = \sum_{i=1}^{n} \alpha_i^{\sigma}\gamma_i \in KL$. In other words, for $\Delta_{\mathcal{B}} = [\alpha_i^{\sigma}]_{\sigma,i}$ we get $[\gamma_1, \dots, \gamma_n] \cdot \Delta_{\mathcal{B}}^{\mathrm{tr}} = [\omega^{\widehat{\sigma}}; \sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)]$.

Hence Cramer's Rule yields $\det(\Delta_{\mathcal{B}}) \cdot [\gamma_1, \dots, \gamma_n] = [\gamma_1, \dots, \gamma_n] \cdot \Delta_{\mathcal{B}}^{\mathrm{tr}} \cdot \mathrm{adj}(\Delta_{\mathcal{B}})^{\mathrm{tr}} = [\omega^{\widehat{\sigma}}; \sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)] \cdot \mathrm{adj}(\Delta_{\mathcal{B}})^{\mathrm{tr}}$, implying $\det(\Delta_{\mathcal{B}}) \cdot \gamma_i \in \widehat{\mathcal{O}}$. Since $\delta = \det(\Delta_{\mathcal{B}})^2$ this yields $\delta\gamma_i = \frac{\delta}{c} \cdot \sum_{j=1}^{m} c_{ij}\beta_j \in \widetilde{\mathcal{O}}$. Thus we have $\frac{\delta \cdot c_{ij}}{c} \in \mathbb{Z}$, for all $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$, which by coprimeness of c and the c_{ij} entails that $c \mid \delta \in \mathbb{Z}$.

ii) The elements of $\mathrm{Inj}_{\mathbb{Q}}(KL)$ are, by restriction to K and L, respectively, in natural bijection with $\mathrm{Inj}_{\mathbb{Q}}(K) \times \mathrm{Inj}_{\mathbb{Q}}(L)$. Letting $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)$ and $\tau \in \mathrm{Inj}_{\mathbb{Q}}(L)$, we have $\Delta_{\mathcal{C}} = [\alpha_i^{\sigma}\beta_j^{\tau}]_{\sigma,\tau;i,j} = [\alpha_i^{\sigma}]_{\sigma,i} \otimes [\beta_j^{\tau}]_{\tau,j} = \Delta_{\mathcal{A}} \otimes \Delta_{\mathcal{B}}$, thus $\mathrm{disc}(\mathcal{O}\widetilde{\mathcal{O}}) = \det(\Delta_{\mathcal{C}})^2 = \big(\det(\Delta_{\mathcal{A}})^m \cdot \det(\Delta_{\mathcal{B}})^n\big)^2 = \mathrm{disc}(\mathcal{O})^m \cdot \mathrm{disc}(\widetilde{\mathcal{O}})^n = \delta^m\widetilde{\delta}^n$. ♯

The condition on the greatest common divisor of the discriminants of the components of a composite field is necessary indeed, as we will see in (3.10) below.

(3.9) Computing integral bases. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, and let $\mathcal{O}$ be its ring of integers. We proceed towards a method to compute $\mathcal{O}$ explicitly:

Starting with a $\mathbb{Z}$-submodule $\mathcal{U} \subseteq \mathcal{O}$ of rank n, we try to enlarge $\mathcal{U}$ step by step, in order to approximate $\mathcal{O}$ better, and where we want to be able to conclude that if this is no longer possible, then we have actually reached $\mathcal{U} = \mathcal{O}$. To start with, for example, we may take a primitive element $\alpha \in K$, which we may assume to be contained in $\mathcal{O}$; then since the minimum polynomial $\mu_\alpha \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ has degree n, the subring $\mathbb{Z}[\alpha] = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle_{\mathbb{Z}} \subseteq \mathcal{O}$ is $\mathbb{Z}$-free of rank n.

Proposition. i) We have $\mathrm{disc}(\mathcal{U}) = [\mathcal{O}\colon \mathcal{U}]^2 \cdot \mathrm{disc}(\mathcal{O})$.

In particular, if $\mathrm{disc}(\mathcal{U})$ is square-free, then we have $\mathcal{U} = \mathcal{O}$. (The converse does not hold, as the example of the Gaussian integers shows.)

ii) If $\mathcal{U} \neq \mathcal{O}$, then there is $\omega \in \mathcal{O} \setminus \mathcal{U}$ such that $p\omega \in \mathcal{U}$, for some prime $p \in \mathbb{Z}$ such that $p^2 \mid \mathrm{disc}(\mathcal{U})$; letting $\widehat{\mathcal{U}} := \mathcal{U} + \langle \omega \rangle_{\mathbb{Z}} \subseteq \mathcal{O}$ we have $\mathrm{disc}(\mathcal{U}) = p^2 \cdot \mathrm{disc}(\widehat{\mathcal{U}})$.

Hence, letting $\mathcal{C} = \{\omega_1, \ldots, \omega_n\} \subseteq \mathcal{U}$ be a $\mathbb{Z}$-basis, we may assume that $\omega = \frac{1}{p} \cdot \sum_{i=1}^{n} a_i \omega_i$, for suitable integers $a_i \in \{0, \ldots, p-1\}$.

Proof. i) We may assume that $\mathcal{B} \subseteq \mathcal{O}$ is a $\mathbb{Z}$-basis such that $\mathcal{C} = \mathcal{B} \cdot D$, where $D := \operatorname{diag}[m_1, \ldots, m_n] \in \mathbb{Z}^{n \times n}$, for suitable $m_i > 0$ such that $m_1 \mid m_2 \mid \cdots \mid m_n$. Hence we have $\mathcal{O}/\mathcal{U} \cong \bigoplus_{i=1}^{n} \mathbb{Z}/(m_i)$, in particular $[\mathcal{O} \colon \mathcal{U}] = \prod_{i=1}^{n} m_i$. Moreover, we get $\operatorname{disc}(\mathcal{U}) = \det(D)^2 \cdot \operatorname{disc}(\mathcal{O}) = (\prod_{i=1}^{n} m_i)^2 \cdot \operatorname{disc}(\mathcal{O})$.

ii) We have $\mathcal{U} \neq \mathcal{O}$ if and only if there is a prime $p \in \mathbb{Z}$ such that $p \mid [\mathcal{O} \colon \mathcal{U}]$; then we have $p^2 \mid [\mathcal{O} \colon \mathcal{U}]^2 \mid \operatorname{disc}(\mathcal{U})$. Hence there is $\omega \in \mathcal{O} \setminus \mathcal{U}$ such that $p\omega \in \mathcal{U}$. Thus we have $\widehat{\mathcal{U}}/\mathcal{U} \cong \mathbb{Z}/(p)$, so that we have $\operatorname{disc}(\mathcal{U}) = p^2 \cdot \operatorname{disc}(\widehat{\mathcal{U}})$. ♯

(3.10) Example: The biquadratic field $\mathbb{Q}(i, \sqrt{2})$. We consider the splitting field $K \subseteq \mathbb{C}$ of the polynomial $f := (X^2 - 2)(X^2 + 1) \in \mathbb{Q}[X]$: Letting $\alpha := \sqrt{2} \in \mathbb{R}$ we have $K = \mathbb{Q}(i, \alpha)$, which is Galois of degree $[K \colon \mathbb{Q}] = 4$.

Letting $K_1 := \mathbb{Q}(i)$ and $K_2 := \mathbb{Q}(\alpha)$ be the (quadratic) splitting fields of the irreducible factors of f, from $K = K_1 K_2$ and $K_1 \cap K_2 = \mathbb{Q}$ we infer that $\operatorname{Aut}_{\mathbb{Q}}(K) \cong V_4$, being given by $\alpha \mapsto \pm\alpha$ and $i \mapsto \pm i$. Hence let $K_3 := \mathbb{Q}(i\alpha)$ be the (quadratic) splitting field of $X^2 + 2 \in \mathbb{Q}[X]$, being the third strictly intermediate field between $\mathbb{Q}$ and K.

i) We first determine the rings of integers of the proper subfields: We have $\mathcal{O}_{K_1} = \mathbb{Z}[i]$, where $\operatorname{disc}(\mathbb{Z}[i]) = -4$. We show that $\mathcal{O}_{K_2} = \mathbb{Z}[\alpha]$ and $\mathcal{O}_{K_3} = \mathbb{Z}[i\alpha]$:

We have $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{K_2}$, where $\operatorname{disc}(\mathbb{Z}[\alpha]) = \det(\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}) = \det(\begin{bmatrix} 1 & \alpha \\ 1 & -\alpha \end{bmatrix})^2 = 8$. Hence we have to check the elements $\frac{1}{2}(a + b\alpha) \in K_2$, where $a, b \in \{0, 1\}$, for integrality. Since we may assume that $b \neq 0$, we only have to consider $\frac{\alpha}{2}$ and $\frac{1+\alpha}{2}$. We have $N_{K_2/\mathbb{Q}}(\frac{\alpha}{2}) = \frac{\alpha}{2} \cdot \frac{-\alpha}{2} = -\frac{1}{2}$, and $N_{K_2/\mathbb{Q}}(\frac{1+\alpha}{2}) = \frac{1+\alpha}{2} \cdot \frac{1-\alpha}{2} = -\frac{1}{4}$, entailing that neither of them is integral.

We have $\mathbb{Z}[i\alpha] \subseteq \mathcal{O}_{K_3}$, where $\operatorname{disc}(\mathbb{Z}[i\alpha]) = \det(\begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix}) = \det(\begin{bmatrix} 1 & i\alpha \\ 1 & -i\alpha \end{bmatrix})^2 = -8$. Hence we have to check the elements $\frac{1}{2}(a + bi\alpha) \in K_3$, where $a, b \in \{0, 1\}$, for integrality. Since we may assume that $b \neq 0$, we only have to consider $\frac{i\alpha}{2}$ and $\frac{1+i\alpha}{2}$. We have $N_{K_3/\mathbb{Q}}(\frac{i\alpha}{2}) = \frac{i\alpha}{2} \cdot \frac{-i\alpha}{2} = \frac{1}{2}$, and $N_{K_3/\mathbb{Q}}(\frac{1+i\alpha}{2}) = \frac{1+i\alpha}{2} \cdot \frac{1-i\alpha}{2} = \frac{3}{4}$, entailing that neither of them is integral.

ii) Letting $\mathcal{O} := \mathcal{O}_K$, by (3.8) we have $\mathcal{U} := \mathcal{O}_{K_1}\mathcal{O}_{K_2} \subseteq \mathcal{O} \subseteq \frac{1}{d} \cdot \mathcal{U}$, where $d \in \gcd(\operatorname{disc}(\mathcal{O}_{K_1}), \operatorname{disc}(\mathcal{O}_{K_2})) = \gcd(-4, 8) = \{\pm 4\}$, and $\operatorname{disc}(\mathcal{U}) = (-4)^2 \cdot 8^2 = 2^{10}$.

Hence we check the elements $\omega := \frac{1}{2}(a + b\alpha + ci + di\alpha) \in K$, where $a, b, c, d \in \{0, 1\}$, for integrality. To this end, we consider the regular representation with respect to the $\mathbb{Q}$-basis $\{1, \alpha, i, i\alpha\} \subseteq K$, for which we get

$$2 \cdot \rho(\omega) = a \cdot E_4 + b \cdot E_2 \otimes \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} + c \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes E_2 + d \cdot \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}.$$

This yields $16 \cdot N(\omega) = (a^2-2b^2-c^2+2d^2)^2+4(ac-2bd)^2$. Checking $N(\omega) \in \mathbb{Q}$ for integrality, we get the only non-zero solution $a = c = 0$ and $b = d = 1$.

Thus we have to check whether $\zeta = \zeta_8 := \frac{1}{2}(1+i)\alpha = \frac{1+i}{\alpha} \in K$ is integral: We observe that ζ is a primitive 8-th root of unity, thus is a root of $\Phi_8 := X^4+1 \in \mathbb{Q}[X]$, and hence is integral indeed. Moreover, since ζ is not contained in any of the proper subfields of K, we conclude that $K = \mathbb{Q}(\zeta)$, the 8-th **cyclotomic field**, and that $\mu_\zeta = \Phi_8$ is irreducible.

iii) Let $\mathcal{V} := \mathcal{U} + \langle\zeta\rangle_\mathbb{Z} = \langle 1, \alpha, i, \zeta\rangle_\mathbb{Z} \subseteq \mathcal{O}$. Since $\zeta^2 = i$ and $\zeta^3 = \frac{1}{2}(i-1)\alpha$, we conclude that $\mathcal{V} = \langle 1, \zeta, \zeta^2, \zeta^3\rangle_\mathbb{Z} = \mathbb{Z}[\zeta]$. We have $\operatorname{disc}(\mathcal{V}) = \frac{1}{4} \cdot \operatorname{disc}(\mathcal{U}) = 2^8$.

Hence we have to check the elements $\omega := \frac{1}{2}(a + b\zeta + c\zeta^2 + d\zeta^3) \in K$, where $a, b, c, d \in \{0, 1\}$, for integrality. To this end, we again consider the regular representation, with respect to the $\mathbb{Q}$-basis $\{1, \zeta, \zeta^2, \zeta^3\} \subseteq K$, for which we get $2 \cdot \rho(\omega) = a \cdot E_4 + b \cdot C_\zeta^2 + c \cdot C_\zeta^3 + d \cdot C_\zeta^4 \in K^{4\times 4}$, where $C_\zeta \in K^{4\times 4}$ is the companion matrix associated with Φ_8.

This yields $16 \cdot N(\omega) = (a^2+c^2)^2+(b^2+d^2)^2+4(a^2-c^2)bd+4(d^2-b^2)ac$. Checking $N(\omega) \in \mathbb{Q}$ for integrality, it turns out that there is no non-zero solution. Thus we indeed have $\mathcal{O} = \mathcal{V} = \mathbb{Z}[\zeta]$, where $\operatorname{disc}(\mathcal{O}) = \operatorname{disc}(\zeta) = 2^8$. ♯

Alternatively, we can proceed in a single step from $\mathcal{U}$, using the divisibility condition in (3.6), since $\operatorname{disc}(\mathcal{U}) = (2^5)^2$, by checking the elements $\omega := \frac{1}{2^5} \cdot (a + b\alpha + ci + di\alpha) \in K$, where $a, b, c, d \in \{0, \ldots, 2^5 - 1\}$, for integrality; or better by using the divisibility condition in (3.8), by only checking the elements $\omega := \frac{1}{4} \cdot (a + b\alpha + ci + di\alpha) \in K$, where $a, b, c, d \in \{0, \ldots, 3\}$, for integrality. Checking $N(\omega) \in \mathbb{Q}$ for integrality as above, we get the only non-zero solution $\omega = \zeta$. Hence we conclude directly that $\mathcal{O} = \mathcal{V}$. Finally, $[\mathcal{O} \colon \mathcal{U}] = 2$ shows that the greatest common divisor condition in (3.8) is necessary.

4 Dedekind domains

(4.1) Noetherian rings. Let R be a commutative ring. Then R is called **Noetherian** if it fulfills the **ascending chain condition**, saying that all ascending chains of (proper) ideals eventually stabilize; or equivalently if any ideal of R is finitely generated (that is as an R-module).

Proposition. Any non-empty set of ideals of R has a maximal element, with respect to set-theoretic inclusion. In particular, given a proper ideal $I \lhd R$, then there is a maximal ideal $J \lhd R$ such that $I \subseteq J$.

Proof. Let $\mathcal{I} \neq \emptyset$ be a non-empty set of ideals of R. Since any chain of ideals of R eventually stabilizes, any ascending chain in $\mathcal{I}$ has an upper bound. Hence by Zorn's Lemma $\mathcal{I}$ has a maximal element. (As far as we see, using **Zorn's Lemma**, or equivalently using the **Axiom if Choice**, cannot be replaced here by an argument using induction only.) For the second statement, consider the set $\mathcal{I}$ of proper ideals of R containing I, then $I \in \mathcal{I}$ implies that $\mathcal{I} \neq \emptyset$. ♯

Proposition. Any non-zero non-unit of R can be written (not necessarily uniquely) as a (finite) product of irreducible elements.

Proof. Consider the set $\mathcal{I}$ of ideals $\{0\} \neq (a) \lhd R$ such that a is not a product of irreducible elements, and assume that $\mathcal{I} \neq \emptyset$. Then there is a maximal element $(a) \in \mathcal{I}$. Since $a \in R \setminus R^*$ is reducible, there are $b, c \in R \setminus R^*$ such that $a = bc$. Hence we have $(a) \subset (b)$ and $(a) \subset (c)$. Thus by maximality of (a), both b and c are a product of irreducible elements, thus so is a, a contradiction. ♯

(4.2) Fractional ideals. Let R be an integral domain, and let $K := \mathrm{Q}(R)$. An R-submodule $\{0\} \neq \mathfrak{f} \subseteq K$ such that $r\mathfrak{f} \subseteq R$ for some $0 \neq r \in R$ is called a **fractional ideal**; note that $r\mathfrak{f} \trianglelefteq R$ is an ideal. In particular, (genuine) ideals of R are fractional ideals.

If R is Noetherian, then any fractional ideal, being isomorphic to an ideal of R as R-modules, is a finitely generated R-module; conversely, if $\{0\} \neq \mathfrak{f} \subseteq K$ is a finitely generated R-module, then considering a finite R-generating set of $\mathfrak{f}$ shows that there is $0 \neq r \in R$ such that $r\mathfrak{f} \subseteq R$, thus $\mathfrak{f}$ is a fractional ideal.

In any case, the set $\mathcal{F}$ of all fractional ideals in K is a commutative monoid with respect to ideal multiplication, having neutral element R: Indeed, if $\mathfrak{f}, \mathfrak{g} \subseteq K$ are fractional ideals, such that $r\mathfrak{f} \subseteq R$ and $s\mathfrak{g} \subseteq R$ where $0 \neq r, s \in R$, then we have $rs \cdot \mathfrak{fg} \subseteq R$, so that $\{0\} \neq \mathfrak{fg}$ is a fractional ideal as well.

The question arises how the units in $\mathcal{F}$ look like: To this end, let $\mathfrak{f}^{-1} := \{x \in K; x\mathfrak{f} \subseteq R\} \subseteq K$ be the **(ideal-theoretic) inverse** of $\mathfrak{f} \in \mathcal{F}$, which indeed is a fractional ideal again: From $r\mathfrak{f} \subseteq R$ we conclude that $r \in \mathfrak{f}^{-1}$, so that $\mathfrak{f}^{-1} \neq \{0\}$; moreover, $\mathfrak{f}^{-1} \subseteq K$ is an R-submodule; and for any $0 \neq x \in \mathfrak{f}$ we have $x\mathfrak{f}^{-1} \subseteq R$.

Then for fractional ideals $\mathfrak{f} \subseteq \mathfrak{g}$ we have $\mathfrak{g}^{-1} \subseteq \mathfrak{f}^{-1}$, where $R^{-1} = R$; in particular, if $\mathfrak{f} \trianglelefteq R$ is an ideal then $R \subseteq \mathfrak{f}^{-1}$.

By definition we have $\mathfrak{f}\mathfrak{f}^{-1} \subseteq R$, where $\mathfrak{f}$ is called **invertible** if $\mathfrak{f}\mathfrak{f}^{-1} = R$; in this case $\mathfrak{f}$ is a unit in $\mathcal{F}$. Conversely, if $\mathfrak{g} \in \mathcal{F}$ such that $\mathfrak{fg} = R$, then we have $\mathfrak{g} \subseteq \mathfrak{f}^{-1}$, and thus $R = \mathfrak{fg} \subseteq \mathfrak{f}\mathfrak{f}^{-1} \subseteq R$ shows that $\mathfrak{f}$ is invertible, such that $\mathfrak{f}^{-1} = \mathfrak{f}^{-1}\mathfrak{fg} = \mathfrak{g}$. In conclusion, the group of units of $\mathcal{F}$ consists precisely of the invertible fractional ideals, inverses being given by ideal-theoretic inverses.

Example: Principal ideal domains. Let R be a principal ideal domain. Then for a fractional ideal $\mathfrak{f}$ such that $r\mathfrak{f} \subseteq R$ where $0 \neq r \in R$, we have $r\mathfrak{f} = (s) \trianglelefteq R$, for some $0 \neq s \in R$, thus $\mathfrak{f} = \frac{s}{r} \cdot R$. Conversely, all subsets of K of the latter form are fractional ideals. Thus we have $\mathcal{F} = \{\frac{s}{r} \cdot R \subseteq K; 0 \neq r, s \in R\}$; hence all fractional ideals are **principal**, that is R-free of rank 1. Moreover, since $(\frac{s}{r} \cdot R)(\frac{r}{s} \cdot R) = R$, where $0 \neq r, s \in R$, we conclude that all fractional ideals are invertible, with inverses given as $(\frac{s}{r} \cdot R)^{-1} = \frac{r}{s} \cdot R$. ♯

(4.3) Dedekind domains. A Noetherian integrally closed integral domain, whose non-zero prime ideals are maximal, is called a **Dedekind domain**. (In

terms of commutative algebra, the latter condition says that the domain in question has Krull dimension ≤ 1.)

Example: Principal ideal domains. Let R be a principal ideal domain; in particular R might be a field. Then R is a Dedekind domain:

All ideals being finitely generated, R is Noetherian; R is factorial and thus integrally closed; and an ideal $\{0\} \neq (a) \lhd R$ is maximal if and only if $a \in R$ is irreducible, which R being factorial is equivalent to $a \in R$ being a prime, which holds if and only if $\{0\} \leq (a) \lhd R$ is a prime ideal. ♯

Theorem. Let K be an algebraic number field. Then its ring of integers $\mathcal{O}$ is a Dedekind domain. (Actually, $\mathcal{O}$ is not necessarily a principal ideal domain.)

Proof. The domain $\mathcal{O}$ is integrally closed by construction; and any ideal of $\mathcal{O}$ even is a finitely generated $\mathbb{Z}$-module, hence $\mathcal{O}$ is Noetherian.

Hence let $\{0\} \neq \mathfrak{p} \lhd \mathcal{O}$ be a prime ideal. Since both $\mathcal{O}$ and $\mathfrak{p}$ are free $\mathbb{Z}$-modules of rank n, the quotient $\mathcal{O}/\mathfrak{p}$ is finite. Since $\mathcal{O}/\mathfrak{p}$ is an integral domain, we conclude that it is a (finite) field, thus $\mathfrak{p} \trianglelefteq \mathcal{O}$ is maximal. ♯

(4.4) Theorem: Factorization of ideals. Let R be a Dedekind domain, and let $\{0\} \neq \mathfrak{a} \trianglelefteq R$. Then there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \lhd R$, for some $k \in \mathbb{N}_0$, unique up to order, such that $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i$, the empty product being $(1) = R$.

Proof. We proceed in a series of steps, where we may assume that $\mathfrak{a} \neq R$:

i) There are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \lhd R$, for $k \in \mathbb{N}$, such that $\{0\} \neq \prod_{i=1}^{k} \mathfrak{p}_i \subseteq \mathfrak{a}$:

Assume that the assertion does not hold for $\mathfrak{a}$, where we may assume that $\mathfrak{a}$ is maximal with this property. Moreover, $\mathfrak{a}$ is not a prime ideal, that is there are $b, c \in R \setminus \mathfrak{a}$ such that $bc \in \mathfrak{a}$. Let $\mathfrak{b} := \mathfrak{a} + (b)$ and $\mathfrak{c} := \mathfrak{a} + (c)$, then we have $\mathfrak{bc} \subseteq \mathfrak{a}$, as well as $\mathfrak{a} \subset \mathfrak{b} \lhd R$ and $\mathfrak{a} \subset \mathfrak{c} \lhd R$. Hence both $\mathfrak{b}$ and $\mathfrak{c}$ contain a non-zero product of prime ideals, thus so does $\mathfrak{a}$, a contradiction. ♯

ii) We have $R \subset \mathfrak{a}^{-1}$: Let $\mathfrak{a} \subseteq \mathfrak{p} \lhd R$ be a maximal ideal. Since $R \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, it suffices to provide an element in $\mathfrak{p}^{-1} \setminus R$:

Let $0 \neq a \in \mathfrak{p}$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \lhd R$ be prime ideals such that $\{0\} \neq \prod_{i=1}^{k} \mathfrak{p}_i \subseteq (a) \subseteq \mathfrak{p} \lhd R$, where $k \in \mathbb{N}$ is chosen minimal. Since $\mathfrak{p}$ is a prime ideal, we may assume that $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Since non-zero prime ideals are maximal, we have $\mathfrak{p}_1 = \mathfrak{p}$. By the minimality of k we have $\mathfrak{b} := \prod_{i=2}^{k} \mathfrak{p}_i \not\subseteq (a)$. Letting $b \in \mathfrak{b} \setminus (a)$, we have $b\mathfrak{p} \subseteq \mathfrak{bp} \subseteq (a)$, thus $\frac{b}{a} \cdot \mathfrak{p} \subseteq R$, hence $\frac{b}{a} \in \mathfrak{p}^{-1}$; and $b \notin (a)$ says that $\frac{b}{a} \notin R$. ♯

iii) Let $x \in K := \mathrm{Q}(R)$. Then we have $x\mathfrak{a} \subseteq \mathfrak{a}$ if and only if $x \in R$:

We may assume that $x\mathfrak{a} \subseteq \mathfrak{a}$. Since R is Noetherian, we have $\mathfrak{a} = (a_1, \ldots, a_l) \lhd R$ for some $0 \neq a_i \in R$ and $l \in \mathbb{N}$. Then there are $b_{ij} \in R$ such that $a_j x =$

$\sum_{i=1}^{l} a_i b_{ij}$, for $j \in \{1, \dots, l\}$. Let $B := XE_l - [b_{ij}] \in R[X]^{l \times l}$ be the characteristic matrix associated with $[b_{ij}] \in R^{l \times l}$. Thus $\det(B) \in R[X]$ is monic of degree $l \geq 1$. Moreover, we have $[a_1, \dots, a_l] \cdot B(x) = 0 \in K^l$, where $[a_1, \dots, a_l] \neq 0 \in K^l$, implying that $\det(B)(x) = \det(B(x)) = 0$. Thus x is integral over R, since R is integrally closed entailing that $x \in R$. ♯

iv) Let $\{0\} \neq \mathfrak{p} \lhd R$ be a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then we have $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subseteq R$; and in particular we have $\mathfrak{p}\mathfrak{p}^{-1} = R$:

We have $R \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, entailing $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq R$. Assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, then by ii) and iii) we have $R \subset \mathfrak{p}^{-1} \subseteq R$, a contradiction; hence $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$. For $\mathfrak{a} = \mathfrak{p}$ we get $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$, which by maximality of $\mathfrak{p}$ implies $\mathfrak{p}\mathfrak{p}^{-1} = R$. ♯

v) There are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k$, for some $k \in \mathbb{N}$, such that $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i$:

Assume that the assertion does not hold for $\mathfrak{a}$, where we may assume that $\mathfrak{a}$ is maximal with this property. Letting $\mathfrak{a} \subseteq \mathfrak{p} \lhd R$ be maximal, we have $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subseteq R$, thus there are prime ideals $\mathfrak{p}_2, \dots, \mathfrak{p}_k \lhd R$, for some $k \in \mathbb{N}$, such that $\mathfrak{a}\mathfrak{p}^{-1} = \prod_{i=2}^{k} \mathfrak{p}_i$. Hence we have $\mathfrak{a} = \mathfrak{a} \cdot \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{a}\mathfrak{p}^{-1} \cdot \mathfrak{p} = \mathfrak{p} \cdot \prod_{i=2}^{k} \mathfrak{p}_i$. ♯

vi) Allowing for $\mathfrak{a} = R$ as well, let $\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i = \prod_{j=1}^{l} \mathfrak{q}_j$, where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals, and $k, l \in \mathbb{N}_0$. Then $[\mathfrak{p}_1, \dots, \mathfrak{p}_k] = [\mathfrak{q}_1, \dots, \mathfrak{q}_l]$ up to reordering:

Assuming $k \leq l$, we proceed by induction on $k \in \mathbb{N}_0$; the case $k = 0$ being clear, let $k \geq 1$. Since $\prod_{j=1}^{l} \mathfrak{q}_j = \mathfrak{a} \subseteq \mathfrak{p}_k$, and $\mathfrak{p}_k \lhd R$ is prime, we may assume that $\mathfrak{q}_l \subseteq \mathfrak{p}_k$. Since $\mathfrak{q}_l \lhd R$ is maximal, we get $\mathfrak{q}_l = \mathfrak{p}_k$. Multiplying with $\mathfrak{p}_k^{-1} = \mathfrak{q}_l^{-1}$ yields $\prod_{i=1}^{k-1} \mathfrak{p}_i = \prod_{j=1}^{l-1} \mathfrak{q}_j$, for which the assertion holds by induction. ♯

Corollary. We have $\mathfrak{a}\mathfrak{a}^{-1} = R$.

Proof. By factorization of ideals, and all non-zero prime ideals being invertible in $\mathcal{F}$, we conclude that $\mathfrak{a}$ is a unit of $\mathcal{F}$ as well. ♯

Theorem: Characterization of Dedekind domains. Let R be an integral domain. Then the following assertions are equivalent:
i) R is a Dedekind domain (that is integrally closed, Noetherian, $\dim(R) \leq 1$).
ii) Every non-zero ideal of R can be written as a product of prime ideals.
iii) Every non-zero ideal of R is invertible.

Proof. We have seen the implications 'i)⇒ii)' and 'i)⇒iii)' (which are the ones important here), but we are not able to prove the other implications here; at least Exercise (14.10) shows that iii) implies that R is Noetherian. ♯

Example: Principal ideal domains. Let R be a principal ideal domain. Then the non-zero prime ideals of R are in bijection with the associate classes of prime elements of R. Writing $0 \neq r = \prod_{i=1}^{k} p_i$, for primes $p_i \in R$ and $k \in \mathbb{N}_0$,

$\{0\} \neq (r) = \prod_{i=1}^{k}(p_i) \trianglelefteq R$. Thus in this case factorization of ideals of R is equivalent to prime factorization of elements of R. Moreover, recalling that all fractional ideals are principal, and writing $\{0\} \neq (s) = \prod_{j=1}^{l}(q_j) \trianglelefteq R$, for primes $q_j \in R$ and $l \in \mathbb{N}_0$, we get $\frac{r}{s} \cdot R = (r)(s)^{-1} = \prod_{i=1}^{k}(p_i) \cdot \prod_{j=1}^{l}(q_j)^{-1} \in \mathcal{F}$. ♯

(4.5) Divisibility of ideals. We generalize divisibility of elements to ideals:

a) Let R be an integral domain. For ideals $\mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq R$ we also write $\mathfrak{b} \mid \mathfrak{a}$, and $\mathfrak{b}$ is said to be a **divisor** of $\mathfrak{a}$. In particular, an ideal $\mathfrak{p} \triangleleft R$ is prime, if whenever $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ are ideals such that $\mathfrak{p} \mid \mathfrak{ab}$, then we have $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.

For ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ we let $\gcd(\mathfrak{a}, \mathfrak{b}) := \mathfrak{a} + \mathfrak{b} \trianglelefteq R$ be their **greatest common divisor**, and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) := \mathfrak{a} \cap \mathfrak{b} \trianglelefteq R$ be their **least common multiple**. In particular, $\mathfrak{a}$ and $\mathfrak{b}$ are called **coprime**, if $\gcd(\mathfrak{a}, \mathfrak{b}) = (1) = R$. (Note that this always works, while these notions for elements in general do not.)

For $a \in R$ we have $\mathfrak{a} \mid (a)$ if and only if $a \in \mathfrak{a}$; in this case we also write $\mathfrak{a} \mid a$. For $a, b \in R$ we have $a \mid b \in R$ if and only if $(b) \subseteq (a)$, that is $(a) \mid (b) \subseteq R$.

b) Let R be a Dedekind domain. Then all non-zero ideals of R are invertible, which entails that divisibility of ideals has the same formal property as divisibility of elements: For ideals $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ we have $\mathfrak{b} \mid \mathfrak{a}$, that is $\mathfrak{a} \subseteq \mathfrak{b}$, if and only if there is $\mathfrak{c} \trianglelefteq R$ such that $\mathfrak{a} = \mathfrak{bc}$:

We may assume that $\{0\} \neq \mathfrak{a} \subseteq \mathfrak{b} \triangleleft R$. Then we have $\mathfrak{b}^{-1}\mathfrak{a} \subseteq \mathfrak{b}^{-1}\mathfrak{b} = R$, thus $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a} \trianglelefteq R$ is an ideal, and we have $\mathfrak{bc} = \mathfrak{b} \cdot \mathfrak{b}^{-1}\mathfrak{a} = \mathfrak{b}\mathfrak{b}^{-1} \cdot \mathfrak{a} = \mathfrak{a}$. ♯

Let $\mathcal{P}$ be the set of non-zero prime ideals of R, and let $\{0\} \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq R$ have factorizations $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\nu_\mathfrak{p}}$ and $\mathfrak{b} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\mu_\mathfrak{p}}$. Then there are only finitely many ideals of R dividing $\mathfrak{a}$. Moreover, we get $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\min\{\nu_\mathfrak{p}, \mu_\mathfrak{p}\}} \trianglelefteq R$ and $\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\max\{\nu_\mathfrak{p}, \mu_\mathfrak{p}\}} \trianglelefteq R$; where $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, that is $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) = R$, if and only if $\mathfrak{a}$ and $\mathfrak{b}$ do not have a common prime divisor, which is equivalent to $\mathfrak{a} \cap \mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{ab}$.

Proposition: Chinese Remainder Theorem. Let $\{0\} \neq \mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\nu_i} \trianglelefteq R$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise distinct prime ideals, for some $r \in \mathbb{N}_0$, and $\nu_i \geq 1$. Then we have $R/\mathfrak{a} \cong \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{\nu_i}$ as R-algebras.

Proof. We consider the natural homomorphism $\pi\colon R \to \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{\nu_i}$ of R-algebras given by $a \mapsto [a \pmod{\mathfrak{p}_i^{\nu_i}}]_i$. Since the ideals $\mathfrak{p}_i^{\nu_i}$ are pairwise coprime, we have $\ker(\pi) = \bigcap_{i=1}^{r} \mathfrak{p}_i^{\nu_i} = \operatorname{lcm}(\mathfrak{p}_1^{\nu_1}, \ldots, \mathfrak{p}_r^{\nu_r}) = \prod_{i=1}^{r} \mathfrak{p}_i^{\nu_i} = \mathfrak{a}$, hence π induces an embedding $R/\mathfrak{a} \to \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{\nu_i}$. We show that π is an epimorphism:

Let $\mathfrak{a}_i := \prod_{j \neq i} \mathfrak{p}_j^{\nu_j} \trianglelefteq R$. Then $\mathfrak{a}_i$ and $\mathfrak{p}_i^{\nu_i}$ are coprime, hence there are $\alpha_i \in \mathfrak{a}_i$ and $\beta_i \in \mathfrak{p}_i^{\nu_i}$ such that $1 = \alpha_i + \beta_i$. Then we have $\alpha_i \equiv 1 \pmod{\mathfrak{p}_i^{\nu_i}}$, and $\alpha_i \equiv 0 \pmod{\mathfrak{p}_j^{\nu_j}}$ for all $j \neq i$. Now, given any element $[a_i + \mathfrak{p}_i^{\nu_i}]_i \in \bigoplus_{i=1}^{r} R/\mathfrak{p}_i^{\nu_i}$, where $a_i \in R$, we indeed have $\pi(\sum_{j=1}^{r} a_j \alpha_j) = [\sum_{j=1}^{r} a_j(\alpha_j + \mathfrak{p}_i^{\nu_i})]_i = [a_i + \mathfrak{p}_i^{\nu_i}]_i$. ♯

(4.6) Theorem: Generation of ideals. Let R be a Dedekind domain, let $\{0\} \neq \mathfrak{a} \trianglelefteq R$, and let $0 \neq \alpha \in \mathfrak{a}$. Then there is $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = (\alpha, \beta)$.

Proof. We observe that $\mathfrak{a} = (\alpha, \beta) = (\alpha) + (\beta)$ is equivalent to $\alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} = R$. Hence letting $\mathfrak{b} := \alpha\mathfrak{a}^{-1} \trianglelefteq R$ it suffices to prove the following:

If $\{0\} \neq \mathfrak{b} \trianglelefteq R$ is any ideal, then there is $\beta \in \mathfrak{a}$ such that $\beta\mathfrak{a}^{-1} + \mathfrak{b} = R$:

We may assume that $\mathfrak{b} \neq R$. Then, if β is as desired, we have $\{0\} \neq \beta\mathfrak{a}^{-1} \trianglelefteq R$. Hence we have to choose β such that $\beta\mathfrak{a}^{-1}$ is coprime to $\mathfrak{b}$. Writing $\mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{\nu_i}$, where the $\mathfrak{p}_i \triangleleft R$ are pairwise distinct prime ideals, $\nu_i \geq 1$ and $k \geq 1$, this is the case if and only if $\mathfrak{p}_i \nmid \beta\mathfrak{a}^{-1}$, that is $\mathfrak{a}\mathfrak{p}_i \nmid \beta$, for all i.

For $i \in \{1, \ldots, k\}$ let $\mathfrak{a}_i := \mathfrak{a} \cdot \prod_{j \neq i} \mathfrak{p}_j \subseteq \mathfrak{a} \trianglelefteq R$, let $\beta_i \in \mathfrak{a}_i \setminus \mathfrak{a}_i\mathfrak{p}_i \neq \emptyset$, and let $\beta = \sum_{i=1}^{k} \beta_i \in \mathfrak{a}$. We show that β is as desired: Assume to the contrary that $\mathfrak{a}\mathfrak{p}_i \mid \beta$ for some i. Then since $\mathfrak{a}\mathfrak{p}_i \mid \mathfrak{a}_j \mid \beta_j$ for all $j \neq i$, we infer that $\mathfrak{a}\mathfrak{p}_i \mid \beta_i$ as well. Thus, since we also have $\mathfrak{a}_i \mid \beta_i$, we conclude that $\mathfrak{a}_i\mathfrak{p}_i = \mathfrak{a} \cdot \prod_{j=1}^{k} \mathfrak{p}_j = \mathfrak{a} \cdot \operatorname{lcm}(\prod_{j \neq i} \mathfrak{p}_j, \mathfrak{p}_i) = \operatorname{lcm}(\mathfrak{a}_i, \mathfrak{a}\mathfrak{p}_i) \mid \beta_i$, a contradiction. ♯

(4.7) Theorem: Factoriality. Let R be a Dedekind domain. Then R is factorial if and only if it is a principal ideal domain.

Proof. It is well-known that any principal ideal domain is factorial; alternatively, this also follows from of factorization of ideals. Hence we may assume that R is not a R is not a principal ideal domain.

Thus, by factorization of ideals, there is a non-principal prime ideal $\{0\} \neq \mathfrak{p} \triangleleft R$. Let $\mathcal{I}$ be the set of ideals $\{0\} \neq \mathfrak{a} \trianglelefteq R$ such that $\mathfrak{a}\mathfrak{p}$ is principal; hence by the choice of $\mathfrak{p}$ we have $R \notin \mathcal{I}$. Then we have $\mathcal{I} \neq \emptyset$: Letting $0 \neq \omega \in \mathfrak{p}$, for $\mathfrak{a} := \omega\mathfrak{p}^{-1} \trianglelefteq R$ we get $\mathfrak{a}\mathfrak{p} = (\omega)$. Hence let $\mathfrak{a} \in \mathcal{I}$ be maximal. Letting $\mathfrak{a}\mathfrak{p} = (\omega) \triangleleft R$, where $0 \neq \omega \in R \setminus R^*$, we show that ω is irreducible but not a prime, entailing that R is not factorial:

Firstly, let $\omega = \beta\gamma \in R$, for some $\beta, \gamma \in R$. Since $\mathfrak{a}\mathfrak{p} = (\beta)(\gamma)$ we may assume that $\mathfrak{p} \mid \beta$, that is $(\beta) = \mathfrak{b}\mathfrak{p}$, for some $\{0\} \neq \mathfrak{b} \trianglelefteq R$. Hence we have $\mathfrak{b}\mathfrak{p} \mid \mathfrak{a}\mathfrak{p}$, thus multiplying with $\mathfrak{p}^{-1}$ yields $\mathfrak{b} \mid \mathfrak{a}$. By the maximality of $\mathfrak{a}$ we get $\mathfrak{b} = \mathfrak{a}$, thus $(\beta) = \mathfrak{b}\mathfrak{p} = \mathfrak{a}\mathfrak{p} = (\omega)$, so that $\omega \sim \beta$, entailing that $\gamma \in R^*$.

Secondly, by factorization of ideals we have $\mathfrak{a} \setminus \mathfrak{a}\mathfrak{p} \neq \emptyset$ and $\mathfrak{p} \setminus \mathfrak{a}\mathfrak{p} \neq \emptyset$; hence let $\alpha \in \mathfrak{a} \setminus (\omega)$ and $\delta \in \mathfrak{p} \setminus (\omega)$. Then we have $\alpha\delta \in \mathfrak{a}\mathfrak{p} = (\omega)$. In other words, $\omega \mid \alpha\delta$, but $\omega \nmid \alpha$ and $\omega \nmid \delta$, saying that ω is not a prime. ♯

(4.8) Class groups. a) Let R be a Dedekind domain, and let $K := \mathrm{Q}(R)$. Then all non-zero ideals of R are invertible, and we have factorization of ideals. This directly leads to the following:

Theorem. The set $\mathcal{F} = \mathcal{F}_K$ of fractional ideals in K forms an Abelian group, also called the **group of (fractional) ideals**, which is freely generated by the set $\mathcal{P}_K$ of non-zero prime ideals of R.

In other words, any $\mathfrak{f} \in \mathcal{F}$ can be written uniquely as $\mathfrak{f} = \prod_{\mathfrak{p} \in \mathcal{P}_K} \mathfrak{p}^{\nu_\mathfrak{p}}$, where $\nu_\mathfrak{p} \in \mathbb{Z}$, such that $\nu_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$.

Proof. Let $\mathfrak{f} \in \mathcal{F}$ be a fractional ideal, and let $0 \neq r \in R$ such that $\mathfrak{a} := r\mathfrak{f} \trianglelefteq R$, thus $\mathfrak{f} = \frac{1}{r}\mathfrak{a}$. Hence $\mathfrak{f} \cdot r\mathfrak{a}^{-1} = \frac{1}{r}\mathfrak{a} \cdot r\mathfrak{a}^{-1} = R$ shows that $\mathfrak{f}$ is invertible.

We show that $\mathcal{F}$ is generated by the non-zero prime ideals: Letting $\mathfrak{f}$ be as above, let $\mathfrak{a} = \prod_{i=1}^k \mathfrak{p}_i$ and $(r) = \prod_{j=1}^l \mathfrak{q}_j$, for prime ideals $\{0\} \neq \mathfrak{p}_i, \mathfrak{q}_j \lhd R$ and $k, l \in \mathbb{N}_0$. Then $\frac{1}{r} \cdot R = (r)^{-1} \in \mathcal{F}$ yields $\mathfrak{f} = \frac{1}{r}\mathfrak{a} = \mathfrak{a}(r)^{-1} = \prod_{i=1}^k \mathfrak{p}_i \cdot (\prod_{j=1}^l \mathfrak{q}_j)^{-1}$.

In order to prove freeness, we show that the non-zero prime ideals are independent in $\mathcal{F}$: Let $\{0\} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_k, \mathfrak{q}_1, \ldots, \mathfrak{q}_l \lhd R$ be pairwise distinct prime ideals, for some $k, l \in \mathbb{N}_0$, and let $\nu_i, \mu_j > 0$ such that $\prod_{i=1}^k \mathfrak{p}_i^{\nu_i} \cdot \prod_{j=1}^l \mathfrak{q}_j^{-\mu_j} = R \in \mathcal{F}$. This yields $\prod_{i=1}^k \mathfrak{p}_i^{\nu_i} = \prod_{j=1}^l \mathfrak{q}_j^{\mu_j} \trianglelefteq R$, which entails $k = l = 0$. ♯

b) The principal fractional ideals $\frac{s}{r} \cdot R = (s)(r)^{-1}$, where $0 \neq s, r \in R$ form a subgroup $\mathcal{H}_K \leq \mathcal{F}_K$, being called the **group of principal (fractional) ideals**: We have $R = (1) \in \mathcal{H}_K$, and for $0 \neq s', r' \in R$ we have $(s)(r)^{-1} \cdot ((s')(r')^{-1})^{-1} = (s)(r)^{-1} \cdot (r')(s')^{-1} = (sr')(rs')^{-1} \in \mathcal{H}_K$.

The quotient group $\mathrm{Cl}_K := \mathcal{F}_K / \mathcal{H}_K$, consisting of the classes of fractional ideals modulo principal fractional ideals, is called the **(fractional ideal) class group** of K, or **Picard group** of R; its order $h_K := |\mathrm{Cl}_K| \in \mathbb{N} \,\dot\cup\, \{\infty\}$ is called the **class number** of K. We get the exact sequence of group homomorphisms

$$\{1\} \to R^* \to K^* \to \mathcal{F}_K \to \mathrm{Cl}_K \to \{1\},$$

where the first map is the natural embedding, the second map is given by $\frac{s}{r} \mapsto (s)(r^{-1})$, whose image is $\mathcal{H}_K$, and the third map is the natural epimorphism.

Since for any fractional ideal $\mathfrak{f} \in \mathcal{F}_K$ we have $\mathfrak{f} = \frac{1}{r}\mathfrak{a}$, for some $0 \neq r \in R$ and $\{0\} \neq \mathfrak{a} \trianglelefteq R$, any element of Cl_K is represented by an ideal of R, where ideals $\{0\} \neq \mathfrak{a}, \mathfrak{b} \trianglelefteq R$ are equivalent in Cl_K if and only if there are $0 \neq r, s \in R$ such that $r\mathfrak{a} = (r)\mathfrak{a} = (s)\mathfrak{b} = s\mathfrak{b} \trianglelefteq R$.

Example: Trivial class groups. We have $h_K = 1$, that is $\mathrm{Cl}_K = \{1\}$, if and only if $\mathcal{F}_K = \mathcal{H}_K$, that is all fractional ideals are principal. Hence the above exact sequence collapses to $\{1\} \to R^* \to K^* \to \mathcal{F}_K \to \{1\}$.

In this case, in particular all ideals of R are principal; conversely, we have already seen that if R is a principal ideal domain then all fractional ideals are principal. Thus we have $h_K = 1$ if and only if R is a principal ideal domain (which holds if and only if R is factorial). For example, for $K = \mathbb{Q}$ and $R = \mathbb{Z}$ the above exact sequence reads $\{1\} \to \{\pm 1\} \to \mathbb{Q}^* \to \mathcal{F}_\mathbb{Q} \to \{1\}$. ♯

In general, the class groups are not well-understood. In particular, they might be (uncountable) infinite Abelian groups. We will show in (8.3) below that the class group of an algebraic number field actually is finite. Still, the **class number problem**, which is already due to GAUSS, but as yet is open, asks for determining all algebraic number fields having trivial class group; actually, it is not even known whether there are finitely or infinitely many of them.

5 Ideals and ramification

(5.1) Factorization into irreducibles. Let K be an algebraic number field, and let $\mathcal{O}$ be its ring of integers.

Recall that for $\alpha \in \mathcal{O}$ we have $\alpha \in \mathcal{O}^*$ if and only if $N(\alpha) \in \mathbb{Z}^* = \{\pm 1\}$. Considering $|N(\alpha)| \in \mathbb{N}$, we conclude by induction that any $0 \neq \alpha \in \mathcal{O}$ has a factorization into a product of irreducible (also called indecomposable) elements; alternatively, we might just recall that $\mathcal{O}$ is Noetherian.

In particular, $\alpha \in \mathcal{O}$ is irreducible if $N(\alpha) \in \mathbb{Z}$ is irreducible, that is a prime (since $\mathbb{Z}$ is factorial). Note that the converse does not in general hold: For example, the element $3 \in \mathbb{Z}[i] \subseteq \mathbb{Q}(i)$ is a prime, that is irreducible (since $\mathbb{Z}[i]$ is factorial), but has norm $N(3) = 9$; see (1.4).

The question arises whether (or when) $\mathcal{O}$ is factorial, that is whether these factorizations are unique up to associates and order, which amounts to asking whether any irreducible element is a prime. In general this does not hold, as the following example shows.

Example: Non-unique factorization. Let $\alpha := \sqrt{-5} \in \mathbb{C}$ and $K := \mathbb{Q}(\alpha)$, so that $[K\colon \mathbb{Q}] = 2$. Then we have $\mathcal{O} = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(\mathcal{O}) = -4 \cdot 5$; see (10.1). Recall that $N(a+b\alpha) = (a+b\alpha)(a-b\alpha) = a^2+5b^2$, for $a, b \in \mathbb{Z}$, and $\mathcal{O}^* = \{\pm 1\}$.

We have $6 = 2 \cdot 3 = (1+\alpha)(1-\alpha) \in \mathcal{O}$. Moreover, since $2, 3 \notin N(\mathcal{O}) \subseteq \mathbb{N}_0$, from $N(2) = 2^2$ and $N(3) = 3^2$ and $N(1 \pm \alpha) = 2 \cdot 3$ we conclude that 2 and 3 and $1 \pm \alpha$ are all irreducible in $\mathcal{O}$. Since the latter elements are pairwise non-associate, this is an example of a non-unique factorization in $\mathcal{O}$, and none of the latter irreducible elements is a prime. In particular, $\mathcal{O}$ is not factorial. and thus is not a principal ideal domain.

Lacking non-units dividing 2 and $1 \pm \alpha$, or 3 and $1 \pm \alpha$, we look at ideals instead:

We consider $\mathfrak{p}_2 := (2, 1+\alpha) = (2, 1-\alpha) \trianglelefteq \mathcal{O}$. Since $2\alpha = -2 + (2+2\alpha)$ and $(1+\alpha)\alpha = -6 + (1+\alpha)$ we conclude that $\mathfrak{p}_2 = \langle 2, 1+\alpha\rangle_{\mathbb{Z}}$, where $[2, 1+\alpha] = [1, \alpha] \cdot \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. Since the latter matrix has Smith normal form $\operatorname{diag}[1, 2]$, we conclude that $[\mathcal{O}\colon \mathfrak{p}_2] = 2$, hence $\mathfrak{p}_2 \trianglelefteq \mathcal{O}$ is maximal. But since 2 and $1 \pm \alpha$ are coprime, $\mathfrak{p}_2$ is not principal.

We consider $\mathfrak{q}_3 := (3, 1+\alpha) \trianglelefteq \mathcal{O}$ and $\mathfrak{q}_3' := (3, 1-\alpha) \trianglelefteq \mathcal{O}$. Since $3\alpha = -3+(3+3\alpha)$ and $(1+\alpha)\alpha = -6+(1+\alpha)$ we conclude that $\mathfrak{q}_3 = \langle 3, 1+\alpha\rangle_{\mathbb{Z}}$, where $[3, 1+\alpha] =$

$[1,\alpha]\cdot\begin{bmatrix}3&1\\0&1\end{bmatrix}$. Since the latter matrix has Smith normal form diag$[1,3]$, we conclude that $[\mathcal{O}\colon \mathfrak{q}_3]=3$, hence $\mathfrak{q}_3\lhd\mathcal{O}$ is maximal. Since 3 and $1+\alpha$ are coprime, $\mathfrak{q}_3$ is not principal; by conjugation, $\mathfrak{q}_3'\lhd\mathcal{O}$ is maximal, but not principal.

Indeed, we get $\mathfrak{p}_2^2=(4,2+2\alpha,-4+2\alpha)=(2)$ and $\mathfrak{q}_3\mathfrak{q}_3'=(9,3\pm3\alpha,6)=(3)$, as well as $\mathfrak{p}_2\mathfrak{q}_3=(6,2+2\alpha,3+3\alpha,-4+2\alpha)=(1+\alpha)$ and $\mathfrak{p}_2\mathfrak{q}_3'=(1-\alpha)$. Thus we have $(6)=(2)(3)=\mathfrak{p}_2^2\cdot\mathfrak{q}_3\mathfrak{q}_3'=\mathfrak{p}_2\mathfrak{q}_3\cdot\mathfrak{p}_2\mathfrak{q}_3'=(1+\alpha)(1-\alpha)\trianglelefteq\mathcal{O}$, so that the two distinct factorizations of the element 6 into irreducible elements derive from a regrouping of a single factorization of the ideal (6) into prime ideals. ♯

(5.2) Absolute norms. Let K be an algebraic number field of degree $n:=[K\colon\mathbb{Q}]$, and let $\mathcal{O}$ be its ring of integers, having discriminant $\operatorname{disc}(\mathcal{O})\in\mathbb{Z}$.

Recall that any ideal $\{0\}\neq\mathfrak{a}\trianglelefteq\mathcal{O}$ is $\mathbb{Z}$-free of rank n, and let $\operatorname{disc}(\mathfrak{a})\in\mathbb{Z}$ be its discriminant. Thus $N(\mathfrak{a})=N_K(\mathfrak{a}):=[\mathcal{O}\colon\mathfrak{a}]\in\mathbb{N}$ is finite, being called the **(absolute) norm** of $\mathfrak{a}$. Moreover, recall that we have $\operatorname{disc}(\mathfrak{a})=[\mathcal{O}\colon\mathfrak{a}]^2\cdot\operatorname{disc}(\mathcal{O})$, so that we get $N(\mathfrak{a})=\sqrt{\frac{\operatorname{disc}(\mathfrak{a})}{\operatorname{disc}(\mathcal{O})}}$.

We have $N(\mathfrak{a})=1$ if and only if $\mathfrak{a}=\mathcal{O}$; for $0\neq\alpha\in\mathfrak{a}$ we have $N(\mathfrak{a})\mid N((\alpha))$, where equality holds if and only if $\mathfrak{a}=(\alpha)$. Moreover, applying Lagrange's Theorem to the additive group $\mathcal{O}/\mathfrak{a}$ we get $N(\mathfrak{a})\cdot\mathcal{O}\subseteq\mathfrak{a}$, hence we conclude that $\mathfrak{a}\mid N(\mathfrak{a})$. In particular, by factorization of ideals we conclude that there are only finitely many ideals having (or dividing) a given norm.

Proposition. For $0\neq\alpha\in\mathcal{O}$ we have $N((\alpha))=|N_{K/\mathbb{Q}}(\alpha)|$.

Proof. Let $\mathcal{B}=\{\alpha_1,\dots,\alpha_n\}\subseteq\mathcal{O}$ be an integral basis. Then $\mathcal{C}:=\alpha\cdot\mathcal{B}$ is a $\mathbb{Z}$-basis of (α), and letting $\operatorname{Inj}_{\mathbb{Q}}(K)=\{\sigma_1,\dots,\sigma_n\}$ we get $\operatorname{disc}((\alpha))=\det(\Delta_{\mathcal{C}})^2=\det([(\alpha\alpha_j)^{\sigma_i}]_{ij})^2=\det([\alpha^{\sigma_i}\alpha_j^{\sigma_i}]_{ij})^2=(\prod_{i=1}^n\alpha^{\sigma_i})^2\cdot\det([\alpha_j^{\sigma_i}]_{ij})^2=N(\alpha)^2\cdot\det(\Delta_{\mathcal{B}})^2=N(\alpha)^2\cdot\operatorname{disc}(\mathcal{O})$, where we write $N(\alpha):=N_{K/\mathbb{Q}}(\alpha)$. ♯

Proposition. For ideals $\{0\}\neq\mathfrak{a},\mathfrak{b}\trianglelefteq\mathcal{O}$ we have $N(\mathfrak{a}\mathfrak{b})=N(\mathfrak{a})N(\mathfrak{b})$.

In particular, if $N(\mathfrak{a})\in\mathbb{Z}$ is a prime, then $\{0\}\neq\mathfrak{a}\lhd\mathcal{O}$ is a prime ideal.

Proof. By factorization of ideals it is sufficient, by induction on their length, to show that $N(\mathfrak{a}\mathfrak{p})=N(\mathfrak{a})N(\mathfrak{p})$ for all prime ideals $\{0\}\neq\mathfrak{p}\lhd\mathcal{O}$:

Considering the natural $\mathcal{O}$-module epimorphism $\mathcal{O}/\mathfrak{a}\mathfrak{p}\to\mathcal{O}/\mathfrak{a}$, having kernel $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, we get $[\mathcal{O}\colon\mathfrak{a}\mathfrak{p}]=[\mathcal{O}\colon\mathfrak{a}]\cdot[\mathfrak{a}\colon\mathfrak{a}\mathfrak{p}]$. Hence it suffices to show that $\mathfrak{a}/\mathfrak{a}\mathfrak{p}\cong\mathcal{O}/\mathfrak{p}$ as $\mathcal{O}$-modules; then we have $N(\mathfrak{a}\mathfrak{p})=[\mathcal{O}\colon\mathfrak{a}\mathfrak{p}]=[\mathcal{O}\colon\mathfrak{a}]\cdot[\mathcal{O}\colon\mathfrak{p}]=N(\mathfrak{a})N(\mathfrak{p})$:

By uniqueness of factorization of ideals we have $\mathfrak{a}\mathfrak{p}\subset\mathfrak{a}$, and there is no ideal of $\mathcal{O}$ (that is $\mathcal{O}$-module) strictly between $\mathfrak{a}\mathfrak{p}$ and $\mathfrak{a}$. Hence letting $\alpha\in\mathfrak{a}\setminus\mathfrak{a}\mathfrak{p}$ we have $\mathfrak{a}\mathfrak{p}+(\alpha)=\mathfrak{a}$. Thus the map $\mathcal{O}\to\mathfrak{a}/\mathfrak{a}\mathfrak{p}\colon\omega\mapsto\alpha\omega+\mathfrak{a}\mathfrak{p}$ is an epimorphism of $\mathcal{O}$-modules such that $\mathfrak{p}\subseteq\ker(\varphi)\lhd\mathcal{O}$. Since $\mathfrak{p}$ is maximal, we conclude that $\ker(\varphi)=\mathfrak{p}$, so that $\mathcal{O}/\mathfrak{p}\cong\mathfrak{a}/\mathfrak{a}\mathfrak{p}$. ♯

(5.3) Varying the field. Let $K \subseteq L$ be algebraic number fields, and let $\mathcal{O} := \mathcal{O}_K$ and $\widehat{\mathcal{O}} := (\mathcal{O}_K)^L = \mathcal{O}_L$ be their rings of integers; hence $\widehat{\mathcal{O}} \cap K = \mathcal{O}$.

Theorem. i) Let $\{0\} \neq \mathfrak{q} \lhd \widehat{\mathcal{O}}$ be a prime ideal. Then there is a unique prime ideal $\{0\} \neq \mathfrak{p} \lhd \mathcal{O}$ which **lies under** $\mathfrak{q}$, that is $\mathfrak{p} \subseteq \mathfrak{q}$.
ii) Let $\{0\} \neq \mathfrak{p} \lhd \mathcal{O}$ be a prime ideal. Then there is a prime ideal $(\{0\} \neq)\ \mathfrak{q} \lhd \widehat{\mathcal{O}}$ which **lies over** $\mathfrak{p}$, that is $\mathfrak{p} \subseteq \mathfrak{q}$; and there are only finitely many such ideals.

Proof. i) We consider the prime ideal $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O} \lhd \mathcal{O}$ lying under $\mathfrak{q}$. Since $0 \neq N_L(\mathfrak{q}) \in \mathfrak{q} \cap \mathbb{Z} \subseteq \mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$ we conclude that $\mathfrak{p} \neq \{0\}$. Since any non-zero prime ideal of $\mathcal{O}$ lying under $\mathfrak{q}$ necessarily contains (that is divides) $\mathfrak{p}$, the latter is the unique such ideal.

ii) Since any prime ideal of $\widehat{\mathcal{O}}$ lying over $\mathfrak{p}$ necessarily divides $\{0\} \neq \mathfrak{p}\widehat{\mathcal{O}} \trianglelefteq \widehat{\mathcal{O}}$, the latter are precisely the prime divisors of $\mathfrak{p}\widehat{\mathcal{O}}$; in particular there are only finitely many such ideals. Hence it remains to be shown that $\mathfrak{p}\widehat{\mathcal{O}} \neq \widehat{\mathcal{O}}$: Assume to the contrary that $\mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathcal{O}}$; then we get $\mathfrak{p}^{-1} \subseteq \mathfrak{p}^{-1}\widehat{\mathcal{O}} = \mathfrak{p}^{-1}\mathfrak{p}\widehat{\mathcal{O}} = \mathcal{O} \cdot \widehat{\mathcal{O}} = \widehat{\mathcal{O}}$, hence $\mathfrak{p}^{-1} \subseteq \widehat{\mathcal{O}} \cap K = \mathcal{O}$, entailing $\mathcal{O} = \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathcal{O} = \mathfrak{p}$, a contradiction. ♯

Corollary. There is a unique prime $p \in \mathcal{P}_{\mathbb{Z}}$ such that $\mathfrak{p} \mid (p) \lhd \mathcal{O}$, and we have $N(\mathfrak{p}) = p^m$ for some $m \in \{1, \ldots, n\}$, where $n := [K\colon \mathbb{Q}]$.

Proof. We have $N(\mathfrak{p}) \mid N((p)) = N(p) = p^n$. ♯

(5.4) Ramification. a) Let $K \subseteq L$ be algebraic number fields, let $\mathcal{O} := \mathcal{O}_K$ and $\widehat{\mathcal{O}} := \mathcal{O}_L$ be their rings of integers, and let $\mathfrak{p} \in \mathcal{P}_K$ be a prime ideal of $\mathcal{O}$.

Then the prime ideals in $\mathcal{P}_L$ lying over $\mathfrak{p}$ consist precisely of the (non-empty finite) set $\mathcal{P}_L(\mathfrak{p}) \subseteq \mathcal{P}_L$ of prime divisors of $\mathfrak{p}\widehat{\mathcal{O}} \lhd \widehat{\mathcal{O}}$. Letting $r := |\mathcal{P}_L(\mathfrak{p})|$, the ideal $\mathfrak{p}$ is called **non-split** in L if $r = 1$, otherwise it is called **split**; it is called **completely** or **totally split** if $r = [L\colon K]$. (The reason for this terminology will become clear in (5.6) below.)

Writing $\mathfrak{p}\widehat{\mathcal{O}} = \prod_{\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})} \mathfrak{q}^{\nu_{\mathfrak{q}}(\mathfrak{p})}$, the number $e_K(\mathfrak{q}) = e(\mathfrak{q}/\mathfrak{p}) := \nu_{\mathfrak{q}}(\mathfrak{p}) \in \mathbb{N}$ is called the **ramification index** of $\mathfrak{q}$ over $\mathfrak{p}$, or over K; for $K = \mathbb{Q}$ we write $e(\mathfrak{q}) := e_{\mathbb{Q}}(\mathfrak{q})$. The ideal $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$ is called **unramified** over K if $e_K(\mathfrak{q}) = 1$, otherwise it is called **ramified**; it is called **completely** or **totally ramified** if $e_K(\mathfrak{q}) = [L\colon K]$. Finally, the ideal $\mathfrak{p}$ is called **unramified** or **square-free** in L if all $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$ are unramified over K.

b) Letting $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$, the natural embedding $\mathcal{O} \to \widehat{\mathcal{O}}$ induces a ring homomorphism $\mathcal{O} \to \widehat{\mathcal{O}}/\mathfrak{q}$, having kernel $\mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$. Thus we get a natural embedding $F := \mathcal{O}/\mathfrak{p} \to \widehat{\mathcal{O}}/\mathfrak{q} =: E$. Since both $\mathfrak{p} \lhd \mathcal{O}$ and $\mathfrak{q} \lhd \widehat{\mathcal{O}}$ are maximal ideals, F and E are fields, called the **residue fields** associated with $\mathfrak{p}$ and $\mathfrak{q}$, respectively.

Since both $\mathcal{O}$ and $\mathfrak{p}$ are $\mathbb{Z}$-free of rank $\mathrm{rk}_{\mathbb{Z}}(\mathfrak{p}) = \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}) = [K\colon \mathbb{Q}]$, we conclude that F is a finite field. Similarly, E is a finite field, so that $F \subseteq E$ is finite; since

finite fields are perfect, $F \subseteq E$ is separable. The number $f_K(\mathfrak{q}) = f(\mathfrak{q}/\mathfrak{p}) := [E\colon F] \in \mathbb{N}$ is called the **inertial degree** of $\mathfrak{q}$ over $\mathfrak{p}$, or over K; for $K = \mathbb{Q}$ we write $f(\mathfrak{q}) := f_{\mathbb{Q}}(\mathfrak{q})$. The ideal $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$ is called **pure** over K if $f_K(\mathfrak{q}) = 1$.

In particular, there is a unique prime $p \in \mathcal{P}_\mathbb{Z}$ such that $\mathfrak{p} \in \mathcal{P}_K(p) := \mathcal{P}_K((p))$. Hence $F = \mathcal{O}/\mathfrak{p}$ has degree $f(\mathfrak{p}) = f_{\mathbb{Q}}(\mathfrak{p})$ over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, so that F is the field with $p^{f(\mathfrak{p})} = N(\mathfrak{p})$ elements.

c) We show that ramification indices and inertial degrees are multiplicative in the following sense: Let $K \subseteq M \subseteq L$ be an intermediate field, let $\mathfrak{p} \in \mathcal{P}_K$ and $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$, and let $\mathfrak{q}' := \mathfrak{q} \cap M \in \mathcal{P}_M(\mathfrak{p})$, thus $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{q}')$.

Proposition. We have $e_K(\mathfrak{q}) = e_M(\mathfrak{q})e_K(\mathfrak{q}')$ and $f_K(\mathfrak{q}) = f_M(\mathfrak{q})f_K(\mathfrak{q}')$.

Proof. Firstly, letting $\mathcal{O}' := \mathcal{O}_M$, we have $\mathfrak{p}\mathcal{O}' = \mathfrak{q}'^{e_K(\mathfrak{q}')} \cdot \mathfrak{a}'$, where $\mathfrak{a}' \trianglelefteq \mathcal{O}'$ is coprime to $\mathfrak{q}'$. Thus we get $\mathfrak{p}\widehat{\mathcal{O}} = (\mathfrak{p}\mathcal{O}')\widehat{\mathcal{O}} = (\mathfrak{q}'\widehat{\mathcal{O}})^{e_K(\mathfrak{q}')} \cdot \mathfrak{a}'\widehat{\mathcal{O}} = \mathfrak{q}^{e_M(\mathfrak{q})e_K(\mathfrak{q}')} \cdot \mathfrak{a} \cdot \mathfrak{a}'\widehat{\mathcal{O}}$ where $\mathfrak{a} \trianglelefteq \widehat{\mathcal{O}}$ is coprime to $\mathfrak{q}$. Since $\mathfrak{a}'\widehat{\mathcal{O}} \trianglelefteq \widehat{\mathcal{O}}$ is coprime to $\mathfrak{q}'\widehat{\mathcal{O}}$ anyway, and thus is coprime to $\mathfrak{q}$, we infer that $e_K(\mathfrak{q}) = e_M(\mathfrak{q})e_K(\mathfrak{q}')$.

Secondly, letting $E' := \mathcal{O}'/\mathfrak{q}'$, we have the field tower $F \subseteq E' \subseteq E$, from which we get $f_K(\mathfrak{q}) = [E\colon F] = [E\colon E'] \cdot [E'\colon F] = f_M(\mathfrak{q})f_K(\mathfrak{q}')$. ♯

(5.5) Example: Gaussian numbers. Let $K := \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$, hence $[K\colon \mathbb{Q}] = 2$, so that K is Galois; we have $\operatorname{disc}(\mathcal{O}) = -4$. Recalling that $\mathcal{O}$ is factorial, that is a principal ideal domain, for $p \in \mathcal{P}_\mathbb{Z}$ by (1.4) we have:

i) If $p = 2$, then $\mathcal{P}_K(2) = \{\mathfrak{p}\}$, where $\mathfrak{p} = (1+i)$ and $2\mathcal{O} = \mathfrak{p}^2$, that is $e(\mathfrak{p}) = 2$, so that 2 is non-split and completely ramified in K; and from $N(\mathfrak{p})^2 = N(\mathfrak{p}^2) = N(2) = 4$ we get $f(\mathfrak{p}) = 1$.

ii) If $p \equiv -1 \pmod 4$, then $\mathcal{P}_K(p) = \{\mathfrak{p}\}$, where $p\mathcal{O} = \mathfrak{p}$, that is $e(\mathfrak{p}) = 1$, so that p is non-split and unramified; and from $N(\mathfrak{p}) = N(p) = p^2$ we get $f(\mathfrak{p}) = 2$.

iii) If $p \equiv 1 \pmod 4$, then $\mathcal{P}_K(p) = \{\mathfrak{p}, \mathfrak{p}'\}$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are conjugate. We have $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, that is $e(\mathfrak{p}) = e(\mathfrak{p}') = 1$, so that p is completely split and unramified; from $N(\mathfrak{p})N(\mathfrak{p}') = N(\mathfrak{p}\mathfrak{p}') = N(p) = p^2$ we get $f(\mathfrak{p}) = f(\mathfrak{p}') = 1$.

(5.6) The fundamental equality. Let $K \subseteq L$ be algebraic number fields such that $n := [L\colon K]$, and let $\mathcal{O} := \mathcal{O}_K$ and $\widehat{\mathcal{O}} := \mathcal{O}_L$.

Theorem. Let $\mathfrak{p} \in \mathcal{P}_K$. Then we have $\sum_{\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})} e_K(\mathfrak{q})f_K(\mathfrak{q}) = n$.

Proof. Since $\mathfrak{p}\widehat{\mathcal{O}} = \prod_{\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})} \mathfrak{q}^{e_K(\mathfrak{q})} \lhd \widehat{\mathcal{O}}$, by the Chinese Remainder Theorem we have $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}} \cong \bigoplus_{\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})} \widehat{\mathcal{O}}/\mathfrak{q}^{e_K(\mathfrak{q})}$ as $\widehat{\mathcal{O}}$-algebras. In particular, $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ and $\widehat{\mathcal{O}}/\mathfrak{q}^{e_K(\mathfrak{q})}$ are $\mathcal{O}$-modules, and letting $F := \mathcal{O}/\mathfrak{p}$ they are F-vector spaces, which since $\widehat{\mathcal{O}}$ is a finitely generated $\mathbb{Z}$-module are finitely generated. We show that $\dim_F(\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}) = n$ and $\dim_F(\widehat{\mathcal{O}}/\mathfrak{q}^{e_K(\mathfrak{q})}) = e_K(\mathfrak{q})f_K(\mathfrak{q})$:

i) We first consider $\widehat{\mathcal{O}}/\mathfrak{q}^{e_K(\mathfrak{q})}$: Abbreviating $e := e_K(\mathfrak{q})$, we have the strictly ascending chain of ideals $\mathfrak{q}^e \subset \mathfrak{q}^{e-1} \subset \cdots \subset \mathfrak{q} \subset \widehat{\mathcal{O}}$. Letting $E := \widehat{\mathcal{O}}/\mathfrak{q}$, we have $[E\colon F] = f_K(\mathfrak{q})$. We consider the layers of the chain, for $k \in \{1, \ldots, e\}$:

The quotient $\mathfrak{q}^{k-1}/\mathfrak{q}^k$ is an E-vector space. Letting $\alpha_k \in \mathfrak{q}^{k-1} \setminus \mathfrak{q}^k$, we have a non-zero $\widehat{\mathcal{O}}$-module homomorphism $\widehat{\mathcal{O}} \to \mathfrak{q}^{k-1}/\mathfrak{q}^k\colon a \mapsto a\alpha_k + \mathfrak{q}^k$, having kernel $\mathfrak{q}$. Moreover, we have $(\alpha)+\mathfrak{q}^k = \mathfrak{q}^{k-1} \trianglelefteq \widehat{\mathcal{O}}$, entailing surjectivity. Thus we have an isomorphism of E-vector spaces $\widehat{\mathcal{O}}/\mathfrak{q} \to \mathfrak{q}^{k-1}/\mathfrak{q}^k$. Hence we have $\dim_F(\widehat{\mathcal{O}}/\mathfrak{q}^e) = [E\colon F] \cdot \sum_{k=1}^{e} \dim_E(\mathfrak{q}^{k-1}/\mathfrak{q}^k) = f_K(\mathfrak{q}) \cdot \sum_{k=1}^{e} \dim_E(E) = e_K(\mathfrak{q}) f_K(\mathfrak{q})$.

ii) We now consider $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$: Let $\mathcal{B} := \{\omega_1, \ldots, \omega_m\} \subseteq \widehat{\mathcal{O}}$, where $m \in \mathbb{N}$, be a lift of an F-basis of $\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$. We proceed to show that $\mathcal{B} \subseteq L$ is a K-basis:

Assume that $\mathcal{B}$ is K-linearly dependent. Since $K = \mathrm{Q}(R)$ we conclude that $\mathcal{B}$ is $\mathcal{O}$-linearly dependent, that is there are $\alpha_1, \ldots, \alpha_m \in \mathcal{O}$, not all being zero, such that $\sum_{k=1}^{m} \alpha_k \omega_k = 0 \in \widehat{\mathcal{O}}$. Let $\{0\} \neq \mathfrak{a} := (\alpha_1, \ldots, \alpha_m) \trianglelefteq \mathcal{O}$, and let $\alpha \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. Then we have $\alpha\mathfrak{a} \subseteq \mathcal{O}$, but $\alpha\mathfrak{a} \not\subseteq \mathfrak{p}$. Hence there is $k \in \{1, \ldots, m\}$ such that $\alpha\alpha_k \notin \mathfrak{p}$. Recalling that $\mathfrak{p}\widehat{\mathcal{O}} \cap \mathcal{O} = \mathfrak{p}$, this yields the non-trivial F-linear combination $\sum_{k=1}^{m} \alpha\alpha_k\omega_k \equiv 0 \pmod{\mathfrak{p}\widehat{\mathcal{O}}}$, a contradiction.

We show that $\mathcal{B}$ is a K-generating set of L: Let $\mathcal{U} := \langle \mathcal{B} \rangle_{\mathcal{O}} \subseteq \widehat{\mathcal{O}}$, then by construction we have $\mathcal{U} + \mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathcal{O}}$ as $\mathcal{O}$-modules. Hence letting $\mathcal{M} := \widehat{\mathcal{O}}/\mathcal{U}$ we have $\mathcal{M}\mathfrak{p} = (\widehat{\mathcal{O}}/\mathcal{U})\mathfrak{p} = (\mathfrak{p}\widehat{\mathcal{O}} + \mathcal{U})/\mathcal{U} = \widehat{\mathcal{O}}/\mathcal{U} = \mathcal{M}$. Thus, letting $\{\alpha_1, \ldots, \alpha_l\} \subseteq \mathcal{M}$ be an $\mathcal{O}$-generating set for some $l \in \mathbb{N}$, for $j \in \{1, \ldots, l\}$ we get $\alpha_j = \sum_{k=1}^{l} \alpha_k \beta_{kj}$, where $\beta_{kj} \in \mathfrak{p}$. Hence letting $B := E_l - [\beta_{kj}] \in \mathcal{O}^{l \times l}$ and $\beta := \det(B) \in \mathcal{O}$, we have $[\alpha_1, \ldots, \alpha_l] \cdot B = 0 \in \mathcal{M}^l$, and thus by Cramer's Rule we get $[\alpha_1, \ldots, \alpha_l] \cdot B \cdot \mathrm{adj}(B) = [\alpha_1, \ldots, \alpha_l] \cdot \beta = 0 \in \mathcal{M}^l$. This implies that $\mathcal{M}\beta = \{0\}$, that is $\beta\widehat{\mathcal{O}} \subseteq \mathcal{U}$. Laplace expansion of $\det(B)$ shows that $\beta \equiv 1 \pmod{\mathfrak{p}}$, hence $\beta \neq 0$. Thus recalling $L = \frac{\widehat{\mathcal{O}}}{K^*}$, we get $L = \beta L = \frac{\beta\widehat{\mathcal{O}}}{K^*} \subseteq \frac{\mathcal{U}}{K^*} = \frac{\langle \mathcal{B} \rangle_{\mathcal{O}}}{K^*} = \langle \mathcal{B} \rangle_K$. ♯

Corollary. Let $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$. Then we have $N_L(\mathfrak{a}\widehat{\mathcal{O}}) = N_K(\mathfrak{a})^n$.

Proof. By the multiplicativity of N_K and N_L, and factorization of ideals, we may assume that $\mathfrak{a} = \mathfrak{p} \in \mathcal{P}_K$ is a prime ideal. Then we have $\dim_{\mathcal{O}/\mathfrak{p}}(\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}) = n$, so that $N_L(\mathfrak{p}\widehat{\mathcal{O}}) = |\widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}| = |\mathcal{O}/\mathfrak{p}|^n = N_K(\mathfrak{p})^n$. ♯

(5.7) Ramification and discriminants. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, with ring of integers $\mathcal{O} := \mathcal{O}_K$, let $p \in \mathcal{P}_{\mathbb{Z}}$, let $\mathcal{P}_K(p) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, where $r \in \mathbb{N}$, and let $e_i := e(\mathfrak{p}_i)$ and $f_i := f(\mathfrak{p}_i)$.

Theorem. Then $p^\delta \mid \mathrm{disc}(\mathcal{O})$, where $\delta := \sum_{i=1}^{r}(e_i - 1)f_i = n - \sum_{i=1}^{r} f_i \in \mathbb{N}_0$.

Proof. Recalling the proof of the fundamental equality in (5.6), in the special case considered here we have $\mathcal{O}/p\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{p}_i^{e_i}$ as $\mathbb{F}_p$-algebras, where letting

$F_i := \mathcal{O}/\mathfrak{p}_i$ we have $\dim_{\mathbb{F}_p}(F_i) = f_i$, and for $k \in \{1, \dots, e_i\}$ we have $\mathfrak{p}_i^{k-1}/\mathfrak{p}_i^k \cong F_i$ as F_i-vector spaces; in particular $\dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p}_i^{e_i}) = e_i f_i$.

For $i \in \{1, \dots, r\}$ let $\{\beta_{i1}, \dots, \beta_{i,f_i}\} \subseteq \mathcal{O}$ be a lift of an $\mathbb{F}_p$-basis of F_i, and for $k \in \{1, \dots, e_i\}$ let $\alpha_{ik} \in (\mathfrak{p}_i^{k-1} \setminus \mathfrak{p}_i^k) \cap \prod_{l \neq i} \mathfrak{p}_l^{e_l}$. Letting $\mathcal{B}_i := \{\alpha_{ik}\beta_{ij} \in \mathcal{O}; k \in \{1, \dots, e_i\}, j \in \{1, \dots, f_i\}\}$, the set $\mathcal{B} := \coprod_{i=1}^r \mathcal{B}_i \subseteq \mathcal{O}$ is a lift of an $\mathbb{F}_p$-basis of $\mathcal{O}/p\mathcal{O}$, such that $\mathcal{B}_i \subseteq \mathcal{O}$ is a lift of an $\mathbb{F}_p$-basis of $\overline{\mathcal{O}}_i := \mathcal{O}/\mathfrak{p}_i^{e_i}$.

Let $\mathcal{U} := \langle \mathcal{B} \rangle_{\mathbb{Z}} \subseteq \mathcal{O}$, which since $\mathcal{B} \subseteq K$ is a $\mathbb{Q}$-basis is a free Abelian group of rank n. Hence $\mathcal{O}/\mathcal{U}$ is finite, and we have $\operatorname{disc}(\mathcal{U}) = [\mathcal{O} \colon \mathcal{U}]^2 \cdot \operatorname{disc}(\mathcal{O})$. Since $\mathcal{O}/\mathcal{U}$ is annihilated by an element $b \in \mathbb{Z}$ such that $b \equiv 1 \pmod{p}$ (see the proof in (5.6)), we conclude that $p \nmid [\mathcal{O} \colon \mathcal{U}]$, so that it suffices to show that $p^\delta \mid \operatorname{disc}(\mathcal{U})$:

Let $\overline{\ } \colon \mathcal{O} \to \mathcal{O}/p\mathcal{O}$ be the natural epimorphism. Generalizing straightforwardly from the field extension case, considering traces with respect to the regular representation yields the symmetric $\mathbb{F}_p$-bilinear **trace form** $\langle \cdot, \cdot \rangle_{\overline{\mathcal{O}}} \colon \overline{\mathcal{O}} \times \overline{\mathcal{O}} \to \mathbb{F}_p \colon [x, y] \mapsto T_{\overline{\mathcal{O}}/\mathbb{F}_p}(xy)$. Since $p \nmid [\mathcal{O} \colon \mathcal{U}]$, the representing matrix of any element $\omega \in \mathcal{O}$ with respect to the $\mathbb{Q}$-basis $\mathcal{B}$ has entries in the **localization** $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q}; a, b \in \mathbb{Z}, p \nmid b\} \subseteq \mathbb{Q}$ of $\mathbb{Z}$ at its prime ideal (p). Hence its **p-modular reduction**, given by the natural epimorphism $\mathbb{Z}_{(p)} \to \mathbb{F}_p$, yields the representing matrix of $\overline{\omega} \in \overline{\mathcal{O}}$ with respect to the $\mathbb{F}_p$-basis $\overline{\mathcal{B}}$. In conclusion, letting $\Gamma_{\mathcal{B}} \in \mathbb{Z}^{n \times n}$ be the Gram matrix of the trace form on K with respect to the $\mathbb{Q}$-basis $\mathcal{B}$, we conclude that its p-modular reduction coincides with the Gram matrix $\Gamma_{\overline{\mathcal{B}}} \in \mathbb{F}_p^{n \times n}$ of the trace form on $\overline{\mathcal{O}}$ with respect to the $\mathbb{F}_p$-basis $\overline{\mathcal{B}}$.

Since $\mathcal{B}_i$ annihilates $\bigoplus_{l \neq i} \overline{\mathcal{O}}_l$, we conclude that $\Gamma_{\overline{\mathcal{B}}} = \bigoplus_{i=1}^r \Gamma_{\overline{\mathcal{B}}_i}$ is a block diagonal matrix, where $\Gamma_{\overline{\mathcal{B}}_i} \in \mathbb{F}_p^{e_i f_i \times e_i f_i}$ is the Gram matrix of the trace form on $\overline{\mathcal{O}}_i$ with respect to the $\mathbb{F}_p$-basis $\overline{\mathcal{B}}_i$. Moreover, since $\alpha_{ik}\beta_{ij} \in \mathcal{B}_i$ acts nilpotently on $\overline{\mathcal{O}}_i$, for $k \in \{2, \dots, e_i\}$, we get $\mathfrak{p}_i/\mathfrak{p}_i^{e_i} \subseteq \operatorname{rad}(\langle \cdot, \cdot \rangle_{\overline{\mathcal{O}}_i}) \trianglelefteq \overline{\mathcal{O}}_i$. Thus we have $\operatorname{rk}_{\mathbb{F}_p}(\Gamma_{\overline{\mathcal{B}}_i}) = \dim_{\mathbb{F}_p}(\overline{\mathcal{O}}_i/\operatorname{rad}(\langle \cdot, \cdot \rangle_{\overline{\mathcal{O}}_i})) \leq \dim_{\mathbb{F}_p}(\overline{\mathcal{O}}_i/(\mathfrak{p}_i/\mathfrak{p}_i^{e_i})) = \dim_{\mathbb{F}_p}(F_i) = f_i$. Hence we infer $d := \operatorname{rk}_{\mathbb{F}_p}(\overline{\Gamma}_{\mathcal{B}}) = \operatorname{rk}_{\mathbb{F}_p}(\Gamma_{\overline{\mathcal{B}}}) = \sum_{i=1}^r \operatorname{rk}_{\mathbb{F}_p}(\Gamma_{\overline{\mathcal{B}}_i}) \leq \sum_{i=1}^r f_i \leq n$.

Considering the Smith normal form $\operatorname{diag}[m_1, \dots, m_n] \in \mathbb{Z}^{n \times n}$ of $\Gamma_{\mathcal{B}}$, where $m_1 \mid m_2 \mid \cdots \mid m_n \in \mathbb{Z}$, from $\operatorname{rk}_{\mathbb{Q}}(\Gamma_{\mathcal{B}}) = n$ we get $m_s \neq 0$ for all $s \in \{1, \dots, n\}$. We conclude that $m_1, \dots, m_d$ are coprime to p, while $m_{d+1}, \dots, m_n$ are divisible by p. Hence we get $p^\delta = p^{n - \sum_{i=1}^r f_i} \mid p^{n-d} \mid \prod_{s=1}^n m_s = \det(\Gamma_{\mathcal{B}}) = \operatorname{disc}(\mathcal{U})$. ♯

Corollary. The prime p is ramified in K if and only if $p \mid \operatorname{disc}(\mathcal{O}) \in \mathbb{Z}$.

Proof. We have $p \mid \operatorname{disc}(\mathcal{O})$ if and only if $p \mid \operatorname{disc}(\mathcal{U}) = \det(\Gamma_{\mathcal{B}})$, which is equivalent to $p \mid m_n$, which holds if and only if $d = \operatorname{rk}_{\mathbb{F}_p}(\Gamma_{\overline{\mathcal{B}}}) = \operatorname{rk}_{\mathbb{F}_p}(\overline{\Gamma}_{\mathcal{B}}) < n$. Moreover, p is ramified in K, that is $e_i > 1$ for some $i \in \{1, \dots, r\}$, if and only if $\delta > 0$, which is equivalent to $\sum_{i=1}^r f_i < n$.

Letting first $p \nmid \operatorname{disc}(\mathcal{O})$, then we have $n = d \leq \sum_{i=1}^r f_i \leq n$, thus $\sum_{i=1}^r f_i = n$, saying that p is unramified in K. Conversely, letting p be unramified in K, we have to show that $d = n$:

Since $e_i = 1$, for all $i \in \{1, \dots, r\}$, we have $\overline{\mathcal{O}} = \bigoplus_{i=1}^r \overline{\mathcal{O}}_i = \bigoplus_{i=1}^r \mathcal{O}_i/\mathfrak{p}_i = \bigoplus_{i=1}^r F_i$. Hence the induced trace form on $\overline{\mathcal{O}}_i = F_i$ coincides with the non-degenerate trace form on the separable field extension $\mathbb{F}_p \subseteq F_i$. Hence we infer $\operatorname{rad}(\langle \cdot, \cdot \rangle_{\overline{\mathcal{O}}}) = \bigoplus_{i=1}^r \operatorname{rad}(\langle \cdot, \cdot \rangle_{\overline{\mathcal{O}}_i}) = \{0\}$, thus $d = \operatorname{rk}_{\mathbb{F}_p}(\Gamma_{\overline{\mathcal{B}}}) = \dim_{\mathbb{F}_p}(\overline{\mathcal{O}}) = n$. ♯

Corollary. Let $K \subseteq L$ be algebraic number fields. Then there are only finitely many prime ideals in K which are ramified in L.

Proof. If $\mathfrak{p} \in \mathcal{P}_K$ is ramified in L, then $\mathfrak{p} \cap \mathbb{Q} \in \mathcal{P}_{\mathbb{Q}}$ is ramified in L as well. ♯

(5.8) Computing ramification. a) Let $K \subseteq L$ be algebraic number fields such that $n := [L\colon K]$, let $\mathcal{O} := \mathcal{O}_K$ and $\widehat{\mathcal{O}} := \mathcal{O}_L$, and let $\alpha \in \widehat{\mathcal{O}}$ be a primitive element of L over K, having minimum polynomial $\mu_\alpha \in \mathcal{O}[X]$ over K.

Then $\widetilde{\mathcal{O}} := \mathcal{O}[\alpha] \subseteq \widehat{\mathcal{O}}$ is a (possibly proper) subring. To describe the relationship between these rings, for any subring $R \subseteq \widehat{\mathcal{O}}$ we consider the annihilator $\mathfrak{c}_R := \operatorname{ann}_R(\widehat{\mathcal{O}}/\widetilde{\mathcal{O}}) := \{\omega \in R; \omega\widehat{\mathcal{O}} \subseteq \widetilde{\mathcal{O}}\} \trianglelefteq R$, called the associated R**-conductor**; note that the $\widehat{\mathcal{O}}$-conductor is the largest ideal of $\widehat{\mathcal{O}}$ being contained in the subring $\widetilde{\mathcal{O}}$.

We show that $\mathfrak{c}_R \neq \{0\}$: To this end, it suffices to consider $\mathfrak{c}_{\mathbb{Z}} = \mathfrak{c}_R \cap \mathbb{Z}$. Now $\widehat{\mathcal{O}}$ is a free $\mathbb{Z}$-module of rank $[L\colon \mathbb{Q}] = [L\colon K] \cdot [K\colon \mathbb{Q}] = n \cdot [K\colon \mathbb{Q}]$; moreover $\widetilde{\mathcal{O}}$ is a free $\mathcal{O}$-module of rank n, where $\mathcal{O}$ is a free $\mathcal{O}$-module of rank $[K\colon \mathbb{Q}]$, hence $\widetilde{\mathcal{O}}$ is a free $\mathbb{Z}$-module of rank $n \cdot [K\colon \mathbb{Q}]$ as well. Thus $\widehat{\mathcal{O}}/\widetilde{\mathcal{O}}$ is a finite Abelian group, where hence $0 \neq [\widehat{\mathcal{O}}\colon \widetilde{\mathcal{O}}] \in \mathfrak{c}_{\mathbb{Z}}$.

The ideal $\{0\} \neq \mathfrak{c}_{\mathbb{Z}} \trianglelefteq \mathbb{Z}$ is generated by the exponent of the Abelian group $\widehat{\mathcal{O}}/\widetilde{\mathcal{O}}$. Hence its prime divisors coincide with those of $[\widehat{\mathcal{O}}\colon \widetilde{\mathcal{O}}]$. Thus from $\operatorname{disc}(\widetilde{\mathcal{O}}) = [\widehat{\mathcal{O}}\colon \widetilde{\mathcal{O}}]^2 \cdot \operatorname{disc}(\widehat{\mathcal{O}})$ we infer that the prime divisors of $\mathfrak{c}_{\mathbb{Z}}$ and those of $\frac{\operatorname{disc}(\widetilde{\mathcal{O}})}{\operatorname{disc}(\widehat{\mathcal{O}})} \in \mathbb{Z}$ coincide; in particular, the prime divisors of $\mathfrak{c}_{\mathbb{Z}}$ occur amongst those of $\operatorname{disc}(\widetilde{\mathcal{O}})$.

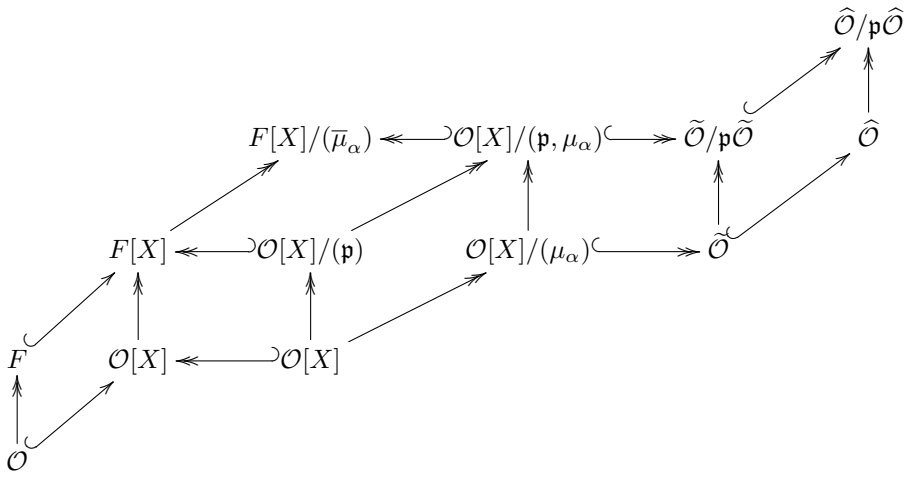
b) Given $\mathfrak{p} \in \mathcal{P}_K$, let $\overline{\ }\colon \mathcal{O} \to \mathcal{O}/\mathfrak{p} =: F$ be the natural epimoprhism. Moreover, let $g_1, \dots, g_r \in \mathcal{O}[X]$ be monic, such that $\overline{\mu}_\alpha = \prod_{i=1}^r \overline{g}_i^{e_i} \in F[X]$, where $r \in \mathbb{N}$ and $e_i \in \mathbb{N}$, and where $\overline{g}_1, \dots, \overline{g}_r \in F[X]$ are pairwise distinct and irreducible; hence letting $f_i := \deg(g_i) \in \mathbb{N}$ we have $n = \deg(\mu_\alpha) = \sum_{i=1}^r e_i f_i$.

Theorem. Assume that $\mathfrak{p}$ does not divide $\mathfrak{c}_{\mathcal{O}} = \operatorname{ann}_{\mathcal{O}}(\widehat{\mathcal{O}}/\widetilde{\mathcal{O}})$. Then we have $\mathcal{P}_L(\mathfrak{p}) = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$, where the $\mathfrak{q}_i := (\mathfrak{p}, g_i(\alpha)) \lhd \widehat{\mathcal{O}}$ are pairwise distinct prime ideals, such that $\mathfrak{p}\widehat{\mathcal{O}} = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$, that is we have $e_K(\mathfrak{q}_i) = e_i$, where $f_K(\mathfrak{q}_i) = f_i$.

Proof. We consider the commutative diagram of natural algebra homomorphisms depicted in Table 2, where monomorphisms and epimorphisms are indicated by hooked arrows and two-headed arrows, respectively. The upright epimorphisms are induced by the natural map $\overline{\ }\colon \mathcal{O} \to \mathcal{O}/\mathfrak{p} = F$.

i) The natural embedding $\widetilde{\mathcal{O}} \to \widehat{\mathcal{O}}$ induces a homomorphism $\widetilde{\mathcal{O}}/\mathfrak{p}\widetilde{\mathcal{O}} \to \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$. We show that the latter is an isomorphism, by using the conductor condition:

Table 2: Computing ramification.



Since $\mathfrak{c}_\mathcal{O} + \mathfrak{p} = \mathcal{O}$ and $\mathfrak{c}_\mathcal{O} \subseteq \widetilde{\mathcal{O}}$, we have $\widehat{\mathcal{O}} = \mathcal{O} \cdot \widehat{\mathcal{O}} = (\mathfrak{c}_\mathcal{O} + \mathfrak{p})\widehat{\mathcal{O}} \subseteq \widetilde{\mathcal{O}} + \mathfrak{p}\widehat{\mathcal{O}} \subseteq \widehat{\mathcal{O}}$, entailing that $\widetilde{\mathcal{O}} + \mathfrak{p}\widehat{\mathcal{O}} = \widehat{\mathcal{O}}$. Hence the natural map $\widetilde{\mathcal{O}} \to \widehat{\mathcal{O}}/\mathfrak{p}\widehat{\mathcal{O}}$ is an epimorphism, having kernel $\widetilde{\mathcal{O}} \cap \mathfrak{p}\widehat{\mathcal{O}}$. We have $\mathfrak{p}\widetilde{\mathcal{O}} \subseteq \widetilde{\mathcal{O}} \cap \mathfrak{p}\widehat{\mathcal{O}} = (\widetilde{\mathcal{O}} \cap \mathfrak{p}\widehat{\mathcal{O}}) \cdot \mathcal{O} = (\widetilde{\mathcal{O}} \cap \mathfrak{p}\widehat{\mathcal{O}})(\mathfrak{c}_\mathcal{O} + \mathfrak{p}) \subseteq \mathfrak{p}\widetilde{\mathcal{O}}$, entailing that $\widetilde{\mathcal{O}} \cap \mathfrak{p}\widehat{\mathcal{O}} = \mathfrak{p}\widetilde{\mathcal{O}}$.

ii) Hence it suffices to consider $\widetilde{\mathcal{O}}$: The isomorphism $\mathcal{O}[X]/(\mu_\alpha) \to \mathcal{O}[\alpha] = \widetilde{\mathcal{O}}$ is induced by the evaluation map $\mathcal{O}[X] \to \widetilde{\mathcal{O}}$ defined by $X \mapsto \alpha$. Hence the natural map induced by $\bar{}$ entails a natural isomorphism $\mathcal{O}[X]/(\mathfrak{p},\mu_\alpha) \to \widetilde{\mathcal{O}}/\mathfrak{p}\widetilde{\mathcal{O}}$.

Similarly, from the identity on $\mathcal{O}[X]$ we get a natural isomorphism $\mathcal{O}[X]/(\mathfrak{p}) \to (\mathcal{O}/\mathfrak{p})[X] = F[X]$; and the natural maps induced by μ_α and $\overline{\mu}_\alpha$, respectively, yield a natural isomorphism $\mathcal{O}[X]/(\mathfrak{p},\mu_\alpha) \to F[X]/(\overline{\mu}_\alpha)$.

Now, since the $\overline{g}_i$ are pairwise coprime, the Chinese Remainder Theorem yields $F[X]/(\overline{\mu}_\alpha) \cong \bigoplus_{i=1}^r F[X]/(\overline{g}_i^{e_i})$. Hence the prime ideals of $F[X]/(\overline{\mu}_\alpha)$ are the principal ideals $(\overline{g}_i) \lhd F[X]$, where $[F[X]/(\overline{g}_i)\colon F] = \deg(\overline{g}_i) = f_i$.

Thus, transporting through the above isomorphisms, we conclude that the prime ideals of $\widetilde{\mathcal{O}}/\mathfrak{p}\widetilde{\mathcal{O}}$, coinciding with the prime ideals of $\widetilde{\mathcal{O}}$ dividing $\mathfrak{p}\widetilde{\mathcal{O}}$, are the ideals $\mathfrak{q}_i := (\mathfrak{p}, g_i(\alpha)) \lhd \widetilde{\mathcal{O}}$, where $\mathfrak{p}\widetilde{\mathcal{O}} = \prod_{i=1}^r \mathfrak{q}_i^{e_i}$ and $[\widetilde{\mathcal{O}}/\mathfrak{q}_i\colon \mathcal{O}/\mathfrak{p}] = f_i$. ♯

Note that the conductor condition in particular is fulfilled if $\widetilde{\mathcal{O}} = \widehat{\mathcal{O}}$. It will be shown in (10.2) below that the conductor condition cannot be dispensed of.

(5.9) Example: The pure cubic field $\mathbb{Q}(\sqrt[3]{2})$. Let $\alpha := \sqrt[3]{2} \in \mathbb{R}$, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} = \mathcal{O}_K$. Since $\mu_\alpha := X^3 - 2 \in \mathbb{Q}[X]$ splits as $\mu_\alpha = \prod_{i=0}^2 (X -$

$\zeta^i\alpha) \in \mathbb{C}[X]$, where $\zeta := \zeta_3 = \frac{1}{2}(-1+\sqrt{-3}) \in \mathbb{C}$ is a primitive 3-rd root of unity, the embeddings of K into $\mathbb{C}$ are given by $\alpha \mapsto \zeta^i\alpha$ for $i \in \{0,1,2\}$.

We determine $\mathcal{O}$: We have $\mathbb{Z}[\alpha] \subseteq \mathcal{O}$, where $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(\mu_\alpha)$. Letting

$$\Delta := \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \zeta\alpha & \zeta^2\alpha^2 \\ 1 & \zeta^2\alpha & \zeta\alpha^2 \end{bmatrix} = [\zeta^{i+j-2}]_{ij} \cdot \operatorname{diag}[1,\alpha,\alpha^2],$$

we get $\operatorname{disc}(\mathbb{Z}[\alpha]) = \det(\Delta)^2 = \alpha^6 \cdot \big((1-\zeta)(1-\zeta^2)(\zeta-\zeta^2)\big)^2 = -4 \cdot 27$.

Hence we have to check the elements $\omega := \frac{1}{p}(a+b\alpha+c\alpha^2) \in K$, where $p \in \{2,3\}$ and $a,b,c \in \{0,\dots,p-1\}$, for integrality. To this end, we consider the regular representation ρ with respect to the $\mathbb{Q}$-basis $\{1,\alpha,\alpha^2\} \subseteq K$, for which $\rho(\alpha)$ is the companion matrix associated with μ_α. This yields $p^3 \cdot N(\omega) = \det(p \cdot \rho(\omega)) = a^3 + 2b^3 + 4c^3 - 6abc$. Checking $N(\omega) \in \mathbb{Q}$ for integrality, we find no non-zero solution. Hence we infer that $\mathcal{O} = \mathbb{Z}[\alpha]$, and the ramified primes are $p \in \{2,3\}$:

For $p := 2$ we get $\overline{\mu}_\alpha = X^3 \in \mathbb{F}_2[X]$, so that we find the unique prime divisor $\mathfrak{p}_2 := (2,\alpha) = (\alpha) \lhd \mathcal{O}$, such that $2\mathcal{O} = \mathfrak{p}_2^3$ is non-split and completely ramified.

For $p := 3$ we get $\overline{\mu}_\alpha = (X+1)^3 \in \mathbb{F}_3[X]$, yielding the prime divisor $\mathfrak{p}_3 := (3,\alpha+1) = (\alpha+1) \lhd \mathcal{O}$, such that $3\mathcal{O} = \mathfrak{p}_3^3$ is non-split and completely ramified.

Here are a few unramified cases: (Note that in unramified cases the tuple of inertia degrees forms a partition of the field degree, up to reordering. The examples are chosen to exhibit all partitions of $[K\colon \mathbb{Q}] = 3$.)

For $p := 5$ we get the factorization $\overline{\mu}_\alpha = (X+2)(X^2-2X-1) \in \mathbb{F}_5[X]$, so that we find the prime divisors $\mathfrak{p}_5 := (5,\alpha+2) \lhd \mathcal{O}$ and $\mathfrak{q}_5 := (5,\alpha^2-2\alpha-1) \lhd \mathcal{O}$, such that $5\mathcal{O} = \mathfrak{p}_5\mathfrak{q}_5$ is split, where $f(\mathfrak{p}_5) = 1$ and $f(\mathfrak{q}_5) = 2$.

For $p := 7$ we find that $\overline{\mu}_\alpha = X^3 - 2 \in \mathbb{F}_7[X]$ is irreducible, thus $(7) \lhd \mathcal{O}$ is inert.

For $p := 31$ we get $\overline{\mu}_\alpha = (X-4)(X-7)(X+11) \in \mathbb{F}_{31}[X]$, so that we find the prime divisors $\mathfrak{p}_{31} := (31,\alpha-4) \lhd \mathcal{O}$ and $\mathfrak{p}'_{31} := (31,\alpha-7) \lhd \mathcal{O}$ and $\mathfrak{p}''_{31} := (31,\alpha+11) \lhd \mathcal{O}$, such that $31\mathcal{O} = \mathfrak{p}_{31}\mathfrak{p}'_{31}\mathfrak{p}''_{31}$ is completely split.

(5.10) Example: Another cubic field. Let $\alpha \in \mathbb{R}$ a root of $f := X^3 - X - 1 \in \mathbb{Z}[X]$; note that $\overline{f} \in \mathbb{F}_2[X]$ is irreducible, hence $f \in \mathbb{Q}[X]$ also is. Moreover, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} = \mathcal{O}_K$. We determine $\mathcal{O}$:

We have $\mathbb{Z}[\alpha] \subseteq \mathcal{O}$, where $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$. We consider the regular representation with respect to the $\mathbb{Q}$-basis $\{1,\alpha,\alpha^2\} \subseteq K$, for which $\rho(\alpha)$ is the companion matrix associated with f. This yields $\operatorname{disc}(\mathbb{Z}[\alpha]) = \det(\Gamma) = -23$, where

$$\Gamma = [T(\alpha^{i+j-2})]_{ij} = \begin{bmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{bmatrix}.$$

Hence we have to check the elements $\omega := \frac{1}{23}(a+b\alpha+c\alpha^2) \in K$, where $a,b,c \in \{0,\dots,22\}$, for integrality. Considering the regular representation again, we get

$23^3 \cdot N(\omega) = \det(23 \cdot \rho(\omega)) = a^3 + b^3 + c^3 + 2a^2c + ac^2 - ab^2 - bc^2 - 3abc$. Checking $N(\omega) \in \mathbb{Q}$ for integrality, we find the non-zero solutions $[a, b, c] \in \{[18, 1, 8], [22, 15, 13]\}$, while these elements have the characteristic polynomial $\chi_\omega = \chi_{\rho(\omega)} = X^3 - \frac{70}{23}X^2 + 3X - 1 \in \mathbb{Q}[X]$ and $\chi_\omega = \chi_{\rho(\omega)} = X^3 - 4X^2 + \frac{85}{23}X - 1 \in \mathbb{Q}[X]$, respectively, thus are not integral. Hence we infer that $\mathcal{O} = \mathbb{Z}[\alpha]$, and the only rational prime ramified is $p = 23$:

For $p := 23$ we get $\overline{f} = (X - 3)(X - 10)^2 \in \mathbb{F}_{23}[X]$, so that we find the prime divisors $\mathfrak{p}_{23} := (23, \alpha - 3) \lhd \mathcal{O}$ and $\mathfrak{q}_{23} := (23, \alpha - 10) \lhd \mathcal{O}$, such that $23\mathcal{O} = \mathfrak{p}_{23}\mathfrak{q}_{23}^2$ is split and ramified, where $e(\mathfrak{p}_{23}) = 1$ and $e(\mathfrak{q}_{23}) = 2$, and $f(\mathfrak{p}_{23}) = f(\mathfrak{q}_{23}) = 1$.

Here are a few unramified cases: (Note that in unramified cases the tuple of inertia degrees forms a partition of the field degree, up to reordering. The examples are chosen to exhibit all partitions of $[K\colon \mathbb{Q}] = 3$.)

For $p := 2$ we find $\overline{f} = X^3 + X + 1 \in \mathbb{F}_2[X]$ irreducible, thus $(2) \lhd \mathcal{O}$ is inert.

For $p := 5$ we get the factorization $\overline{f} = (X - 2)(X^2 + 2X - 2) \in \mathbb{F}_5[X]$, so that we find the prime divisors $\mathfrak{p}_5 := (5, \alpha - 2) \lhd \mathcal{O}$ and $\mathfrak{q}_5 := (5, \alpha^2 + 2\alpha - 2) \lhd \mathcal{O}$, such that $5\mathcal{O} = \mathfrak{p}_5\mathfrak{q}_5$ is split, where $f(\mathfrak{p}_5) = 1$ and $f(\mathfrak{q}_5) = 2$.

For $p := 59$ we get $\overline{f} = (X - 4)(X - 13)(X + 17) \in \mathbb{F}_{59}[X]$, so that we find the prime divisors $\mathfrak{p}_{59} := (5, \alpha - 4) \lhd \mathcal{O}$ and $\mathfrak{p}'_{59} := (5, \alpha - 13) \lhd \mathcal{O}$ and $\mathfrak{p}''_{59} := (5, \alpha + 17) \lhd \mathcal{O}$, such that $59\mathcal{O} = \mathfrak{p}_{59}\mathfrak{p}'_{59}\mathfrak{p}''_{59}$ is completely split.

6 Galois ramification

(6.1) Galois ramification. a) Let $K \subseteq L$ be a Galois extension of algebraic number fields such that $n := [L\colon K]$, let $G := \mathrm{Aut}_K(L)$, let $\mathcal{O} := \mathcal{O}_K$ and $\widehat{\mathcal{O}} := \mathcal{O}_L$, and let $\mathfrak{p} \in \mathcal{P}_K$.

Then, since $\mathcal{O}$ is fixed element-wise, G acts by $\mathcal{O}$-algebra automorphisms on $\widehat{\mathcal{O}}$, and since $\mathfrak{p} \lhd \mathcal{O}$ and thus $\mathfrak{p}\widehat{\mathcal{O}} \lhd \widehat{\mathcal{O}}$ are G-**stable**, that is invariant under the G-action, we infer that G permutes the non-empty finite set $\mathcal{P}_L(\mathfrak{p})$.

Proposition. *G acts transitively on $\mathcal{P}_L(\mathfrak{p})$.*

Proof. Assume there are $\mathfrak{q}, \mathfrak{q}' \in \mathcal{P}_L(\mathfrak{p})$ such that $\mathfrak{q}' \neq \mathfrak{q}^\sigma \in \mathcal{P}_L(\mathfrak{p})$ for all $\sigma \in G$. By the Chinese Remainder Theorem there is $\alpha \in \widehat{\mathcal{O}}$ such that $\alpha \equiv 0 \pmod{\mathfrak{q}'}$, and $\alpha \equiv 1 \pmod{\mathfrak{q}^\sigma}$ for all $\sigma \in G$. Since $\alpha \in \mathfrak{q}'$ and $\alpha \mid N(\alpha)$, we infer that $N(\alpha) \in \mathfrak{q}' \cap \mathcal{O} = \mathfrak{p}$. But we have $\alpha^\sigma \notin \mathfrak{q}$, hence $N(\alpha) = \prod_{\sigma \in G} \alpha^\sigma \notin \mathfrak{q}$ as well, thus $N(\alpha) \notin \mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$, a contradiction. ♯

Hence, any ideals $\mathfrak{q}, \mathfrak{q}' \in \mathcal{P}_L(\mathfrak{p})$ are **conjugate**, that is there is $\sigma \in G$ such that $\mathfrak{q}' = \mathfrak{q}^\sigma$. Thus we infer that $\widehat{\mathcal{O}}/\mathfrak{q} \cong \widehat{\mathcal{O}}^\sigma/\mathfrak{q}^\sigma = \widehat{\mathcal{O}}/\mathfrak{q}'$, so that $f := f_K(\mathfrak{q}) = f_K(\mathfrak{q}')$. Moreover, we have $\mathfrak{q}^k \mid \mathfrak{p}\widehat{\mathcal{O}}$ if and only if $\mathfrak{q}'^k = (\mathfrak{q}^\sigma)^k \mid (\mathfrak{p}\widehat{\mathcal{O}})^\sigma = \mathfrak{p}\widehat{\mathcal{O}}$, for $k \in \mathbb{N}$, so that $\mathfrak{p}\widehat{\mathcal{O}} = \big(\prod_{\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})} \mathfrak{q}\big)^e \lhd \widehat{\mathcal{O}}$, where $e := e_K(\mathfrak{q}) = e_K(\mathfrak{q}')$. Hence letting $r := |\mathcal{P}_L(\mathfrak{p})|$, the fundamental equality just reads $ref = n$.

b) The stabilizer $G(\mathfrak{q}/\mathfrak{p}) := G_\mathfrak{q} = \mathrm{Stab}_G(\mathfrak{q}) := \{\sigma \in G; \mathfrak{q}^\sigma = \mathfrak{q}\} \leq G$ is called the **decomposition group** of $\mathfrak{q}$. The fixed field $K \subseteq D(\mathfrak{q}/\mathfrak{p}) = D_\mathfrak{q} := \mathrm{Fix}_L(G_\mathfrak{q}) := \{x \in L; x^\sigma = x \text{ for all } \sigma \in G_\mathfrak{q}\} \subseteq L$ is called the **decomposition field** of $\mathfrak{q}$.

Hence we have $[D_\mathfrak{q}\colon K] = [G\colon G_\mathfrak{q}] = |\mathcal{P}_L(\mathfrak{p})| = r$. In particular, we have $G_\mathfrak{q} = \{1\}$, that is $D_\mathfrak{q} = L$, if and only if $\mathfrak{p}$ is completely split in L; and we have $G_\mathfrak{q} = G$, that is $D_\mathfrak{q} = K$, if and only if $\mathfrak{p}$ is non-split in L.

Proposition. Let $\mathfrak{q}_D := \mathfrak{q} \cap D_\mathfrak{q} \lhd \mathcal{O}_{D_\mathfrak{q}}$ be the prime ideal lying under $\mathfrak{q}$. Then $\mathcal{P}_L(\mathfrak{q}_D) = \{\mathfrak{q}\}$, where $e_{D_\mathfrak{q}}(\mathfrak{q}) = e$ and $f_{D_\mathfrak{q}}(\mathfrak{q}) = f$, while $e_K(\mathfrak{q}_D) = f_K(\mathfrak{q}_D) = 1$.

Proof. Since $D_\mathfrak{q} \subseteq L$ is Galois such that $\mathrm{Aut}_{D_\mathfrak{q}}(L) = G_\mathfrak{q}$, the prime ideals of L lying over $\mathfrak{q}_D$ are given as $\mathcal{P}_L(\mathfrak{q}_D) = \{\mathfrak{q}^\sigma \in \mathcal{P}_L; \sigma \in G_\mathfrak{q}\} = \{\mathfrak{q}\}$.

The fundamental equality yields $[L\colon K] = |\mathcal{P}_L(\mathfrak{p})| \cdot e_K(\mathfrak{q}) f_K(\mathfrak{q}) = [D_\mathfrak{q}\colon K] \cdot e_K(\mathfrak{q}) f_K(\mathfrak{q})$, hence $[L\colon D_\mathfrak{q}] = \frac{[L\colon K]}{[D_\mathfrak{q}\colon K]} = e_K(\mathfrak{q}) f_K(\mathfrak{q})$; similarly, $[L\colon D_\mathfrak{q}] = |\mathcal{P}_L(\mathfrak{q}_D)| \cdot e_{D_\mathfrak{q}}(\mathfrak{q}) f_{D_\mathfrak{q}}(\mathfrak{q}) = e_{D_\mathfrak{q}}(\mathfrak{q}) f_{D_\mathfrak{q}}(\mathfrak{q})$, thus $e_K(\mathfrak{q}) f_K(\mathfrak{q}) = e_{D_\mathfrak{q}}(\mathfrak{q}) f_{D_\mathfrak{q}}(\mathfrak{q})$.

By multiplicativity of ramification indices and inertial degrees we have $e_K(\mathfrak{q}) = e_{D_\mathfrak{q}}(\mathfrak{q}) e_K(\mathfrak{q}_D)$ and $f_K(\mathfrak{q}) = f_{D_\mathfrak{q}}(\mathfrak{q}) f_K(\mathfrak{q}_D)$, in particular $e_{D_\mathfrak{q}}(\mathfrak{q}) \mid e_K(\mathfrak{q})$ and $f_{D_\mathfrak{q}}(\mathfrak{q}) \mid f_K(\mathfrak{q})$. Thus the above equality entails $e_K(\mathfrak{q}) = e_{D_\mathfrak{q}}(\mathfrak{q})$ and $f_K(\mathfrak{q}) = f_{D_\mathfrak{q}}(\mathfrak{q})$. Moreover, from this we infer $e_K(\mathfrak{q}_D) = 1$ and $f_K(\mathfrak{q}_D) = 1$. ♯

c) We consider the residue fields $F := \mathcal{O}/\mathfrak{p}$ and $E := \widehat{\mathcal{O}}/\mathfrak{q}$: To this end, let $^-\colon \widehat{\mathcal{O}} \to E$ be the natural epimorphism. Then $G_\mathfrak{q}$ induces $\mathcal{O}$-algebra automorphisms of E, which actually are F-algebra automorphisms, so that we get a group homomorphism $^-\colon G_\mathfrak{q} \to \mathrm{Aut}_F(E)$.

Its kernel $G(\mathfrak{q}/\mathfrak{p})^0 = G_\mathfrak{q}^0 := \{\sigma \in G_\mathfrak{q}; \overline{\sigma} = \mathrm{id}_E\} \trianglelefteq G_\mathfrak{q}$ is called the **inertia group** of $\mathfrak{q}$. The associated fixed field $K \subseteq D_\mathfrak{q} \subseteq I(\mathfrak{q}/\mathfrak{p}) = I_\mathfrak{q} := \mathrm{Fix}_L(G_\mathfrak{q}^0) := \{x \in L; x^\sigma = x \text{ for all } \sigma \in G_\mathfrak{q}^0\} \subseteq L$ is called the **inertia field** of $\mathfrak{q}$; hence $D_\mathfrak{q} \subseteq I_\mathfrak{q}$ is a Galois extension such that $\mathrm{Aut}_{D_\mathfrak{q}}(I_\mathfrak{q}) \cong G_\mathfrak{q}/G_\mathfrak{q}^0$.

Now $F \subseteq E$ is an extension of finite fields of degree $f = f_K(\mathfrak{q})$, hence is Galois such that $\mathrm{Aut}_F(E) = \langle \varphi_q \rangle \cong C_f$, where φ_q is the **Frobenius automorphism** of E over F, where $q := |F|$.

Theorem. The map $^-\colon G_\mathfrak{q} \to \mathrm{Aut}_F(E)$ is surjective.

In particular, the Frobenius automorphism φ_q has a lift $\widehat{\varphi}_q \in G_\mathfrak{q} \leq G$.

Proof. Since $f_K(\mathfrak{q}_D) = 1$, the field E can likewise be considered as an extension of $\mathcal{O}_{D_\mathfrak{q}}/\mathfrak{q}_D \cong F$. Let $\rho \in E$ be a primitive element over F, let $\widehat{\rho} \in \widehat{\mathcal{O}}$ be a lift of ρ, and let $\mu_{\widehat{\rho}} \in \mathcal{O}_{D_\mathfrak{q}}[X]$ and $\mu_\rho \in F[X]$ be their minimum polynomials, respectively. Then ρ is a root of $\overline{\mu}_{\widehat{\rho}}$, thus $\mu_\rho \mid \overline{\mu}_{\widehat{\rho}} \in F[X]$. Moreover, since $D_\mathfrak{q} \subseteq L$ is Galois, $\mu_{\widehat{\rho}}$ splits in $L[X]$, and since all of its roots are integral over $\mathcal{O}_{D_\mathfrak{q}}$, it splits in $\widehat{\mathcal{O}}[X]$. Similarly, $F \subseteq E$ is Galois, so that μ_ρ splits in $E[X]$.

Table 3: Galois ramification.

$\mathrm{Aut}_{\mathrm{field}}(L)$	field	degree	ideal	ramification index	inertial degree
$\{1\}$	L		$\mathfrak{q}$		
$\vdots$	$\vert$	e	$\vert$	e	1
$G_{\mathfrak{q}}^0$	$I_{\mathfrak{q}}$		$\mathfrak{q}_I$		
$\vdots$	$\vert$	f	$\vert$	1	f
$G_{\mathfrak{q}}$	$D_{\mathfrak{q}}$		$\mathfrak{q}_D$		
$\vdots$	$\vert$	r	$\vert$	1	1
G	K		$\mathfrak{p}$		

Now let $\varphi \in \mathrm{Aut}_F(E)$. Then $\rho' := \rho^\varphi$ also is a root of μ_ρ, hence of $\overline{\mu}_{\widehat{\rho}}$. Then there is a root $\widehat{\rho}'$ of $\mu_{\widehat{\rho}}$ lifting ρ', and thus there is $\widehat{\varphi} \in \mathrm{Aut}_{D_{\mathfrak{q}}}(L) = G_{\mathfrak{q}}$ such that $\widehat{\rho}^{\widehat{\varphi}} = \widehat{\rho}'$. Since φ is uniquely defined by $\varphi\colon \rho \mapsto \rho'$, we conclude that $\overline{\widehat{\varphi}} = \varphi$. ♯

d) Hence $G_{\mathfrak{q}}/G_{\mathfrak{q}}^0$ is cyclic of order f, so that $[I_{\mathfrak{q}}\colon D_{\mathfrak{q}}] = f$. Thus from $ref = [L\colon K] = [L\colon I_{\mathfrak{q}}] \cdot [I_{\mathfrak{q}}\colon D_{\mathfrak{q}}] \cdot [D_{\mathfrak{q}}\colon K] = [L\colon I_{\mathfrak{q}}] \cdot f \cdot r$ we get $[L\colon I_{\mathfrak{q}}] = e$.

In particular, we have $G_{\mathfrak{q}}^0 = \{1\}$, that is $I_{\mathfrak{q}} = L$, if and only if $\mathfrak{p}$ is unramified in L; in this case we have $\mathrm{Aut}_F(E) \cong G_{\mathfrak{q}}/G_{\mathfrak{q}}^0 \cong G_{\mathfrak{q}} \leq G$, hence we have $G_{\mathfrak{q}} = \langle \widehat{\varphi}_q \rangle$, where $\widehat{\varphi}_q$ is the unique lift of the Frobenius automorphism. Moreover, we have $G_{\mathfrak{q}}^0 = G$, that is $I_{\mathfrak{q}} = K$, if and only if $\mathfrak{p}$ is completely ramified in L.

Proposition. Let $\mathfrak{q}_I := \mathfrak{q} \cap I_{\mathfrak{q}} \lhd \mathcal{O}_{I_{\mathfrak{q}}}$ be the prime ideal lying under $\mathfrak{q}$. Then we have $\mathcal{P}_{I_{\mathfrak{q}}}(\mathfrak{q}_D) = \{\mathfrak{q}_I\}$ and $\mathcal{P}_L(\mathfrak{q}_I) = \{\mathfrak{q}\}$. Moreover, we have $e_{I_{\mathfrak{q}}}(\mathfrak{q}) = e$ and $f_{I_{\mathfrak{q}}}(\mathfrak{q}) = 1$, while $e_{D_{\mathfrak{q}}}(\mathfrak{q}_I) = 1$ and $f_{D_{\mathfrak{q}}}(\mathfrak{q}_I) = f$.

Proof. Since $\mathfrak{q}_D$ is non-split in L, it is non-split in $I_{\mathfrak{q}}$, and $\mathfrak{q}_I$ is non-split in L.

Next, we show that $E = \widehat{\mathcal{O}}/\mathfrak{q} \cong \mathcal{O}_{I_{\mathfrak{q}}}/\mathfrak{q}_I =: E'$, that is $f_{I_{\mathfrak{q}}}(\mathfrak{q}) = 1$: Applying the above theorem to the Galois extension $I_{\mathfrak{q}} \subseteq L$, where $\mathrm{Aut}_{I_{\mathfrak{q}}}(L) = G_{\mathfrak{q}}^0$, shows that $\mathrm{Aut}_{E'}(E)$ is an epimorphic image of $G_{\mathfrak{q}}^0/G_{\mathfrak{q}}^0 = \{1\}$, thus $\mathrm{Aut}_{E'}(E) = \{1\}$.

The fundamental equality, applied to $I_{\mathfrak{q}} \subseteq L$, yields $e = [L\colon I_{\mathfrak{q}}] = |\mathcal{P}_L(\mathfrak{q}_I)| \cdot e_{I_{\mathfrak{q}}}(\mathfrak{q}) \cdot f_{I_{\mathfrak{q}}}(\mathfrak{q}) = 1 \cdot e_{I_{\mathfrak{q}}}(\mathfrak{q}) \cdot 1$. Then we have $e = e_K(\mathfrak{q}) = e_{I_{\mathfrak{q}}}(\mathfrak{q}) e_{D_{\mathfrak{q}}}(\mathfrak{q}_I) e_K(\mathfrak{q}_D) = e \cdot e_{D_{\mathfrak{q}}}(\mathfrak{q}_I) \cdot 1$ and $f = f_K(\mathfrak{q}) = f_{I_{\mathfrak{q}}}(\mathfrak{q}) f_{D_{\mathfrak{q}}}(\mathfrak{q}_I) f_K(\mathfrak{q}_D) = 1 \cdot f_{D_{\mathfrak{q}}}(\mathfrak{q}_I) \cdot 1$. ♯

(6.2) Galois ramification continued. Let $K \subseteq L$ be a Galois extension of algebraic number fields, let $G := \mathrm{Aut}_K(L)$, and let $\mathfrak{p} \in \mathcal{P}_K$ and $\mathfrak{q} \in \mathcal{P}_L(\mathfrak{p})$. The picture developed above is summarized in Table 3.

We derive a couple of consequences: Firstly, we observe that the situation becomes particularly smooth in the case of Abelian Galois groups, shedding some light on the name-giving properties of 'decomposition fields' and 'inertial fields'. Secondly, we obtain a characterization of decomposition fields and inertia fields.

Corollary: Abelian Galois ramification. Assume additionally that both the decomposition group $G_\mathfrak{q}$ and the inertia group $G_\mathfrak{q}^0$ are normal in G. (Note that, in particular, this is fulfilled if G is Abelian.) Then we have:

i) The ideal $\mathfrak{p}$ splits completely in $D_\mathfrak{q}$.
ii) The ideals in $\mathcal{P}_{D_\mathfrak{q}}(\mathfrak{p})$ are **inert** in $I_\mathfrak{q}$, that is non-split and unramified.
iii) The ideals in $\mathcal{P}_{I_\mathfrak{q}}(\mathfrak{p})$ are completely ramified in L.

Proof. From $G_\mathfrak{q} \trianglelefteq G$ we conclude that $D_\mathfrak{q}$ is the decomposition field for all primes in $\mathcal{P}_L(\mathfrak{p})$. Then, from $G_\mathfrak{q}^0 \trianglelefteq G$ we conclude that $I_\mathfrak{q}$ is the inertia field for all primes in $\mathcal{P}_L(\mathfrak{p})$. Hence, by the treatment in (6.1), the maps $\mathcal{P}_L(\mathfrak{p}) \to \mathcal{P}_{I_\mathfrak{q}}(\mathfrak{p})\colon \mathfrak{r} \mapsto \mathfrak{r} \cap I_\mathfrak{q}$ and $\mathcal{P}_{I_\mathfrak{q}}(\mathfrak{p}) \to \mathcal{P}_{D_\mathfrak{q}}(\mathfrak{p})\colon \mathfrak{r} \mapsto \mathfrak{r} \cap D_\mathfrak{q}$ are injective, and since by the fundamental equality we have $|\mathcal{P}_L(\mathfrak{p})| = |\mathcal{P}_{I_\mathfrak{q}}(\mathfrak{p})| = |\mathcal{P}_{D_\mathfrak{q}}(\mathfrak{p})|$, they are bijections. From this and Table 3 the assertions follow. ♯

Corollary: Characterization of decomposition fields and inertia fields. For all intermediate fields $K \subseteq M \subseteq L$ we have:

a) i) We have $M \subseteq D_\mathfrak{q}$ if and only if $e_K(\mathfrak{q} \cap M) = f_K(\mathfrak{q} \cap M) = 1$.

ii) We have $D_\mathfrak{q} \subseteq M$ if and only if $|\mathcal{P}_L(\mathfrak{q} \cap M)| = 1$ (that is $\mathcal{P}_L(\mathfrak{q} \cap M) = \{\mathfrak{q}\}$).

b) i) We have $M \subseteq I_\mathfrak{q}$ if and only if $e_K(\mathfrak{q} \cap M) = 1$.

ii) We have $I_\mathfrak{q} \subseteq M$ if and only if $e_M(\mathfrak{q}) = [L\colon M]$.

Proof. We have $M = \mathrm{Fix}_L(H)$ for some $H \leq G := \mathrm{Aut}_K(L)$; then $M \subseteq L$ is Galois such that $\mathrm{Aut}_M(L) = H$. With respect to the prime ideal $\mathfrak{q} \cap M \in \mathcal{P}_M(\mathfrak{p})$, we have the decomposition and inertia groups $H_\mathfrak{q} = G_\mathfrak{q} \cap H$ and $H_\mathfrak{q}^0 = G_\mathfrak{q}^0 \cap H$, respectively. Thus by Galois correspondence for the extension $M \subseteq L$ we get the decomposition and inertia fields $M \subseteq D_\mathfrak{q}M \subseteq I_\mathfrak{q}M \subseteq L$, respectively.

a) i) We have $M \subseteq D_\mathfrak{q}$ if and only if $D_\mathfrak{q}M = D_\mathfrak{q}$, which holds if and only if $[L\colon D_\mathfrak{q}M] = [L\colon D_\mathfrak{q}]$, or equivalently $e_K(\mathfrak{q})f_K(\mathfrak{q}) = e_M(\mathfrak{q})f_M(\mathfrak{q})$. By multiplicativity we have $e_K(\mathfrak{q}) = e_M(\mathfrak{q})e_K(\mathfrak{q} \cap M)$ and $f_K(\mathfrak{q}) = f_M(\mathfrak{q})f_K(\mathfrak{q} \cap M)$, hence the latter equality is equivalent to $e_K(\mathfrak{q} \cap M)f_K(\mathfrak{q} \cap M) = 1$, which holds if and only if $e_K(\mathfrak{q} \cap M) = f_K(\mathfrak{q} \cap M) = 1$.

ii) We have $D_\mathfrak{q} \subseteq M$ if and only if $H \leq G_\mathfrak{q}$, which holds if and only if $H = H_\mathfrak{q}$, which in turn is equivalent to $\mathcal{P}_L(\mathfrak{q} \cap M) = \{\mathfrak{q}\}$.

b) i) We have $M \subseteq I_\mathfrak{q}$ if and only if $I_\mathfrak{q}M = I_\mathfrak{q}$, which holds if and only if $[L\colon I_\mathfrak{q}M] = [L\colon I_\mathfrak{q}]$, or equivalently $e_K(\mathfrak{q}) = e_M(\mathfrak{q})$. Multiplicativity $e_K(\mathfrak{q}) = e_M(\mathfrak{q})e_K(\mathfrak{q} \cap M)$ says that the latter equality is equivalent to $e_K(\mathfrak{q} \cap M) = 1$.

ii) We have $I_\mathfrak{q} \subseteq M$ if and only if $I_\mathfrak{q} M = M$, which is equivalent to $|\mathcal{P}_L(\mathfrak{q} \cap M)| = f_M(\mathfrak{q}) = 1$, which in turn holds if and only if $e_M(\mathfrak{q}) = [L\colon M]$. ♯

(6.3) Example: The biquadratic field $\mathbb{Q}(\sqrt{5}, \sqrt{3})$. Let $\beta := \sqrt{5} \in \mathbb{R}$, and $\gamma := \sqrt{3} \in \mathbb{R}$, and $\alpha := \beta\gamma = \sqrt{15}$. Then $L := \mathbb{Q}(\beta, \gamma)$ is Galois of degree $[L\colon \mathbb{Q}] = 4$, being the splitting field of $f := (X^2 - 5)(X^2 - 3) \in \mathbb{Q}[X]$, so that $G := \mathrm{Aut}_\mathbb{Q}(L) \cong V_4$, being given by $\beta \mapsto \pm\beta$ and $\gamma \mapsto \pm\gamma$.

Hence L has the quadratic subfields $K = \mathbb{Q}(\alpha)$, and $K' := \mathbb{Q}(\beta)$, and $K'' := \mathbb{Q}(\gamma)$. We have $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\mathrm{disc}(\mathcal{O}) = 4 \cdot 3 \cdot 5$; and $\mathcal{O}' := \mathcal{O}_{K'} = \mathbb{Z}[\widehat{\beta}]$, where $\widehat{\beta} := \frac{1}{2}(1 + \beta)$ and $\mathrm{disc}(\mathcal{O}') = 5$; and $\mathcal{O}'' := \mathcal{O}_{K''} = \mathbb{Z}[\gamma]$, where $\mathrm{disc}(\mathcal{O}'') = 4 \cdot 3$; see (10.1). Note that, since $L = K'K''$ where $K' \cap K'' = \mathbb{Q}$, and $\gcd(\mathrm{disc}(\mathcal{O}'), \mathrm{disc}(\mathcal{O}'')) = \{\pm 1\}$, by (3.8) we conclude that $\widehat{\mathcal{O}} := \mathcal{O}_L = \mathcal{O}'\mathcal{O}'' = \mathbb{Z}[\widehat{\beta}, \gamma]$ (although this is not needed in the sequel).

a) We describe how the primes $p \in \{2, 5\}$ ramify in L; to this end we first consider the quadratic subfields, see (10.2):

i) We consider $p := 2$: We have $2\mathcal{O} = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 := (2, 1 + \alpha) \lhd \mathcal{O}$, saying that 2 is completely ramified in K. We have $2\mathcal{O}' \lhd \mathcal{O}'$ being prime, saying that 2 is inert in K'. We have $2\mathcal{O}'' = (2, \gamma - 1)^2 = (\gamma - 1)^2 \lhd \mathcal{O}''$, saying that 2 is completely ramified in K''.

Now we consider L: For the number r of prime ideals lying over 2, their ramification indices e and their inertial degrees f we have $ref = 4$. Since 2 is ramified in K and K'', it is ramified in L as well, so that $2 \mid e$. Since 2 is inert in K', so that the associated inertial degree in K' equals 2, we infer that $2 \mid f$.

Hence in conclusion we get $e = f = 2$ and $r = 1$, so that $2\widehat{\mathcal{O}} = \mathfrak{q}_2^2 \lhd \widehat{\mathcal{O}}$ where $N(\mathfrak{q}_2) = 2^f = 4$; since $\gamma - 1 \in \mathfrak{q}_2$, where $N(\gamma - 1) = N_{K''}(\gamma - 1)^2 = 4$, we infer that $\mathfrak{q}_2 = (\gamma - 1) \lhd \widehat{\mathcal{O}}$. Thus we have $D_{\mathfrak{q}_2} = \mathbb{Q}$. Hence we have $[I_{\mathfrak{q}_2}\colon \mathbb{Q}] = 2$, where $I_{\mathfrak{q}_2} \subseteq L$ is the largest subfield such that 2 is unramified; since 2 is inert in K' we infer that $I_{\mathfrak{q}_2} = K' = \mathbb{Q}(\beta)$.

ii) We consider $p := 5$: We have $5\mathcal{O} = \mathfrak{p}_5^2$, where $\mathfrak{p}_5 := (5, \alpha) \lhd \mathcal{O}$ saying that 5 is completely ramified in K. We have $5\mathcal{O}' = (5, \widehat{\beta} - 3)^2 = (\beta)^2 \lhd \mathcal{O}'$, saying that 5 is completely ramified in K'; note that $\widehat{\beta} - 3 = \frac{1}{2}(-5 + \beta) = -\beta \cdot \frac{1}{2}(-1 + \beta) \sim \beta \in \mathcal{O}'$. We have $5\mathcal{O}'' \lhd \mathcal{O}''$ being prime, saying that 5 is inert in K''.

Now we consider L: For the number r of prime ideals lying over 5, their ramification indices e and their inertial degrees f we have $ref = 4$. Since 5 is ramified in K and K', it is ramified in L as well, so that $2 \mid e$. Since 2 is inert in K'', so that the associated inertial degree in K'' equals 2, we infer that $2 \mid f$.

Hence in conclusion we get $e = f = 2$ and $r = 1$, so that $5\widehat{\mathcal{O}} = \mathfrak{q}_5^2 \lhd \widehat{\mathcal{O}}$, where $N(\mathfrak{q}_5) = 5^f = 25$; since $\beta \in \mathfrak{q}_5$, where $N(\beta) = N_{K'}(\beta)^2 = 25$, we infer that $\mathfrak{q}_5 = (\beta) \lhd \widehat{\mathcal{O}}$. Thus we have $D_{\mathfrak{q}_5} = \mathbb{Q}$. Hence we have $[I_{\mathfrak{q}_5}\colon \mathbb{Q}] = 2$, where $I_{\mathfrak{q}_5} \subseteq L$ is the largest subfield such that 5 is unramified; since 5 is inert in K'' we infer that $I_{\mathfrak{q}_5} = K'' = \mathbb{Q}(\gamma)$.

b) Actually, this is motivated by the idea of 'making ideals principal': We consider the field K, where we observe that $10 = 2 \cdot 5 = (5+\alpha)(5-\alpha) = (5+\alpha)^2 \cdot (4-\alpha) \in \mathcal{O}$, where $N(4-\alpha) = 1$ shows that $4-\alpha \in \mathcal{O}^*$.

We show that there are no elements $\omega \in \mathcal{O}$ such that $N(\omega) \in \{\pm 2, \pm 5\}$; recall that $N(a+b\alpha) = (a+b\alpha)(a-b\alpha) = a^2 - 15b^2$, for $a, b \in \mathbb{Z}$: Writing $\omega = a+b\alpha \in \mathcal{O}$, for some $a, b \in \mathbb{Z}$, assume that $N(\omega) = a^2 - 15b^2 = \pm 2$; then we have $a^2 \equiv \pm 2 \pmod 5$, a contradiction. Similarly, assume that $N(\omega) = a^2 - 15b^2 = \pm 5$; then we have $5 \mid a$, hence writing $a = 5a'$, for some $a' \in \mathbb{Z}$, we get $5a'^2 - 3b^2 = \pm 1$, thus $b^2 \equiv \mp 2 \pmod 5$, a contradiction.

Hence we conclude that 2 and 5 and $5+\alpha$ are irreducible, but pairwise non-associate, so that they are not primes. (Note that the factorizations exhibit different multiplicities.) In particular, $\mathcal{O}$ is not factorial.

In an attempt to 'rescue' uniqueness of factorizations, we observe that $10 = 2 \cdot 5 = (5+\sqrt{15})(5-\sqrt{15}) \in \mathcal{O}$ can be rewritten as $(\sqrt{5}+\sqrt{3})(\sqrt{5}-\sqrt{3}) \cdot \sqrt{5}^2 = \sqrt{5}(\sqrt{5}+\sqrt{3}) \cdot \sqrt{5}(\sqrt{5}-\sqrt{3})$, that is $(\beta+\gamma)(\beta-\gamma) \cdot \beta^2 = \beta(\beta+\gamma) \cdot \beta(\beta-\gamma) \in \widehat{\mathcal{O}}$, which hence is one and the same decomposition of 10. (It actually is a factorization, as will be shown below.)

Considering $\mathfrak{p}_2 = (2, 1+\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_5 := (5, \alpha) \lhd \mathcal{O}$ again, we have $\mathfrak{p}_2\mathfrak{p}_5 = (10, 5+\alpha) = (5+\alpha) = (5-\alpha)$, and thus $(10) = (2) \cdot (5) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_5^2 = (\mathfrak{p}_2\mathfrak{p}_5)^2 = (5+\alpha) \cdot (5-\alpha) \lhd \mathcal{O}$. Since $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_5) = 5$, both prime ideals are not principal. But the (unique) prime ideals $\mathfrak{q}_2 = (\gamma-1) \lhd \widehat{\mathcal{O}}$ and $\mathfrak{q}_5 = (\beta) \lhd \widehat{\mathcal{O}}$ lying over $\mathfrak{p}_2$ and $\mathfrak{p}_5$, respectively, are principal; note that $(\beta+\gamma)(4-\alpha) = \beta - \gamma$, where $4-\alpha \in \mathcal{O}^*$, hence $(\beta+\gamma) = (\beta-\gamma) \lhd \widehat{\mathcal{O}}$, and from $(\beta+\gamma)(\beta-\gamma) = (\beta^2 - \gamma^2) = (2) \lhd \widehat{\mathcal{O}}$ we conclude that $(\beta+\gamma) = \mathfrak{q}_2$. Hence β and $\beta \pm \gamma$ are prime and thus irreducible indeed.

(6.4) Example: The triquadratic field $\mathbb{Q}(i, \sqrt{2}, \sqrt{5})$. Let $\alpha := \sqrt{2} \in \mathbb{R}$ and $\beta := \sqrt{5} \in \mathbb{R}$, and let $L := \mathbb{Q}(i, \alpha, \beta)$, which is Galois of degree $[L\colon \mathbb{Q}] = 8$, being the splitting field of $f := (X^2+1)(X^2-2)(X^2-5) \in \mathbb{Q}[X]$, so that $G := \mathrm{Aut}_{\mathbb{Q}}(L) = \langle \sigma, \sigma', \sigma'' \rangle \cong C_2^3$, an elementary Abelian group of order 8, being generated by $\sigma\colon i \mapsto -i$ fixing $\mathbb{Q}(\alpha, \beta)$, and $\sigma'\colon \alpha \mapsto -\alpha$ fixing $\mathbb{Q}(i, \beta)$, and $\sigma''\colon \beta \mapsto -\beta$ fixing $\mathbb{Q}(i, \alpha)$.

i) The field L has the quadratic subfields $K := \mathbb{Q}(i)$ and $K' := \mathbb{Q}(\alpha)$ and $K'' := \mathbb{Q}(\beta)$ (amongst others). Let $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[i]$, where $\mathrm{disc}(\mathcal{O}) = -4$; let $\mathcal{O}' := \mathcal{O}_{K'} = \mathbb{Z}[\alpha]$, where $\mathrm{disc}(\mathcal{O}') = 8$; and let $\mathcal{O}'' := \mathcal{O}_{K''} = \mathbb{Z}[\widehat{\beta}]$, where $\widehat{\beta} := \frac{1}{2}(1+\beta)$ and $\mathrm{disc}(\mathcal{O}'') = 5$; see (10.1).

We record how the prime $p := 5$ ramifies in the quadratic subfields mentioned; see (10.2): We have $5\mathcal{O} = (5, i-2)(5, i+2) = (i-2)(i+2) \lhd \mathcal{O}$, saying that 5 is split in K. We have $5\mathcal{O}' \lhd \mathcal{O}'$ being prime, saying that 5 is inert in K'. We have $5\mathcal{O}'' = (5, \beta)^2 = (\beta)^2 \lhd \mathcal{O}''$, saying that 5 is ramified in K''.

For the subfield $\mathbb{Q}(i, \alpha) \subseteq L$ of index 2, by (3.10) we have $\widetilde{\mathcal{O}} := \mathcal{O}_{\mathbb{Q}(i,\alpha)} = \mathbb{Z}[\zeta_8]$

such that $\mathrm{disc}(\widetilde{\mathcal{O}}) = 2^8$, where $\zeta_8 = \frac{1+i}{\alpha}$ is a primitive 8-th root of unity. Since $L = \mathbb{Q}(i,\alpha) \cdot K''$ where $\mathbb{Q}(i,\alpha) \cap K'' = \mathbb{Q}$, and $\gcd(\mathrm{disc}(\widetilde{\mathcal{O}}), \mathrm{disc}(\mathcal{O}'')) = \gcd(2^8, 5) = \{\pm 1\}$, from (3.8) we conclude that $\widehat{\mathcal{O}} := \mathcal{O}_L = \widetilde{\mathcal{O}}\mathcal{O}'' = \mathbb{Z}[\zeta_8, \widehat{\beta}]$.

ii) Now we consider how 5 ramifies in L: For the number r of prime ideals lying over 5, their ramification indices e and their inertial degrees f we have $ref = 8$. Since 5 splits in K, it splits in L as well, so that $2 \mid r$. Since 5 is ramified in K'', it is ramified in L as well, so that $2 \mid e$. Since 5 is inert in K', so that the associated inertial degree in K' equals 2, we infer that $2 \mid f$.

Hence in conclusion we get $r = e = f = 2$, so that $5\widehat{\mathcal{O}} = \mathfrak{q}_+^2\mathfrak{q}_-^2 \lhd \widehat{\mathcal{O}}$, where $\mathfrak{q}_\pm \lhd \widehat{\mathcal{O}}$ are conjugate prime ideals of norm $N(\mathfrak{q}_\pm) = 5^f = 25$.

Intersecting with the quadratic subfields mentioned yields: We have $\mathfrak{q}_\pm \cap \mathcal{O} = (i \pm 2) \lhd \mathcal{O}$, say, so that $(i \pm 2)\mathcal{O} \cdot \widehat{\mathcal{O}} = \mathfrak{q}_\pm^2$ is non-split ramified such that $f_K(\mathfrak{q}_\pm) = 2$. We have $\mathfrak{q}_\pm \cap \mathcal{O}' = (5) \lhd \mathcal{O}'$, so that $5\mathcal{O}' \cdot \widehat{\mathcal{O}} = \mathfrak{q}_+^2\mathfrak{q}_-^2$ is split and purely ramified. We have $\mathfrak{q}_\pm \cap \mathcal{O}'' = (\beta) \lhd \mathcal{O}''$, so that $\beta\mathcal{O}'' \cdot \widehat{\mathcal{O}} = \mathfrak{q}_+\mathfrak{q}_-$ is split unramified such that $f_{K''}(\mathfrak{q}_\pm) = 2$.

In particular, from $(i \pm 2) = \mathfrak{q}_\pm^2 \lhd \widehat{\mathcal{O}}$ and $(\beta) = \mathfrak{q}_+\mathfrak{q}_- \lhd \widehat{\mathcal{O}}$ we get $\mathfrak{q}_\pm = \gcd(\mathfrak{q}_\pm^2, \mathfrak{q}_+\mathfrak{q}_-) = \gcd((i \pm 2), (\beta)) = (i \pm 2, \beta) \lhd \widehat{\mathcal{O}}$.

iii) From G being Abelian we conclude that the decomposition groups $G_\mathfrak{q} := G_{\mathfrak{q}_\pm}$ coincide, and likewise the inertia groups $G_\mathfrak{q}^0 := G_{\mathfrak{q}_\pm}^0$ do so. Moreover, from $[G\colon G_\mathfrak{q}] = r = 2$ we infer that $[D_\mathfrak{q}\colon K] = 2$, and likewise from $[G_\mathfrak{q}\colon G_\mathfrak{q}^0] = f = 2$ we get $[I_\mathfrak{q}\colon K] = [I_\mathfrak{q}\colon D_\mathfrak{q}] \cdot [D_\mathfrak{q}\colon K] = 2 \cdot 2 = 4$.

The inertia field $I_\mathfrak{q} \subseteq L$ is the largest subfield such that 5 is unramified. Hence we have $K \subseteq I_\mathfrak{q}$ and $K' \subseteq I_\mathfrak{q}$, where $[KK'\colon \mathbb{Q}] = 4$ entails $I_\mathfrak{q} = \mathbb{Q}(i,\alpha)$. The decomposition field $D_\mathfrak{q} \subseteq I_\mathfrak{q}$ now is the largest subfield such that 5 additionally is pure. Hence we have $K \subseteq D_\mathfrak{q}$, entailing $D_\mathfrak{q} = \mathbb{Q}(i)$.

We have $(i \pm 2)\mathcal{O} \cdot \widetilde{\mathcal{O}} = \mathfrak{q}_\pm \cap \widetilde{\mathcal{O}} \lhd \widetilde{\mathcal{O}}$, so that the primes $i \pm 2$ in $D_\mathfrak{q}$ are inert in $I_\mathfrak{q}$. We have $G_\mathfrak{q}^0 = \langle \sigma'' \rangle \leq G_\mathfrak{q} = \langle \sigma', \sigma'' \rangle \leq G$. Hence (amongst other choices) we have $\mathfrak{q}_\pm^\sigma = \mathfrak{q}_\mp$, and σ' induces the Frobenius automorphism of $\widetilde{\mathcal{O}}/(i \pm 2)\widetilde{\mathcal{O}} \cong \mathbb{F}_{25}$.

(6.5) Example: The non-Abelian field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Let $\alpha := \sqrt[3]{2} \in \mathbb{R}$, let $\zeta := \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$ be a primitive 3-rd root of unity, and let $L := \mathbb{Q}(\alpha, \zeta)$. Hence $\mathbb{Q} \subseteq L$ is Galois of degree $[L\colon \mathbb{Q}] = 6$, being the splitting field of $\mu_\alpha := X^3 - 2 \in \mathbb{Q}[X]$. We have $\mu_\alpha = \prod_{i=1}^3 (X - \zeta^{i-1}\alpha) \in L[X]$, hence the faithful action of $\mathrm{Aut}_\mathbb{Q}(L)$ on the roots of μ_α in L yields an isomorphism $\mathrm{Aut}_\mathbb{Q}(L) \cong \mathcal{S}_3 =: G$, the symmetric group on 3 letters, which is non-Abelian.

Hence L has 3 subfields of degree 3, namely $K := \mathrm{Fix}_L(\langle (2,3) \rangle) = \mathbb{Q}(\alpha)$, and $K' := \mathrm{Fix}_L(\langle (1,3) \rangle)i = \mathbb{Q}(\zeta\alpha)$, and $K'' := \mathrm{Fix}_L(\langle (1,2) \rangle) = \mathbb{Q}(\zeta^2\alpha)$; these are mutually conjugate, where K has been considered in (5.9). Moreover, there is a unique subfield of degree 2, namely $D := \mathrm{Fix}_L(\langle (1,2,3) \rangle) = \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$, which is Galois; see (10.2).

Thus we have $L = KD$, where $[L\colon \mathbb{Q}] = [K\colon \mathbb{Q}] \cdot [D\colon \mathbb{Q}]$. Moreover, by (5.9) we have $\operatorname{disc}(\mathcal{O}_K) = -4 \cdot 27$, and by (10.1) we have $\operatorname{disc}(\mathcal{O}_D) = -3$; hence $\gcd(\operatorname{disc}(\mathcal{O}_K), \operatorname{disc}(\mathcal{O}_D)) = \{\pm 3\}$. Thus by (3.8) we have $\mathcal{O}_K\mathcal{O}_D \subseteq \mathcal{O}_L \subseteq \frac{1}{3} \cdot \mathcal{O}_K\mathcal{O}_D$, so that $\operatorname{disc}(\mathcal{O}_L) \mid \operatorname{disc}(\mathcal{O}_K\mathcal{O}_D) = (-4 \cdot 27)^2 \cdot (-3)^3 = -2^4 \cdot 3^9$. Hence the rational primes ramified in L are $p \in \{2, 3\}$:

For $p := 2$ we find that $2\mathcal{O}_K = \mathfrak{p}_2^3$ is completely ramified, where $\mathfrak{p}_2 := (\alpha) \lhd \mathcal{O}_K$; while $2\mathcal{O}_D \lhd \mathcal{O}_D$ is inert. Hence for $\mathfrak{q}_2 \in \mathcal{P}_L(2)$ we have $e(\mathfrak{q}_2) = 3$ and $f(\mathfrak{q}_2) = 2$, so that $2\mathcal{O}_L = \mathfrak{q}_2^3$, where $\mathfrak{q}_2 := (\alpha) \lhd \mathcal{O}_L$. Thus we have $D_{\mathfrak{q}_2} = \mathbb{Q}$ and $I_{\mathfrak{q}_2} = D$.

For $p := 3$ we find that $3\mathcal{O}_K = \mathfrak{p}_3^3$ is completely ramified, where $\mathfrak{p}_3 := (\alpha + 1) \lhd \mathcal{O}_K$; and $3\mathcal{O}_D = \mathfrak{r}_3^2$ is completely ramified as well, where $\mathfrak{r}_3 = (\sqrt{-3}) \lhd \mathcal{O}_D$. Hence for $\mathfrak{q}_3 \in \mathcal{P}_L(3)$ we have $e(\mathfrak{q}_3) = 6$, that is $3\mathcal{O}_L = \mathfrak{q}_3^6$ is completely ramified, where $\mathfrak{q}_3 := (\alpha + 1, \sqrt{-3}) \lhd \mathcal{O}_L$. Thus we have $D_{\mathfrak{q}_3} = \mathbb{Q}$ and $I_{\mathfrak{q}_3} = \mathbb{Q}$.

Here are a few unramified cases, where inertia fields coincide with L anyway: (Note that in unramified cases the tuple of inertia degrees forms an equal-part partition of the field degree. The examples are chosen to exhibit all cases.)

Letting $\gamma := \sqrt[6]{2^2 \cdot (-3)^3} = \sqrt[6]{-108} \in L$, we have $\mu_\gamma := X^6 + 108 \in \mathbb{Q}[X]$, thus $L = \mathbb{Q}(\gamma)$. Moreover, we find $\operatorname{disc}(\gamma) = -2^{16} \cdot 3^{21}$, so that for $p \geq 5$ we may utilize $\mathbb{Z}[\gamma] \subseteq \mathcal{O}_L$ to compute ideal factorizations.

For $p := 5$ we find that $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$, where $\mathfrak{p}_5 := (5, \alpha + 2) \lhd \mathcal{O}_K$, so that $f(\mathfrak{p}_5) = 1$ and $f(\mathfrak{p}_5') = 2$; while $5\mathcal{O}_D \lhd \mathcal{O}_D$ is inert. Hence for $\mathfrak{q}_5 \in \mathcal{P}_L(5)$ we have $2 \mid f(\mathfrak{q}_5)$, where $|\mathcal{P}_L(5)| \geq 2$. Thus we have $f(\mathfrak{q}_5) = 2$, hence $|\mathcal{P}_L(5)| = 3$, so that $5\mathcal{O}_L = \mathfrak{q}_5\mathfrak{q}_5'\mathfrak{q}_5''$, where $\mathfrak{p}_5$ is inert in L, that is $\mathfrak{q}_5 := \mathfrak{p}_5\mathcal{O}_L = (5, \alpha+2) \lhd \mathcal{O}_L$ (say), while $\mathfrak{p}_5'$ splits as $\mathfrak{p}_5' \cdot \mathcal{O}_L = \mathfrak{q}_5'\mathfrak{q}_5'' \lhd \mathcal{O}_L$. Thus we have $D_{\mathfrak{q}_5} = K$, while $D_{\mathfrak{q}_5'} = K'$ (say) and $D_{\mathfrak{q}_5''} = K''$.

For $p := 7$ we find that $7\mathcal{O}_K \lhd \mathcal{O}_K$ is inert; while $7\mathcal{O}_D = \mathfrak{r}_7\mathfrak{r}_7'$ splits, where $\mathfrak{r}_7 = (7, 2 + \sqrt{-3}) = (2 + \sqrt{-3}) \lhd \mathcal{O}_D$. Hence for $\mathfrak{q}_7 \in \mathcal{P}_L(7)$ we have $3 \mid f(\mathfrak{q}_7)$, where $|\mathcal{P}_L(7)| \geq 2$. Thus we have $f(\mathfrak{q}_7) = 3$, hence $|\mathcal{P}_L(7)| = 2$, so that $7\mathcal{O}_L = \mathfrak{q}_7\mathfrak{q}_7'$, where $\mathfrak{r}_7$ and $\mathfrak{r}_7'$ are inert in L, that is $\mathfrak{q}_7 := \mathfrak{r}_7\mathcal{O}_L = (2+\sqrt{-3}) \lhd \mathcal{O}_L$ (say) and $\mathfrak{q}_7' := \mathfrak{r}_7' = (2 - \sqrt{-3})\mathcal{O}_L \lhd \mathcal{O}_L$. Thus we have $D_{\mathfrak{q}_7} = D_{\mathfrak{q}_7'} = D$.

For $p := 31$ we find that $31\mathcal{O}_K = \mathfrak{p}_{31}\mathfrak{p}_{31}'\mathfrak{p}_{31}''$, where $\mathfrak{p}_{31} := (31, \alpha - 4) \lhd \mathcal{O}_K$ (say), and $31\mathcal{O}_D = \mathfrak{r}_{31}\mathfrak{r}_{31}'$ splits as well, where $\mathfrak{r}_{31} := (31, \sqrt{-3} - 11) \lhd \mathcal{O}_D$ (say). Hence we have $|\mathcal{P}_L(31)| \geq 3$, where since $\mathbb{Q} \subseteq D$ is Galois we have $2 \mid |\mathcal{P}_L(31)| \mid 6$, entailing $|\mathcal{P}_L(31)| = 6$. Thus we have $31\mathcal{O}_L = \prod_{i=1}^6 \mathfrak{q}_{31,i}$, where $f(\mathfrak{q}_{31,i} = 1$, and we get $\mathfrak{q}_{31,1} = \mathfrak{p}_{31}\mathcal{O}_L + \mathfrak{r}_{31}\mathcal{O}_L \lhd \mathcal{O}_L$ (say). Thus we have $D_{\mathfrak{q}_{31,i}} = L$.

III Geometry

7 Euclidean lattices

(7.1) Euclidean spaces. a) Let V be an Euclidean $\mathbb{R}$-vector space, where $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$, equipped with scalar product $\langle \cdot, \cdot \rangle$, and induced metric defined by $\|v\| := \sqrt{\langle v, v \rangle}$, for $v \in V$. Note that, by specifying an orthonormal $\mathbb{R}$-basis, V can be identified with $\mathbb{R}^n$ together with its standard $\mathbb{R}$-basis and the standard scalar product $\langle [x_1, \ldots, x_n], [y_1, \ldots, y_n] \rangle := \sum_{i=1}^n x_i y_i$, with associated metric $\|[x_1, \ldots, x_n]\| = \sqrt{\sum_{i=1}^n x_i^2}$.

For $r \geq 0$ and $v \in V$ let $B_r(v) := \{w \in V; \|v - w\| \leq r\} \subseteq V$ be the **(closed) sphere** or **ball** with **radius** r and **center** v. Similarly, its **interior** $B_\epsilon^\circ(v) := \{w \in V; \|v - w\| < r\} \subseteq V$ is called the associated **open sphere** or **open ball**. In particular, $X \subseteq V$ is called **bounded** if there is $r \geq 0$ such that $X \subseteq B_r(0)$.

b) A subset $X \subseteq V$ is called **discrete** if it consists of **isolated** points only, that is for any $v \in X$ there is an open neighborhood $v \in U \subseteq V$ such that $U \cap X = \{v\}$, or equivalently, since the open spheres are a basis of the metric topology on V, for any $v \in X$ there is $\epsilon > 0$ such that $B_\epsilon(v) \cap X = \{v\}$. Note there are non-closed discrete sets, for example $\{\frac{1}{2^k} \in \mathbb{R}; k \in \mathbb{N}_0\} \subseteq \mathbb{R}$.

Lemma. The subset $X \subseteq V$ is closed and discrete if and only if all bounded subsets of X are finite.

Proof. Let first X be closed and discrete, and let $r \geq 0$. Then $Y := X \cap B_r(0)$ is closed and bounded, that is compact. Thus any open covering of Y has a finite sub-covering, which, since Y is discrete as well, implies finiteness.

Conversely, assume that X is not discrete or not closed. Then there is $v \in V$ (in the former case even $v \in X$) and a sequence $[v_k \in X \setminus \{v\}; k \in \mathbb{N}]$ such that $\lim_{k \to \infty} v_k = v$. In particular, $\{v_k \in X \setminus \{v\}; k \in \mathbb{N}\}$ is infinite and bounded. ♯

(7.2) Euclidean lattices. a) Let V be an Euclidean $\mathbb{R}$-vector space, where $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$, let $\mathcal{B} := \{v_1, \ldots, v_m\} \subseteq V$ be $\mathbb{R}$-linearly independent, where $m \in \{0, \ldots, n\}$, and let $U := \langle \mathcal{B} \rangle_{\mathbb{R}} \leq V$. Restricting the scalar product on V yields a scalar product on U. Letting $\Gamma_{\mathcal{B}} := [\langle v_i, v_j \rangle]_{ij} \in \mathbb{R}^{m \times m}$ be its Gram matrix with respect to $\mathcal{B}$, the determinant $\mathrm{disc}(\mathcal{B}) := \det(\Gamma_{\mathcal{B}}) \in \mathbb{R}$ is called the **discriminant** of $\mathcal{B}$, where positive definiteness implies that $\mathrm{disc}(\mathcal{B}) > 0$.

The (free) Abelian group $\Lambda := \langle \mathcal{B} \rangle_{\mathbb{Z}} \subseteq V$ is called an **(Euclidean) lattice** of **rank** $\mathrm{rk}_{\mathbb{Z}}(\Lambda) := m$; if $m = n$ then Λ is called **full** or **complete**. The set $\mathcal{F} = \mathcal{F}_{\mathcal{B}} := \{\sum_{i=1}^m x_i v_i \in V; 0 \leq x_i < 1\} \subseteq V$, which depends on $\mathcal{B}$, is called the associated **fundamental domain** or **fundamental parallelotope** for Λ. From $\|v\| \leq \sum_{i=1}^m \|v_i\|$, for all $v \in \mathcal{F}$, we conclude that $\mathcal{F}$ is bounded.

Given $u = \sum_{i=1}^m x_i v_i \in U$, where $x_i \in \mathbb{R}$, letting $v := \sum_{i=1}^m a_i v_i$, where $a_i := \lfloor x_i \rfloor \in \mathbb{Z}$, and $w := u - v = \sum_{i=1}^m (x_i - a_i) v_i$, shows that u can be written

uniquely as $u = v + w$, where $v \in \Lambda$ and $w \in \mathcal{F}$. Hence $U = \coprod_{v\in\Lambda}(v + \mathcal{F})$, that is the **($\Lambda$-)translates** of $\mathcal{F}$ form a partition of U; in particular $\mathcal{F} \cap \Lambda = \{0\}$. Moreover, Λ is a full lattice if and only if the Λ-translates of $\mathcal{F}$ cover all of V.

b) Actually, having a $\mathbb{Z}$-basis which is $\mathbb{R}$-linearly independent is a distinctive property of lattices, compared to arbitrary additive subgroups of V. For example, $\langle 1, \sqrt{2}\rangle_{\mathbb{Z}} \subseteq \mathbb{R}$ is a free Abelian group of rank 2, but cannot possibly be a lattice. We proceed to characterize lattices in terms of discreteness, and subsequently characterize full lattices amongst arbitrary ones.

Proposition. i) A discrete additive subgroup $M \subseteq V$ is closed.
ii) An additive subgroup $M \subseteq V$ is discrete if and only if it is a lattice.

Proof. i) Assume to the contrary that M is not closed. Then there is $v \in V \setminus M$ and a sequence $[v_k \in M; k \in \mathbb{N}]$ such that $\lim_{k\to\infty} v_k = v$. Hence the latter is a Cauchy sequence, implying that the set $\{v_k - v_l \in M; k, l \in \mathbb{N}\}$ is infinite, entailing that $0 \in M$ is not isolated.

ii) Let first $\Lambda := \langle\mathcal{B}\rangle_{\mathbb{Z}}$ be a lattice, where $\mathcal{B} := \{v_1, \ldots, v_m\} \subseteq V$ is $\mathbb{R}$-linearly independent. Completing $\mathcal{B}$ to an $\mathbb{R}$-basis $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\} \subseteq V$, and letting $U := \{\sum_{i=1}^n \epsilon_i v_i \in V; |\epsilon_i| < 1\} \subseteq V$, then for any $v \in \Lambda$ the set $v+U \subseteq V$ is an open neighborhood of v such that $(v + U) \cap \Lambda = \{v\}$,

Let conversely $M \subseteq V$ be a discrete additive subgroup, let $U := \langle M\rangle_{\mathbb{R}} \leq V$, let $\mathcal{C} \subseteq M$ be an $\mathbb{R}$-basis of U, and let $\Lambda := \langle\mathcal{C}\rangle_{\mathbb{Z}} \subseteq U$; then Λ is a full lattice in U being contained in M.

It remains to be shown that the index of Λ in M is finite; then we conclude that $\Lambda \subseteq M \subseteq \frac{1}{[M\colon\Lambda]} \cdot \Lambda$, implying that M is a free Abelian group of rank $\mathrm{rk}_{\mathbb{Z}}(M) = \mathrm{rk}_{\mathbb{Z}}(\Lambda) = \dim_{\mathbb{R}}(U)$, so that any $\mathbb{Z}$-basis of M is an $\mathbb{R}$-basis of $\langle M\rangle_{\mathbb{R}} = \langle\Lambda\rangle_{\mathbb{R}} = U$:

To this end, let $\{v_i \in M; i \in \mathcal{I}\} \subseteq U$ be a transversal for Λ in M, for some index set $\mathcal{I}$. Letting $\mathcal{F} := \mathcal{F}_{\mathcal{C}} \subseteq U$ be the associated fundamental domain, since Λ is full in U there are $w_i \in \mathcal{F}$ such that $v_i - w_i \in \Lambda$. Hence $w_i \in M$ as well, so that $\{w_i \in M; i \in \mathcal{I}\}$ also is a transversal for Λ in M. Now we have $w_i \in M \cap \mathcal{F}$, where since M is discrete (and thus closed) and $\mathcal{F}$ is bounded $M \cap \mathcal{F}$ is finite. ♯

Proposition. The lattice $\Lambda \subseteq V$ is full if and only if there is a bounded subset $M \subseteq V$ such that $V = \bigcup_{v\in\Lambda}(v + M)$.

Proof. If Λ is full, then we may take M as a fundamental domain for Λ. Hence let conversely $M \subseteq V$ be bounded such that $V = \bigcup_{v\in\Lambda}(v + M)$, and let $U := \langle\Lambda\rangle_{\mathbb{R}} \leq V$; we have to show that $U = V$: To this end, let $v \in V$.

Then, by assumption, for any $k \in \mathbb{N}$ there are $v_k \in \Lambda \subseteq U$ and $m_k \in M$ such that $kv = v_k + m_k$. Since M is bounded, we have $\lim_{k\to\infty}(\frac{1}{k}m_k) = 0 \in V$. Thus we have $v = \lim_{k\to\infty}(\frac{1}{k}v_k) + \lim_{k\to\infty}(\frac{1}{k}m_k) = \lim_{k\to\infty}(\frac{1}{k}v_k) \in V$. Hence the latter limit exists, and since $U \subseteq V$ is closed it actually belongs to U. ♯

(7.3) Volumes. a) Recall that $\mathbb{R}^n$ carries the **Lebesgue measure**, where a subset $X \subseteq V$ is called **measurable**, if the integral $\mathrm{vol}(X) := \int_X 1 \in \mathbb{R} \dot\cup \{\infty\}$ with respect to the Lebesgue measure exists; in this case it is also called the **(n-dimensional) volume** of X. The Lebesgue measure is **countably additive**, is translation invariant, scales under linear transformations according to the absolute determinant, thus in particular is invariant under rotations and reflections. Finally, the above Lebesgue integral and the Riemann integral coincide whenever the latter is defined.

Let V be an Euclidean $\mathbb{R}$-vector space, such that $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$. Identifying V with $\mathbb{R}^n$ as Euclidean $\mathbb{R}$-vector spaces, by specifying an orthonormal $\mathbb{R}$-basis, we get a measure on V, independently of the particular choice of basis, sharing the above properties. For example, any (open) sphere $B_r^\circ(0) \subseteq B_r(0) \subseteq V$, where $r \geq 0$, is measurable such that $\mathrm{vol}(B_r^\circ(0)) = \mathrm{vol}(B_r(0)) \in \mathbb{R}$, where for $n = 1$ we have $\mathrm{vol}(B_r(0)) = 2r$, for $n = 2$ we have $\mathrm{vol}(B_r(0)) = \pi r^2$, and more generally for $n = 2m$ we have $\mathrm{vol}(B_r(0)) = \frac{(\pi r^2)^m}{m!}$.

b) Let $\Lambda := \langle \mathcal{B} \rangle_{\mathbb{Z}} \subseteq V$ be a lattice, where $\mathcal{B} \subseteq V$ is $\mathbb{R}$-linearly independent, and let $\mathcal{F}_{\mathcal{B}} \subseteq V$ be the associated fundamental domain. The parallelotope $\mathcal{F}_{\mathcal{B}}$ is measurable and bounded, thus $\mathrm{vol}(\mathcal{F}_{\mathcal{B}}) \in \mathbb{R}$ is defined. If Λ is not full, then $\mathcal{F}_{\mathcal{B}} \subseteq \langle \mathcal{B} \rangle_{\mathbb{R}} < V$ is contained in a proper $\mathbb{R}$-subspace, so that the (n-dimensional) volume of $\mathcal{F}_{\mathcal{B}}$ is $\mathrm{vol}(\mathcal{F}_{\mathcal{B}}) = 0$.

Hence let Λ be full, that is $\mathcal{B} \subseteq V$ is an $\mathbb{R}$-basís. Writing $\mathcal{B}$ in terms of an orthonormal $\mathbb{R}$-basis $\mathcal{C} \subseteq V$, and letting $B \in \mathrm{GL}_n(\mathbb{R})$ be the associated base change matrix, the interpretation of the matrix determinant as an alternating multi-linear 'volume' form entails $\mathrm{vol}(\mathcal{F}_{\mathcal{B}}) = |\det(B)|$. Moreover, the Gram matrix of V with respect to $\mathcal{B}$ is given as $\Gamma_{\mathcal{B}} = B \cdot \Gamma_{\mathcal{C}} \cdot B^{\mathrm{tr}} = BB^{\mathrm{tr}} \in \mathbb{R}^{n \times n}$, hence we get $\mathrm{disc}(\mathcal{B}) = \det(\Gamma_{\mathcal{B}}) = \det(BB^{\mathrm{tr}}) = \det(B)^2 = \mathrm{vol}(\mathcal{F}_{\mathcal{B}})^2 \in \mathbb{R}$.

If $\Lambda' \leq \Lambda$ is a full sublattice, having $\mathbb{Z}$-basis $\mathcal{B}'$, for the associated base change matrix $B' \in \mathrm{GL}_n(\mathbb{R})$ with respect to $\mathcal{C}$ we have $B' = AB$, where $A \in \mathrm{GL}_n(\mathbb{R}) \cap \mathbb{Z}^{n \times n}$ is the base change matrix obtained from writing $\mathcal{B}'$ in terms of $\mathcal{B}$. Since Λ/Λ' is a finite Abelian group, we have $|\det(A)| = [\Lambda \colon \Lambda']$. This entails $\mathrm{vol}(\mathcal{F}_{\mathcal{B}'}) = |\det(B')| = |\det(AB)| = |\det(A)| \cdot |\det(B)| = [\Lambda \colon \Lambda'] \cdot \mathrm{vol}(\mathcal{F}_{\mathcal{B}}) \in \mathbb{R}$. Similarly, we have $\Gamma_{\mathcal{B}'} = A \cdot \Gamma_{\mathcal{B}} \cdot A^{\mathrm{tr}} \in \mathbb{R}^{n \times n}$, hence $\mathrm{disc}(\mathcal{B}') = \det(\Gamma_{\mathcal{B}'}) = \det(A)^2 \cdot \det(\Gamma_{\mathcal{B}}) = [\Lambda \colon \Lambda']^2 \cdot \mathrm{disc}(\mathcal{B}) \in \mathbb{R}$.

In particular, in the case $\Lambda' = \Lambda$, that is $B \in \mathrm{GL}_n(\mathbb{Z})$, we get $\mathrm{vol}(\mathcal{F}_{\mathcal{B}'}) = \mathrm{vol}(\mathcal{F}_{\mathcal{B}})$ and $\mathrm{disc}(\mathcal{B}') = \mathrm{disc}(\mathcal{B})$, saying that both the volume of a fundamental domain and the discriminant of $\mathcal{B}$ only depend on Λ, so that we may define the **volume** and the **discriminant** of Λ as $\mathrm{vol}(\Lambda) := \mathrm{vol}(\mathcal{F}_{\mathcal{B}}) \in \mathbb{R}$ and $\mathrm{disc}(\Lambda) := \mathrm{disc}(\mathcal{B}) \in \mathbb{R}$, respectively, where we have $\mathrm{disc}(\Lambda) = \mathrm{vol}(\Lambda)^2$.

(Actually, it would be more appropriate to call $\mathrm{vol}(\mathcal{F}_{\mathcal{B}})$ the volume of the **torus** V/Λ, which is compact as an Abelian topological group; see also Table 5.)

Example. i) For $\mathbb{Z}^n \subseteq \mathbb{R}^n$ we may choose the standard $\mathbb{R}$-basis $\mathcal{B}$, yielding $\mathcal{F}_{\mathcal{B}} = \{[x_1, \ldots, x_n] \in \mathbb{R}^n; 0 \leq x_i < 1\}$, and thus we get $\mathrm{vol}(\mathbb{Z}^n) = \mathrm{vol}(\mathcal{F}_{\mathcal{B}}) =$

$|\det(E_n)| = 1$ (which is not really a surprise).

For the full sublattice $\Lambda_{A_1^n} := (2\mathbb{Z})^n \subseteq \mathbb{Z}^n$ of index $[\mathbb{Z}^n \colon \Lambda_{A_1^n}] = 2^n$, being called the **root lattice** of **Dynkin type** A_1^n, we get $\mathrm{vol}(\Lambda_{A_1^n}) = |\det(2 \cdot E_n)| = 2^n$.

ii) Let $\mathcal{H}_n := \{[x_1, \ldots, x_{n+1}] \in \mathbb{R}^{n+1}; \sum_{i=1}^{n+1} x_i = 0\} \leq \mathbb{R}^{n+1}$, and let $\Lambda_{A_n} := \mathcal{H}_n \cap \mathbb{Z}^{n+1}$. Then Λ_{A_n} is a discrete subgroup, that is a lattice, being called the **root lattice** of **Dynkin type** A_n. Moreover, let $\mathcal{B}_{n+1} = \{\epsilon_1, \ldots, \epsilon_{n+1}\} \subseteq \mathbb{R}^{n+1}$ be the standard $\mathbb{R}$-basis, let $\alpha_i := \epsilon_i - \epsilon_{i+1} \in \mathbb{R}^{n+1}$ for $i \in \{1, \ldots, n\}$, and let $\mathcal{R}_n := \{\alpha_1, \ldots, \alpha_n\}$ be the set of **fundamental roots**, which is an $\mathbb{R}$-basis of $\mathcal{H}_n$. Then we have $\Lambda_{A_n} := \langle \mathcal{R}_n \rangle_{\mathbb{Z}}$, so that Λ_{A_n} is a full lattice in $\mathcal{H}_n$.

Restricting the standard scalar product on $\mathbb{R}^{n+1}$ to $\mathcal{H}_n$, with respect to the $\mathbb{R}$-basis $\mathcal{R}_n \subseteq \mathcal{H}_n$ we get the Gram matrix $\Gamma_{\mathcal{R}_n} \in \mathbb{R}^{n \times n}$, where

$$[\Gamma_{\mathcal{R}_n}]_{ij} = \langle \alpha_i, \alpha_j \rangle = \begin{cases} 2, & \text{if } i = j, \\ -1, & \text{if } |i-j| = 1, \\ 0, & \text{if } |i-j| \geq 2. \end{cases}$$

In particular, letting $0 \leq \varphi_i \leq \pi$ be the angle between α_i and α_{i+1}, we have $\cos(\varphi_i) = \frac{\langle \alpha_i, \alpha_{i+1} \rangle}{\sqrt{\langle \alpha_i, \alpha_i \rangle \langle \alpha_{i+1}, \alpha_{i+1} \rangle}} = -\frac{1}{2}$, thus $\varphi_i = \frac{2\pi}{3}$.

We determine $\mathrm{disc}(\Lambda_{A_n}) = \det(\Gamma_{\mathcal{R}_n}) = \mathrm{vol}(\mathcal{F}_{\mathcal{R}_n})^2$, where the latter is an n-dimensional volume: Letting $\alpha_0 := \sum_{i=1}^{n+1} \epsilon_i \in \mathbb{R}^{n+1}$, we have $\mathcal{H}_n^{\perp} = \langle \alpha_0 \rangle \leq \mathbb{R}^{n+1}$ and $\langle \alpha_0, \alpha_0 \rangle = n+1$, hence we get $\mathrm{vol}(\mathcal{F}_{\mathcal{R}_n}) = \frac{1}{\sqrt{n+1}} \cdot \mathrm{vol}(\mathcal{F}_{\mathcal{R}_n \dot\cup \{\alpha_0\}})$, where the latter now is an $(n+1)$-dimensional volume. Writing $\mathcal{R}_n \mathbin{\dot\cup} \{\alpha_0\}$ in terms of $\mathcal{B}_{n+1}$, from

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ -1 & -2 & \ldots & -n & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ 1 & 1 & \ldots & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 & & & \\ & 1 & -1 & & \\ & & \ddots & \ddots & \\ & & & 1 & -1 \\ & & & & n+1 \end{bmatrix}$$

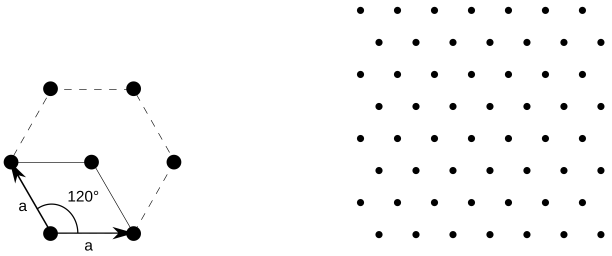
we get $\mathrm{vol}(\mathcal{F}_{\mathcal{R}_n \dot\cup \{\alpha_0\}}) = n+1$, hence $\mathrm{vol}(\mathcal{F}_{\mathcal{R}_n}) = \sqrt{n+1}$, thus $\mathrm{disc}(\Lambda_{A_n}) = n+1$.

In particular, for $n = 2$ we get the **hexagonal** or **triangular lattice**, see Table 4: With respect to an orthonormal $\mathbb{R}$-basis of $\mathcal{H}_2$, since $\langle \alpha_1, \alpha_1 \rangle = 2 = \langle \alpha_2, \alpha_2 \rangle$ and $\langle \alpha_1, \alpha_2 \rangle = -1$, we may choose $\alpha_1 := [\sqrt{2}, 0] \in \mathbb{R}^2$ and $\alpha_2 := \frac{1}{\sqrt{2}} \cdot [-1, \sqrt{3}] \in \mathbb{R}^2$; then we indeed have $\frac{1}{\sqrt{2}} \cdot \det\left(\begin{bmatrix} \sqrt{2} & 0 \\ -1 & \sqrt{3} \end{bmatrix} \right) = \sqrt{3}$.

(7.4) The Lattice Point Theorem. Let V be an Euclidean $\mathbb{R}$-vector space, where $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$, and let $\Lambda \subseteq V$ be a full lattice.

A subset $X \subseteq V$ is called **convex**, if whenever $v, w \in X$ then the straight line segment $\{(1-t)v + tw \in V; 0 \leq t \leq 1\}$ between v and w is completely contained in X as well. In particular, any convex set is measurable [Minkowski, 1910].

Table 4: The hexagonal lattice.



A subset $X \subseteq V$ is called **centrally symmetric**, if whenever $v \in X$ then we have $-v \in X$ as well. In particular, and any non-empty, convex, and centrally symmetric set contains the origin. For example, any (open) sphere $B_r^\circ(0) \subseteq B_r(0) \subseteq \mathbb{R}^n$ is convex and centrally symmetric.

Theorem: Lattice Point Theorem [Minkowski, 1910]**.**
i) Any (measurable) convex and centrally symmetric subset $X \subseteq V$ such that $\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(\Lambda)$ contains a non-zero lattice point in Λ.
ii) If X is additionally compact, then it suffices to assume $\mathrm{vol}(X) \geq 2^n \cdot \mathrm{vol}(\Lambda)$.

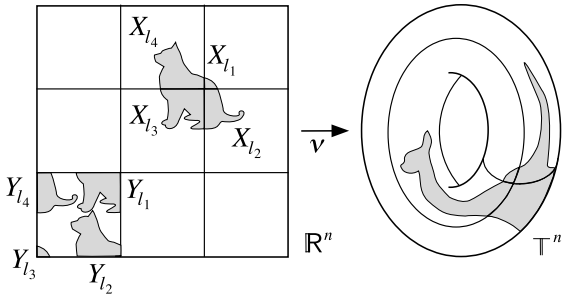
Proof. i) Assume the strict inequality, and let $\mathcal{F} \subseteq V$ be a fundamental domain for Λ; then we have $V = \coprod_{v\in\Lambda}(v+\mathcal{F})$. Let $Y := \frac{1}{2}X := \{\frac{1}{2}u \in V; u \in X\}$. Thus from $Y = \coprod_{v\in\Lambda}(Y \cap (v+\mathcal{F}))$ we get $\mathrm{vol}(\mathcal{F}) = \mathrm{vol}(\Lambda) < \frac{1}{2^n} \cdot \mathrm{vol}(X) = \mathrm{vol}(Y) = \sum_{v\in\Lambda} \mathrm{vol}(Y \cap (v+\mathcal{F})) = \sum_{v\in\Lambda} \mathrm{vol}((Y-v) \cap \mathcal{F})$. Assume that the latter pieces $(Y-v)\cap\mathcal{F}$ are pairwise disjoint, for $v \in \Lambda$, then we have $\coprod_{v\in\Lambda}((Y-v)\cap\mathcal{F}) \subseteq \mathcal{F}$, entailing $\sum_{v\in\Lambda} \mathrm{vol}((Y-v)\cap\mathcal{F}) = \mathrm{vol}(\coprod_{v\in\Lambda}((Y-v)\cap\mathcal{F})) \leq \mathrm{vol}(\mathcal{F})$, a contradiction; see also Table 5.

Hence there are $v, w \in \Lambda$ such that $v \neq w$ and $(Y-v)\cap(Y-w) \neq \emptyset$. Thus we have $0 \neq v - w \in \Lambda$, and there are $u, u' \in X$ such that $\frac{1}{2}u - v = \frac{1}{2}u' - w$. Since X is centrally symmetric and convex, we have $-u' \in X$, hence $\{(1-t)u - tu' \in V; 0 \leq t \leq 1\} \subseteq X$. Thus for $t = \frac{1}{2}$ we get $\frac{1}{2}(u-u') = v - w \in X$.

ii) Let X be compact, that is closed and bounded, and assume the weaker inequality. For $k \in \mathbb{N}$ let $X_k := (1+\frac{1}{k})X \subseteq V$; hence X_k is (measurable) convex and centrally symmetric. Moreover, since $0 \in X_k$ and X_k is convex we have $X = \frac{k}{k+1}X_k \subseteq X_k$, entailing $X \subseteq \cdots \subseteq X_k \subseteq \cdots \subseteq X_2 \subseteq X_1 = 2X$.

Since $\mathrm{vol}(X_k) = (1+\frac{1}{k})^n \cdot \mathrm{vol}(X) > \mathrm{vol}(X) \geq 2^n \cdot \mathrm{vol}(\Lambda)$, by i) there is $0 \neq v_k \in X_k \cap \Lambda$, for all $k \in \mathbb{N}$. Since $\mathcal{V} := \{v_k \in \Lambda; k \in \mathbb{N}\} \subseteq X_1$ is bounded, and Λ is discrete, we conclude that $\mathcal{V}$ is finite. Hence we may assume that $\mathcal{V}$ is a singleton set, that is there is $0 \neq v \in \Lambda$ such that $v \in \bigcap_{k\in\mathbb{N}} X_k$. Thus there are $w_k \in X$ such that $v = (1+\frac{1}{k})w_k$, for all $k \in \mathbb{N}$. This yields $\|v - w_k\| = \frac{1}{k} \cdot \|w_k\|$,

Table 5: The quotient torus modulo a lattice.



---

since X is bounded entailing $\lim_{k\to\infty} w_k = v$. Thus $v \in \overline{X}$, where the latter denotes the closure of X in V, and since X is closed we infer $v \in X$. ♯

We present two immediate applications:

(7.5) Primes as sums of two squares. We have seen in (1.5) that any prime $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod 4$ is a sum of two squares in $\mathbb{Z}$. We present an alternative proof of this assertion using Minkowski's Theorem:

Let $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod p$, that is u is a primitive 4-th root of unity modulo p, and let $\Lambda := \{[a,b] \in \mathbb{Z}^2; b \equiv ua \pmod p\} \subseteq \mathbb{Z}^2 \subseteq \mathbb{R}^2$. Then Λ is an additive subgroup of $\mathbb{Z}^2$, where $(p\mathbb{Z})^2 \subseteq \Lambda \subseteq \mathbb{Z}^2$ shows that Λ is a full sublattice, such that $[\mathbb{Z}^2\colon \Lambda] \mid p^2$. Since for any $a \in \mathbb{Z}/p\mathbb{Z}$ there is a unique $b \in \mathbb{Z}/p\mathbb{Z}$ such that $b = ua \in \mathbb{Z}/p\mathbb{Z}$, we conclude that $[\Lambda\colon (p\mathbb{Z})^2] = p$, so that $[\mathbb{Z}^2\colon \Lambda] = p$. Hence we have $\mathrm{vol}(\Lambda) = \mathrm{vol}(\mathbb{Z}^2) \cdot [\mathbb{Z}^2\colon \Lambda] = p$.

We consider the compact disc $B_r(0)$, having volume $\mathrm{vol}(B_r(0)) = \pi r^2$. For $r := \sqrt{\frac{4p}{\pi}}$ we have $\pi r^2 = 4p$, thus by Minkowski's Theorem there is $0 \neq [a,b] \in \Lambda \cap B_r(0)$. Hence we have $0 \neq a^2 + b^2 \leq r^2 = \frac{4p}{\pi} < 2p$. Moreover, $a^2 + b^2 = a^2 + (ua)^2 = a^2 - a^2 = 0 \in \mathbb{Z}/p\mathbb{Z}$ shows that $p \mid a^2 + b^2$, entailing $a^2 + b^2 = p$. ♯

Example. i) For $p := 5$ we get $r = \sqrt{\frac{4\cdot 5}{\pi}} \sim 2.52$, hence $r^2 = \frac{4\cdot 5}{\pi} \sim 6.37$, and letting $u := 2$ we find $[a,b] \in \{\pm[1,2], \pm[2,-1]\} \subseteq \Lambda$ fulfilling $0 < a^2 + b^2 \leq r^2$. **ii)** For $p := 13$ we get $r = \sqrt{\frac{4\cdot 13}{\pi}} \sim 4.07$, hence $r^2 = \frac{4\cdot 13}{\pi} \sim 16.55$, and letting $u := 5$ we find $[a,b] \in \{\pm[2,-3], \pm[3,2]\} \subseteq \Lambda$ fulfilling $0 < a^2 + b^2 \leq r^2$.

(7.6) Integers as sums of four squares. We have already seen in (1.7) that there are infinitely many primes (or likewise integers) which can be written as a sum of two squares in $\mathbb{Z}$, and infinitely many positive primes (or likewise positive

integers) which cannot. Hence we wonder whether allowing for more summands changes the picture, and so we may ask whether there is a fixed number $s \in \mathbb{N}$ such that any positive integer can be written as a sum of s squares in $\mathbb{Z}$.

Since for any $a \in \mathbb{Z}$ we have $a^2 \equiv \{0, 1, 4\} \pmod 8$, we have $a^2 + b^2 + c^2 \not\equiv 7 \pmod 8$, for any $a, b, c \in \mathbb{Z}$, so that no positive integer n such that $n \equiv 7 \pmod 8$ can be written as a sum of three squares in $\mathbb{Z}$. Thus, we conclude that $s \geq 4$, if it exists at all. Indeed, we have the following:

Theorem: Four-squares Theorem [Lagrange, 1770]**.**
a) Any positive integer can be written as a sum of four squares in $\mathbb{Z}$.
b) Any odd prime $p \in \mathcal{P}_{\mathbb{Z}}$ has precisely $8(p+1)$ representations as a sum of four squares in $\mathbb{Z}$, where sign changes and reorderings are considered distinct.

(From this, it is not too difficult to determine the number of representations for arbitrary positive integers, but we shall not present this here.)

Proof. i) Let $\mathbb{H}$ be the (non-commutative) skew field of **Hamilton quaternions [1856]** or **hypercomplex numbers**, being as a $\mathbb{Q}$-algebra generated by elements $\{i, j\} \subseteq \mathbb{H}$, subject to the relations $i^2 = j^2 = -1$ and $ij = -ji$. Then $\mathbb{H}$ has $\mathbb{Q}$-basis $\mathcal{B} := \{1, i, j, k\}$ where $k := ij \in \mathbb{H}$. The regular representation $\rho\colon \mathbb{H} \to \mathbb{Q}^{4\times 4}$ gives rise to the multiplicative map $\rho \cdot \det\colon \mathbb{H} \to \mathbb{Q}$.

With respect to the $\mathbb{Q}$-basis $\mathcal{B} \subseteq \mathbb{H}$ the regular representation reads

$$\rho(i) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},\ \rho(j) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},\ \rho(k) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

Thus for $Q := a + bi + cj + dk \in \mathbb{H}$, where $a, b, c, d \in \mathbb{Q}$, we get $\det(\rho(Q)) = (a^2+b^2+c^2+d^2)^2$, so that the positive definite (reduced) **quaternionic norm** $N_{\mathbb{H}}(Q) := \sqrt{\det(\rho(Q))} = a^2 + b^2 + c^2 + d^2 \in \mathbb{Q}$ is multiplicative as well. (The quaternions having integral norm are also called **Hurwitz quaternions**.)

This shows that whenever $n, m \in \mathbb{Z}$ such that $n = a^2 + b^2 + c^2 + d^2$ and $m = x^2+y^2+z^2+w^2$ are both sums of four squares, where $a, b, c, d, x, y, z, w \in \mathbb{Z}$, then letting $Q := a+bi+cj+dk \in \mathbb{H}$ and $\widetilde{Q} := x+yi+zj+wk \in \mathbb{H}$ we have $Q\widetilde{Q} = (ax-by-cz-dw)+(ay+bx+cw-dz)i+(az-bw+cx+dy)j+(aw+bz-cy+dx)k$, so that $nm = N_{\mathbb{H}}(Q)N_{\mathbb{H}}(\widetilde{Q}) = N_{\mathbb{H}}(Q\widetilde{Q})$ is a sum of four squares in $\mathbb{Z}$.

ii) Hence it suffices to consider $p \in \mathcal{P}_{\mathbb{Z}}$, where since $2 = 1^2+1^2+0^2+0^2$ we may assume that p is odd: For $a, b \in \mathbb{Z}$ let $M(a, b) := \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{Z}^{2\times 2}$. Recalling that $M(a, b)$ is the matrix of the regular action of $a + ib$ with respect to the $\mathbb{Z}$-basis $\{1, i\} \subseteq \mathbb{Z}[i]$, we get $M(a, b) \cdot M(u, v) = M(au - bv, av + bu) = M(u, v) \cdot M(a, b)$, and $\det(M(a, b)) = a^2 + b^2$, and $M(a, b) \cdot M(a, -b) = (a^2 + b^2) \cdot E_2$.

We now compute in $\mathbb{Z}/p\mathbb{Z}$: Let $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$ such that $a^2 + b^2 = -(c^2 + d^2)$, and assume that $a^2 + b^2 \neq 0$. Then we have $M(a, b) \in \mathrm{GL}_2(\mathbb{F}_p)$, such that

$M(a,b)^{-1} = \frac{1}{a^2+b^2} \cdot M(a,-b)$, and letting $M(u,v) := \frac{1}{a^2+b^2} \cdot M(a,-b) \cdot M(c,d) = \frac{1}{a^2+b^2} \cdot M(ac+bd, ad-bc)$, we get $M(c,d) = M(a,b) \cdot M(u,v)$, where $u^2+v^2 = \det(M(u,v)) = \frac{\det(M(c,d))}{\det(M(a,b))} = \frac{c^2+d^2}{a^2+b^2} = -1$.

Conversely, if $u, v \in \mathbb{Z}/p\mathbb{Z}$ such that $u^2+v^2 = -1$, then for any $a, b \in \mathbb{Z}/p\mathbb{Z}$ letting $M(c,d) := M(a,b) \cdot M(u,v)$ we get $c^2+d^2 = \det(M(c,d)) = \det(M(a,b)) \cdot \det(M(u,v)) = -(a^2+b^2)$. Thus the solutions of $a^2+b^2+c^2+d^2 = 0$ fulfill $a^2+b^2 = 0 = c^2+d^2$, or are related by some pair $[u,v]$ as above.

Since $((\mathbb{Z}/p\mathbb{Z})^*)^2 \dot\cup \{0\}$ has cardinality $\frac{p+1}{2}$, we have $\{x^2 \in \mathbb{Z}/p\mathbb{Z}; x \in \mathbb{Z}/p\mathbb{Z}\} \cap \{-y^2 - z \in \mathbb{Z}/p\mathbb{Z}; y \in \mathbb{Z}/p\mathbb{Z}\} \neq \emptyset$, for all $z \in \mathbb{Z}/p\mathbb{Z}$; in particular there are $u, v \in \mathbb{Z}/p\mathbb{Z}$ such that $u^2+v^2 = -1$. We count the number of such pairs $[u,v]$:

Let first $p \equiv -1 \pmod 4$; then we have $\mathbb{F}_{p^2} = \mathbb{F}_p[\zeta]$, where ζ is a primitive 4-th root of unity. Thus $M(u,v) \in \mathbb{F}_p^{2\times 2}$ is the matrix of the regular action of $u+\zeta v \in \mathbb{F}_{p^2}$ with respect to the $\mathbb{F}_p$-basis $\{1,\zeta\} \subseteq \mathbb{F}_{p^2}$. By the above, the associated determinant homomorphism $\det\colon \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$ is surjective, implying that in this case the number of the pairs equals $|\ker(\det)| = \frac{p^2-1}{p-1} = p+1$.

Let second $p \equiv 1 \pmod 4$; let $\zeta \in \mathbb{F}_p$ be a primitive 4-th root of unity. Then we have $u^2+v^2 = 0$ if and only if $v = \pm\zeta u$. Hence let $\mathcal{U} := \mathbb{F}_p^2 \setminus (\langle [1,\zeta] \rangle \cup \langle [1,-\zeta] \rangle)$, so that $|\mathcal{U}| = p^2-(2p-1) = (p-1)^2$. Then $\mathcal{U}$ becomes a group by transporting the group structure on $M(\mathcal{U}) \leq \mathrm{GL}_2(\mathbb{F}_p)$, so that by the above, we get a surjective group homomorphism $\det\colon \mathcal{U} \to \mathbb{F}_p^*\colon [u,v] \mapsto \det(M(u,v))$. This implies that in this case the number of the pairs equals $|\ker(\det)| = \frac{(p-1)^2}{p-1} = p-1$.

iii) We lift the above considerations to $\mathbb{Z}$: Note first that for any $a,b,c,d \in \mathbb{Z}$ such that $a^2+b^2+c^2+d^2 = p$ we have $|a|, |b|, |c|, |d| \leq \frac{p-1}{2}$: Assuming otherwise, we may replace a, say, by $a \pm p$ in order to get $0 < a^2+b^2+c^2+d^2 < p$, but still $a^2+b^2+c^2+d^2 \equiv 0 \pmod p$, a contradiction. Thus distinct solutions remain distinct upon reduction modulo p.

Moreover, if $p \equiv 1 \pmod 4$, then we have $p = a^2+b^2$ where $0 < a < b$ are unique, which allowing for sign changes and reordering amounts to 8 solutions. Allowing for $p = c^2+d^2$ as well, we get 16 solutions, apart from those for which $a^2+b^2 \neq 0 \neq c^2+d^2$ (which are all for $p \equiv -1 \pmod 4$ anyway).

To catch the latter, for p arbitrary, let $u, v \in \mathbb{Z}$ such that $u^2+v^2 \equiv -1 \pmod p$, and let $\Lambda = \Lambda(u,v) := \{[a,b,c,d] \in \mathbb{Z}^4; [c,d] \equiv [a,b] \cdot M(u,v) \pmod p\} \subseteq \mathbb{Z}^4 \subseteq \mathbb{R}^4$. Then Λ is an additive subgroup of $\mathbb{Z}^4$, where $(p\mathbb{Z})^4 \subseteq \Lambda \subseteq \mathbb{Z}^4$ shows that Λ is a full sublattice, such that $[\mathbb{Z}^4\colon \Lambda] \mid p^4$. Since for any $a, b \in \mathbb{Z}/p\mathbb{Z}$ there are unique $c, d \in \mathbb{Z}/p\mathbb{Z}$ such that $[c,d] \equiv [a,b] \cdot M(u,v) \pmod p$, we conclude that $[\Lambda\colon (p\mathbb{Z})^4] = p^2$, thus $[\mathbb{Z}^4\colon \Lambda] = p^2$. Hence we get $\mathrm{vol}(\Lambda) = \mathrm{vol}(\mathbb{Z}^4) \cdot [\mathbb{Z}^4\colon \Lambda] = p^2$.

We consider the sphere $B_r(0) \subseteq \mathbb{R}^4$, with volume $\mathrm{vol}(B_r(0)) = \frac{1}{2}\pi^2 r^4$. For $r := \sqrt[4]{\frac{32p^2}{\pi^2}}$ we have $\frac{1}{2}\pi^2 r^4 = 16p^2$, thus by Minkowski's Theorem there is $0 \neq [a,b,c,d] \in \Lambda \cap B_r(0)$, hence $0 \neq a^2+b^2+c^2+d^2 \leq r^2 = \sqrt{\frac{32p^2}{\pi^2}} = \frac{4p\cdot\sqrt{2}}{\pi} < 2p$.

Since we have $a^2+b^2+c^2+d^2 \equiv 0 \pmod p$, we get $a^2+b^2+c^2+d^2 = p$.

iv) We count the number of ways how p can be written as a sum of four squares in $\mathbb{Z}$: We fix $[u,v] \in \mathbb{Z}^2$ such that $|u|, |v| \leq \frac{p-1}{2}$ and $u^2+v^2 \equiv -1 \pmod p$; hence distinct choices of $[u,v]$ remain remain distinct upon reduction modulo p. Since for $[a,b,c,d] \in \Lambda(u,v)$ we have $M(u,v) \equiv M(a,b)^{-1} \cdot M(c,d) \pmod p$, we infer that for distinct choices of $[u,v]$ we get disjoint sets of solutions. Writing $\Lambda := \Lambda(u,v)$ again, and letting $X := X(u,v) \subseteq \Lambda$ be the (finite) subset consisting of its elements of norm p, we show that $|X| = 8$:

Let $0 \neq [a,b,c,d] \in X$. Considering the second row of $M(a,b)$ and $M(c,d)$ shows that $[b,-a,d,-c] \in \Lambda$ as well. Moreover, from $\frac{1}{c^2+d^2} \cdot M(c,-d) \cdot M(u,v) \equiv M(c,d)^{-1} \cdot M(u,v) \equiv M(a,b)^{-1} \equiv \frac{1}{a^2+b^2} \cdot M(a,-b) \pmod p$, we get $M(-c,d) \cdot M(u,v) \equiv M(a,-b) \pmod p$, saying that $[c,-d,-a,b] \in \Lambda$. Finally, combining these modifications we get $[d,c,-b,-a] \in \Lambda$. Thus we infer that $\pm\mathcal{B} \subseteq X$, where

$$\mathcal{B} := \{[a,b,c,d], [b,-a,d,-c], [c,-d,-a,b], [d,c,-b,-a]\} \subseteq X.$$

The elements of $\mathcal{B}$ are pairwise orthogonal, of norm p, hence we have $\operatorname{disc}(\mathcal{B}) = \det(\Gamma_{\mathcal{B}}) = p^4$, thus $\operatorname{vol}(\langle\mathcal{B}\rangle_{\mathbb{Z}}) = \sqrt{|\operatorname{disc}(\mathcal{B})|} = p^2 = \operatorname{vol}(\Lambda)$ shows that $\mathcal{B} \subseteq \Lambda$ is a $\mathbb{Z}$-basis. Hence writing $v \in X$ as a $\mathbb{Z}$-linear combination of the orthogonal set $\mathcal{B}$, from v having norm p as well, it follows that $v \in \pm\mathcal{B}$. Thus we have $X = \pm\mathcal{B}$.

In conclusion, taking the number of pairs $[u,v]$ into account, if $p \equiv -1 \pmod 4$ there are $8(p+1)$ representations of p as a sum of four squares in $\mathbb{Z}$; and if $p \equiv 1 \pmod 4$ there are $8(p-1)+16 = 8(p+1)$ such representations as well. ♯

Example. For $p := 71$ we get $r^2 = \frac{4 \cdot 7 \cdot \sqrt{2}}{\pi} \sim 127.8$. Then for example letting $[u,v] \in \{[4,14], [11,34]\}$ we find the following sets of solutions $X_{u,v}$:

$$\begin{aligned} X_{4,14} &= \pm\{[1,-5,3,-6], [3,6,-1,-5], [5,1,6,3], [6,-3,-5,1]\}, \\ X_{11,34} &= \pm\{[2,7,-3,3], [3,-3,-7,-2], [3,3,2,-7], [7,-2,3,3]]\}. \end{aligned}$$

There are precisely $\frac{p+1}{2} = 36$ pairs $[u,v]$ each, giving rise to the representations $p = 71 = 1^2+3^2+5^2+6^2$ and $p = 71 = 2^2+3^2+3^2+7^2$, up to signs and reordering, accounting for all $8(p+1) = 576$ representations.

8 Class groups

(8.1) Geometrical embeddings. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$. Fixing the algebraic closure of K in $\mathbb{C}$, we may consider $\operatorname{Inj}_{\mathbb{Q}}(K)$ as the set of field embeddings of K into $\mathbb{C}$. Given $\sigma \in \operatorname{Inj}_{\mathbb{Q}}(K)$, if $\operatorname{im}(\sigma) \subseteq \mathbb{R}$ then σ is called **real**, while otherwise it is called **non-real**.

Letting $\kappa \in \operatorname{Aut}_{\mathbb{R}}(\mathbb{C})$ denote complex conjugation, let $\overline{\sigma} := \sigma \cdot \kappa \in \operatorname{Inj}_{\mathbb{Q}}(K)$ be the **(complex) conjugate** of σ. Then σ is real if and only if we have $\overline{\sigma} = \sigma$. Let $\sigma_1, \ldots, \sigma_r \in \operatorname{Inj}_{\mathbb{Q}}(K)$ be the real embeddings, and let $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s \in \operatorname{Inj}_{\mathbb{Q}}(K)$ be the conjugate pairs of the non-real ones, where $r, s \in \mathbb{N}_0$ such that $r+2s = n$.

This gives rise to the monomorphism of commutative $\mathbb{Q}$-algebras

$$\widehat{\mathcal{G}}_{r,s}\colon K \to \mathbb{R}^r \oplus \mathbb{C}^s\colon \alpha \mapsto [\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_r}; \alpha^{\tau_1}, \ldots, \alpha^{\tau_s}].$$

Identifying $\mathbb{C} \to \mathbb{R}^2\colon z \mapsto [\mathrm{Re}(z), \mathrm{Im}(z)] = \frac{1}{2}[z + \overline{z}, z - \overline{z}]$, where conversely $z = \mathrm{Re}(z) + i \cdot \mathrm{Im}(z)$ and $\overline{z} = \mathrm{Re}(z) - i \cdot \mathrm{Im}(z)$, we get the embedding

$$\mathcal{G}_{r,s}\colon K \to \mathbb{R}^n\colon \alpha \mapsto [\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_r}, \mathrm{Re}(\alpha^{\tau_1}), \mathrm{Im}(\alpha^{\tau_1}), \ldots, \mathrm{Re}(\alpha^{\tau_s}), \mathrm{Im}(\alpha^{\tau_s})],$$

where $\mathbb{R}^n$ is called the associated **geometric space**, and carries the structure of a commutative $\mathbb{Q}$-algebra, which is inherited from $\mathbb{R}^r \oplus \mathbb{C}^s$.

Theorem. Let $\mathcal{O} := \mathcal{O}_K$ be the ring of integers of K. Then $\Lambda_K = \Lambda_{\mathcal{O}} := \mathcal{G}_{r,s}(\mathcal{O}) \subseteq \mathbb{R}^n$ is a full lattice having volume $\mathrm{vol}(\Lambda_K) = (\frac{1}{2})^s \cdot \sqrt{|\mathrm{disc}(K)|}$.

Proof. Let $\mathcal{B} \subseteq \mathcal{O}$ be an integral basis. Then we have $\Lambda_K = \langle \mathcal{G}_{r,s}(\mathcal{B}) \rangle_{\mathbb{Z}} \subseteq \mathbb{R}^n$, and we have to show that $\mathcal{G}_{r,s}(\mathcal{B})$ is $\mathbb{R}$-linearly independent: To this end, letting $A := [\mathcal{G}_{r,s}(\omega) \in \mathbb{R}^n; \omega \in \mathcal{B}]^{\mathrm{tr}} \in \mathbb{R}^{n \times n}$, we get (the right hand factor being a block diagonal matrix)

$$A \cdot \big(E_r \oplus \bigoplus_{j=1}^{s} \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}\big) = [\omega^{\sigma_1}, \ldots, \omega^{\sigma_r}, \omega^{\tau_1}, \omega^{\overline{\tau}_1}, \ldots, \omega^{\tau_s}, \omega^{\overline{\tau}_s}]^{\mathrm{tr}}_{\omega \in \mathcal{B}} = \Delta_{\mathcal{B}},$$

thus $\det(A) \cdot \det\big(\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}\big)^s = (-2i)^s \cdot \det(A) = \det(\Delta_{\mathcal{B}}) \neq 0$. Thus we conclude that Λ_K is a full lattice, for which from $\mathrm{disc}(K) = \mathrm{disc}(\mathcal{O}) = \det(\Delta_{\mathcal{B}})^2$ we get $\mathrm{vol}(\Lambda_K) = |\det(A)| = (\frac{1}{2})^s \cdot |\det(\Delta_{\mathcal{B}})| = (\frac{1}{2})^s \cdot \sqrt{|\mathrm{disc}(K)|}$. ♯

Corollary. Let $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$. Then $\Lambda_{\mathfrak{a}} := \mathcal{G}_{r,s}(\mathfrak{a}) \subseteq \Lambda_K$ is a full sublattice having volume $\mathrm{vol}(\Lambda_{\mathfrak{a}}) = (\frac{1}{2})^s \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{a})$.

Proof. The ideal $\mathfrak{a} \subseteq \mathcal{O}$ is a free Abelian subgroup of rank n, having finite index $[\mathcal{O}\colon \mathfrak{a}] = N(\mathfrak{a})$. Since $\mathcal{G}_{r,s}$ is a $\mathbb{Z}$-linear embedding, $\Lambda_{\mathfrak{a}} \subseteq \Lambda_K$ has index $N(\mathfrak{a})$, hence is a full sublattice with volume $\mathrm{vol}(\Lambda_{\mathfrak{a}}) = N(\mathfrak{a}) \cdot \mathrm{vol}(\Lambda_K)$. ♯

Corollary. The sign of $\mathrm{disc}(K) \in \mathbb{Z}$ is given as $(-1)^s$.

Proof. We have $\det(\Delta_{\mathcal{B}})^2 = (-1)^s \cdot 4^s \cdot \det(A)^2$, where $\det(A) \in \mathbb{R}$. ♯

(8.2) Geometric spaces. a) Let $n \in \mathbb{N}$, and let $r, s \in \mathbb{N}_0$ such that $n := r + 2s$; thus we exclude the case $r = s = 0$. We consider the map

$$L_{r,s}\colon \mathbb{R}^n \to \mathbb{R}\colon [x_1, \ldots, x_n] \mapsto \sum_{i=1}^{r} |x_i| + 2 \cdot \sum_{j=1}^{s} \sqrt{x_{r+2j-1}^2 + x_{r+2j}^2}.$$

Then $L_{r,s}$ is positive definite; we have proportionality $L_{r,s}(tv) = |t| \cdot L_{r,s}(v)$, for all $t \in \mathbb{R}$ and $v \in \mathbb{R}^n$; and since the summands fulfill the triangle inequality, the same holds for $L_{r,s}$. Hence $L_{r,s}$ is a norm on $\mathbb{R}^n$ (in the topological sense).

b) For $u \geq 0$ let $X := X_{r,s}(u) := \{v \in \mathbb{R}^n; L_{r,s}(v) \leq u\}$; for the case $r = 2$ and $s = 0$ the set $X_{2,0}(1)$, say, is depicted as region B in Table 6.

Then X is bounded (with respect to the Euclidean norm); since $L_{r,s}$ is continuous X is closed, thus X is compact; by proportionality X is centrally symmetric; and by proportionality and the triangle inequality, for $v, w \in X$ and $0 \leq t \leq 1$ we have $L_{r,s}((1-t)v + tw) \leq (1-t)L_{r,s}(v) + tL_{r,s}(w) \leq (1-t)u + tu = u$, thus $(1-t)v + tw \in X$ as well, thus X is convex. In particular, $\mathrm{vol}(X) \in \mathbb{R}$ exists.

Lemma. We have $\mathrm{vol}(X_{r,s}(u)) = \frac{u^n}{n!} \cdot 2^r (\frac{\pi}{2})^s$.

Proof. Let $\gamma_{r,s}(u) := \mathrm{vol}(X_{r,s}(u))$, considered as a function in $u \geq 0$. Then we have $\gamma_{r,s}(u) = u^{r+2s} \cdot \gamma_{r,s}(1)$. We have to show that $\gamma_{r,s}(1) = \frac{1}{(r+2s)!} \cdot 2^r (\frac{\pi}{2})^s$:

We proceed by induction on $r + s \in \mathbb{N}_0$, where for $r = s = 0$ we additionally let $\gamma_{0,0}(1) := 1$, while for $r = 1$ and $s = 0$ we have $\gamma_{1,0}(1) = 2$, and for $r = 0$ and $s = 1$ we have $\gamma_{0,1}(1) = \frac{\pi}{4} = \frac{\pi}{2} \cdot \frac{1}{2!}$ indeed. Hence let now $r + s \geq 2$:

If $r \geq 1$ (and thus $s \geq 1$ if $r = 1$) then $\gamma_{r,s}(1) = 2 \cdot \int_{0 \leq t \leq 1} \gamma_{r-1,s}(1-t) = 2\gamma_{r-1,s}(1) \cdot \int_{0 \leq t \leq 1} (1-t)^{r+2s-1} = \frac{2}{r+2s} \cdot \gamma_{r-1,s}(1)$. Hence by induction we get $\gamma_{r,s}(1) = \frac{2}{r+2s} \cdot \frac{1}{(r+2s-1)!} \cdot 2^{r-1} (\frac{\pi}{2})^s = \frac{1}{(r+2s)!} \cdot 2^r (\frac{\pi}{2})^s$.

If $r = 0$ and $s \geq 2$ then $\gamma_{0,s}(1) = \int_{0 \leq t^2+u^2 \leq \frac{1}{4}} \gamma_{0,s-1}(1 - 2 \cdot \sqrt{t^2+u^2}) = \gamma_{0,s-1}(1) \cdot \int_{0 \leq t^2+u^2 \leq \frac{1}{4}} (1 - 2 \cdot \sqrt{t^2+u^2})^{2s-2}$. Using polar coordinates $t = \rho\cos(\varphi)$ and $u = \rho\sin(\varphi)$, having Jacobian $|\det\left(\begin{bmatrix} \frac{\partial t}{\partial \varphi} & \frac{\partial t}{\partial \rho} \\ \frac{\partial u}{\partial \varphi} & \frac{\partial u}{\partial \rho} \end{bmatrix}\right)| = |\det\left(\begin{bmatrix} -\rho\sin(\varphi) & \cos(\varphi) \\ \rho\cos(\varphi) & \sin(\varphi) \end{bmatrix}\right)| = \rho$, we get $\gamma_{0,s}(1) = \gamma_{0,s-1}(1) \cdot \int_{0 \leq \varphi \leq 2\pi} \int_{0 \leq \rho \leq \frac{1}{2}} (1-2\rho)^{2s-2} \rho = 2\pi\gamma_{0,s-1}(1) \cdot \int_{0 \leq \rho \leq \frac{1}{2}} (1-2\rho)^{2s-2} \rho$. Letting $\rho = \frac{1}{2}(1-\vartheta)$ we get $\gamma_{0,s}(1) = \frac{\pi}{2}\gamma_{0,s-1}(1) \cdot \int_{0 \leq \vartheta \leq 1} \vartheta^{2s-2}(1-\vartheta) = \frac{\pi}{2}\gamma_{0,s-1}(1)(\frac{1}{2s-1} - \frac{1}{2s}) = \frac{\pi}{2} \cdot \frac{1}{2s(2s-1)} \cdot \gamma_{0,s-1}(1)$. Hence by induction we get $\gamma_{0,s}(1) = \frac{\pi}{2} \cdot \frac{1}{2s(2s-1)} \cdot \frac{1}{(2s-2)!} \cdot (\frac{\pi}{2})^{s-1} = \frac{1}{(2s)!} \cdot (\frac{\pi}{2})^s$. ♯

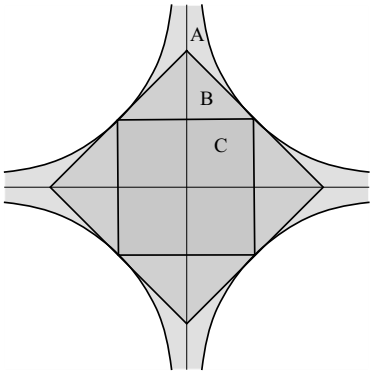
c) Recalling that $\mathbb{R}^n$ may be equipped with the structure of a commutative $\mathbb{Q}$-algebra, which is inherited from $\mathbb{R}^r \oplus \mathbb{C}^s$, we get the multiplicative map

$$N_{r,s} \colon \mathbb{R}^n \to \mathbb{R} \colon [x_1, \ldots, x_n] \mapsto \prod_{i=1}^{r} x_i \cdot \prod_{j=1}^{s} (x_{r+2j-1}^2 + x_{r+2j}^2).$$

In particular, for $t \in \mathbb{R}$ and $v \in \mathbb{R}^n$ we have $N_{r,s}(tv) = t^{r+2s} N_{r,s}(v) = t^n N_{r,s}(v)$.

For the case $r = 2$ and $s = 0$ the set $N_{2,0}^{-1}(\{t \in \mathbb{R}; 0 \leq t \leq 1\})$, say, is depicted as region A in Table 6, in particular showing that these set are not convex. Hence, in order to be able to apply Minkowski's Theorem, we relate these sets

Table 6: Convex and non-convex regions.



---

to those of shape $X_{r,s}(1)$, which are convex indeed. (There are other choices of suitable convex sets, such as region C in Table 6, which work fine as well, but yield weaker bounds; see Exercise (14.30).)

Theorem: Minkowski bound. Let $M_{r,s} := \frac{n!}{n^n} \cdot (\frac{4}{\pi})^s \in \mathbb{R}$ be **Minkowski's constant**. Then any full lattice $\Lambda \subseteq \mathbb{R}^n$ contains a lattice point $0 \neq v \in \Lambda$ such that $|N_{r,s}(v)| \leq 2^s \cdot M_{r,s} \cdot \mathrm{vol}(\Lambda)$.

Proof. i) Let first $X \subseteq \mathbb{R}^n$ be compact, convex, and centrally symmetric such that $\mathrm{vol}(X) > 0$ and any $w \in X$ fulfills $|N_{r,s}(w)| \leq 1$. We show that there is $0 \neq v \in \Lambda$ such that $|N_{r,s}(v)| \leq 2^n \cdot \frac{\mathrm{vol}(\Lambda)}{\mathrm{vol}(X)}$:

Let $c := 2 \cdot \sqrt[n]{\frac{\mathrm{vol}(\Lambda)}{\mathrm{vol}(X)}} \in \mathbb{R}$. Then the set $(cX) \subseteq \mathbb{R}^n$ is compact, convex, and centrally symmetric, such that $\mathrm{vol}(cX) = c^n \cdot \mathrm{vol}(X) = 2^n \cdot \mathrm{vol}(\Lambda)$. Hence by Minkowski's Theorem there is $0 \neq v \in \Lambda \cap (cX)$. Moreover, since $\frac{1}{c}v \in X$ we have $|N_{r,s}(v)| = c^n \cdot |N_{r,s}(\frac{1}{c}v)| \leq c^n = 2^n \cdot \frac{\mathrm{vol}(\Lambda)}{\mathrm{vol}(X)}$.

ii) Now let $X := X_{r,s}(n) := \{w \in \mathbb{R}^n; L_{r,s}(w) \leq n\}$. Then X is compact, convex, and centrally symmetric, such that $\mathrm{vol}(X) = \frac{n^n}{n!} \cdot 2^r(\frac{\pi}{2})^s$.

Moreover, for any $w = [x_1, \ldots, x_n] \in X$ we have $|N_{r,s}(w)| = \prod_{i=1}^r |x_i| \cdot \big(\prod_{j=1}^s \sqrt{x_{r+2j-1}^2 + x_{r+2j}^2}\big)^2$, thus the **geometric-arithmetic mean inequality** yields $\sqrt[n]{|N_{r,s}(w)|} \leq \frac{1}{n} \cdot \big(\sum_{i=1}^r |x_i| + 2 \cdot \sum_{j=1}^s \sqrt{x_{r+2j-1}^2 + x_{r+2j}^2}\big) = \frac{1}{n} \cdot L_{r,s}(w) \leq 1$, hence we have $|N_{r,s}(w)| \leq 1$ as well.

Thus applying part i) to the set X, there is $0 \neq v \in \Lambda$ such that $\frac{|N_{r,s}(v)|}{\mathrm{vol}(\Lambda)} \leq \frac{2^n}{\mathrm{vol}(X)} = 2^{r+2s} \cdot \frac{n!}{n^n} \cdot (\frac{1}{2})^r(\frac{2}{\pi})^s = \frac{n!}{n^n} \cdot (\frac{8}{\pi})^s = 2^s \cdot M_{r,s}$. ♯

(8.3) Finiteness of class groups. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, with ring of integers $\mathcal{O} := \mathcal{O}_K$, let $\sigma_1, \dots, \sigma_r \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the real embeddings, and let $\tau_1, \overline{\tau}_1, \dots, \tau_s, \overline{\tau}_s \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the non-real ones, where $r, s \in \mathbb{N}_0$ and $r + 2s = n$.

Then for $\alpha \in K$ we have $N_K(\alpha) = \prod_{i=1}^{r} \alpha^{\sigma_i} \cdot \prod_{j=1}^{s} (\alpha^{\tau_j} \overline{\alpha^{\tau_j}}) = \prod_{i=1}^{r} \alpha^{\sigma_i} \cdot \prod_{j=1}^{s} |\alpha^{\tau_j}|^2 = \prod_{i=1}^{r} \alpha^{\sigma_i} \cdot \prod_{j=1}^{s} (\mathrm{Re}(\alpha^{\tau_j})^2 + \mathrm{Im}(\alpha^{\tau_j})^2) = N_{r,s}(\mathcal{G}_{r,s}(\alpha))$. Hence the Minkowski bound implies the following:

Corollary. Let $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$ be an ideal. Then there is an element $0 \neq \alpha \in \mathfrak{a}$ such that $|N_K(\alpha)| \leq M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{a})$.

Proof. Recall that $\Lambda_{\mathfrak{a}} \subseteq \Lambda_K$ has volume $\mathrm{vol}(\Lambda_{\mathfrak{a}}) = (\frac{1}{2})^s \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{a})$. ♯

Corollary. Every ideal class contains an ideal $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$ such that $N(\mathfrak{a}) \leq M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|} \in \mathbb{R}$. In particular, the ideal class group Cl_K is finite.

Proof. Let $\{0\} \neq \mathfrak{c} \trianglelefteq \mathcal{O}$ belong to the ideal class in question, let $\{0\} \neq \mathfrak{b} \trianglelefteq \mathcal{O}$ such that $\mathfrak{b} = \mathfrak{c}^{-1} \in \mathrm{Cl}_K$, let $0 \neq \omega \in \mathfrak{b}$ such that $|N_K(\omega)| \leq M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{b})$, and let $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$ such that $(\omega) = \mathfrak{a}\mathfrak{b} \trianglelefteq \mathcal{O}$. Hence we have $\mathfrak{a} = \mathfrak{b}^{-1} = \mathfrak{c} \in \mathrm{Cl}_K$. Moreover, we have $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) = N((\omega)) = |N_K(\omega)| \leq M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{b})$, entailing $N(\mathfrak{a}) \leq M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|}$.

Finally, since any finitely generated free Abelian group has only finitely many subgroups of a fixed finite index, there are only finitely many non-zero ideals of $\mathcal{O}$ of norm not exceeding a fixed finite bound. This implies finiteness of Cl_K. ♯

Corollary. We have $|\mathrm{disc}(K)| \geq \frac{1}{M_{r,s}^2} = (\frac{n^n}{n!})^2 \cdot (\frac{\pi}{4})^{2s} > \frac{1}{2e\pi \cdot n} \cdot (\frac{e^2\pi}{4})^n$; thus we have $|\mathrm{disc}(K)| \to \infty$ for $n \to \infty$. Moreover, we have **Minkowski's Discriminant Theorem** saying that $|\mathrm{disc}(K)| = 1$ if and only if $K = \mathbb{Q}$.

Proof. The first inequality follows from $N(1) = 1$. Moreover, **Stirling's Formula** says $n! = n^n \cdot \sqrt{2\pi n} \cdot \exp(-n + \frac{\epsilon_n}{12n})$, where $0 < \epsilon_n < 1$. Since $2s \leq n$ this yields $(\frac{n^n}{n!})^2 \cdot (\frac{\pi}{4})^{2s} > \frac{1}{2\pi n} \cdot (\frac{\pi}{4})^n \cdot \exp(2n - \frac{1}{6n}) > \frac{1}{2e\pi \cdot n} \cdot (\frac{e^2\pi}{4})^n$.

We have $\frac{n}{n+1} \cdot \frac{e^2\pi}{4} \geq \frac{e^2\pi}{8} \sim 2.90$, thus the sequence $[\frac{1}{2e\pi \cdot n} \cdot (\frac{e^2\pi}{4})^n \in \mathbb{R}; n \in \mathbb{N}]$ is strictly increasing, where for $n = 3$ we get $\frac{1}{2e\pi \cdot 3} \cdot (\frac{e^2\pi}{4})^3 \sim 3.81$. For $n = 2$ we get $\frac{1}{M_{2,0}^2} \geq \frac{1}{M_{0,1}^2} = (\frac{2^2}{2!})^2 \cdot (\frac{\pi}{4})^2 = \frac{\pi^2}{4} \sim 2.47$ (while $\frac{1}{2e\pi \cdot 2} \cdot (\frac{e^2\pi}{4})^2 \sim 0.99$). ♯

(8.4) Theorem. Given $n \in \mathbb{N}$ and $\delta \in \mathbb{Z}$, there are only finitely many algebraic number fields K of degree $[K\colon \mathbb{Q}] = n$ and discriminant $\mathrm{disc}(K) = \delta$.

Proof. We first observe that we may assume that $\mathbb{Q}(i) \subseteq K$: Otherwise, for the composite field $K(i)$ we have $[K(i)\colon \mathbb{Q}] = 2n = [\mathbb{Q}(i)\colon \mathbb{Q}] \cdot [K\colon \mathbb{Q}]$, thus we get $\mathrm{disc}(K(i)) \mid 4^n\delta^2$; hence we may replace K by $K(i)$. (Recall that any algebraic number field has only finitely many subfields.)

Now K does not have any real embeddings; hence let $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the conjugate pairs of non-real ones, where $2s = n \in \mathbb{N}$. Moreover, let $\Lambda := \Lambda_K \subseteq \mathbb{R}^n$ be the full lattice associated with K; then $\mathrm{vol}(\Lambda) = (\frac{1}{2})^s \cdot \sqrt{|\delta|}$.

For $c > 0$ we consider the convex and centrally symmetric open subset

$$X(c) := \{[x_1, \ldots, x_n] \in \mathbb{R}^n; x_1^2 < 1,\, x_2^2 < c^2|\delta|,\, x_{2j-1}^2 + x_{2j}^2 < 1 \text{ for } j \geq 2\} \subseteq \mathbb{R}^n,$$

which has volume $\mathrm{vol}(X(c)) = 4c\pi^{s-1}\sqrt{|\delta|}$. Choosing $c > \frac{1}{2} \cdot (\frac{2}{\pi})^{s-1}$ we get $\mathrm{vol}(X(c)) > 2^s \cdot \sqrt{|\delta|} = 2^n \cdot \mathrm{vol}(\Lambda)$. Hence by Minkowski's Theorem there is $0 \neq [x, y, \ldots] \in \Lambda \cap X(c)$, that is there is $0 \neq \alpha \in \mathcal{O}_K$ such that $\alpha^{\tau_1} = x + iy$, where $|x| < 1$ and $|y| < c\sqrt{|\delta|}$, and $|\alpha^{\tau_j}| < 1$ for $j \in \{2, \ldots, s\}$.

Since $0 \neq |N(\alpha)| = |\alpha^{\tau_1}| \cdot \prod_{j=2}^{s} |\alpha^{\tau_2}| \in \mathbb{Z}$, and $|\alpha^{\tau_j}| < 1$ for $j \geq 2$, we infer that $|\alpha^{\tau_1}|^2 = x^2 + y^2 > 1$. This implies $\mathrm{Im}(\alpha^{\tau_1}) = y \neq 0$, that is $\alpha^{\tau_1} \neq \alpha^{\overline{\tau}_1}$. Moreover, from $|\alpha^{\tau_j}| = |\alpha^{\overline{\tau}_j}| < 1$ we conclude that $\alpha^{\tau_j} \neq \alpha^{\tau_1} \neq \alpha^{\overline{\tau}_j}$, for $j \geq 2$.

Then $\alpha \in K$ is a primitive element: Assume that $\mathbb{Q}(\alpha) \subset K$; then there are at least two embeddings of K mapping α to α^{τ_1}, a contradiction.

Let $\mu_\alpha \in \mathbb{Z}[X]$ be the minimum polynomial of α; hence $\mu_\alpha = \prod_{j=1}^{s}(X^2 - 2 \cdot \mathrm{Re}(\alpha^{\tau_j}) \cdot X + |\alpha^{\tau_j}|^2) \in \mathbb{R}[X]$. Since the geometric embedding of α belongs to the bounded set $X(c)$, it follows that the coefficients of μ_α are bounded in terms of $|\delta|$. This shows that a primitive element of K can be chosen from a finite set. ♯

Corollary: Hermite's Finiteness Theorem. Given $\delta \in \mathbb{Z}$, there are only finitely many algebraic number fields K of discriminant $\mathrm{disc}(K) = \delta$.

Proof. Just recall that the degree $[K\colon \mathbb{Q}]$ is bounded in terms of $|\mathrm{disc}(K)|$. ♯

(8.5) Computing class numbers. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, and let $r, s \in \mathbb{N}_0$ be the number of real and pairs of non-real embeddings, respectively; hence $r + 2s = n$.

By the Minkowski bound, to detect all ideal classes we only have to consider the ideals of norm at most $m_K := M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|} \in \mathbb{R}$, where a few values of Minkowski constants are given in Table 7. Moreover, since the class group is generated by prime ideals, we only have to consider the prime ideals having norm at most m_K, which are hence lying over positive rational primes p such that $p \leq m_K$. In particular, the class number of K equals $h_K = 1$ if and only if all prime ideals in $\coprod_{p \in \mathcal{P}_{\mathbb{Z}}; p \leq m_K} \mathcal{P}_K(p)$ are principal.

Table 7: Minkowski constants.

r	s	$M_{r,s}$
1	0	1
0	1	0.636619
2	0	0.5
1	1	0.282942
3	0	0.222222
0	2	0.151981
2	1	0.119366
4	0	0.09375
1	2	0.062251
3	1	0.048892
5	0	0.0384

r	s	$M_{r,s}$
0	3	0.031853
2	2	0.025017
4	1	0.019648
6	0	0.015432
1	3	0.012632
3	2	0.009921
5	1	0.007792
7	0	0.006119
0	4	0.006315
2	3	0.004960
4	2	0.003896
6	1	0.003059
8	0	0.002403

r	s	$M_{r,s}$
1	4	0.002461
3	3	0.001933
5	2	0.001518
7	1	0.001192
9	0	0.000936
0	5	0.0012142
2	4	0.0009536
4	3	0.0007490
6	2	0.0005882
8	1	0.0004620
10	0	0.000362

(8.6) Example: The pure cubic fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{7})$. a) Let $\alpha := \sqrt[3]{2}$ and $K := \mathbb{Q}(\alpha)$, hence $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(K) = -4 \cdot 27$; see (5.9). We have $r = 1$ and $s = 1$, yielding $M_{r,s} \sim 0.28$. Hence any ideal class contains an ideal of norm at most $m_K \sim 0.28 \cdot \sqrt{108} \sim 2.94 < 3$. We only have to consider $\mathcal{P}_K(2)$:

Since $\mu_\alpha = X^3 - 2 = X^3 \in \mathbb{F}_2[X]$, we conclude that $(2) = \mathfrak{p}^3 \lhd \mathcal{O}_K$, where $\mathfrak{p} := (2, \sqrt[3]{2}) = (\sqrt[3]{2}) \lhd \mathcal{O}_K$ is principal. Hence we have $h_K = 1$. ♯

b) Let $\beta := \sqrt[3]{7}$, let $K := \mathbb{Q}(\beta)$, and let $\mathcal{O} := \mathcal{O}_K$. Since $\mu_\beta := X^3 - 7 \in \mathbb{Z}[X]$ splits as $\mu_\beta = \prod_{i=0}^{2}(X - \zeta^i\beta) \in \mathbb{C}[X]$, where $\zeta := \zeta_3 \in \mathbb{C}$ is a primitive 3-rd root of unity, the embeddings of K into $\mathbb{C}$ are given by $\beta \mapsto \zeta^i\beta$ for $i \in \{0, 1, 2\}$.

i) We determine $\mathcal{O}$: We have $\mathbb{Z}[\beta] \subseteq \mathcal{O}$, where $\mathbb{Z}[\beta] \cong \mathbb{Z}[X]/(\mu_\beta)$. Letting

$$\Delta := \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \zeta\beta & \zeta^2\beta^2 \\ 1 & \zeta^2\beta & \zeta\beta^2 \end{bmatrix} = [\zeta^{i+j-2}]_{ij} \cdot \operatorname{diag}[1, \beta, \beta^2],$$

we get $\operatorname{disc}(\mathbb{Z}[\beta]) = \det(\Delta)^2 = \beta^6 \cdot \big((1-\zeta)(1-\zeta^2)(\zeta-\zeta^2)\big)^2 = -49 \cdot 27$.

Since $(7) = (\beta)^3 \lhd \mathcal{O}$ we conclude that 7 is ramified in K. Thus we have $7 \mid \operatorname{disc}(K)$, entailing $3 \cdot 7^2 \mid \operatorname{disc}(K)$, in other words $\mathcal{O} = \mathbb{Z}[\beta]$ or $[\mathcal{O} \colon \mathbb{Z}[\beta]] = 3$.

To exclude the latter case, we consider the regular representation ρ with respect to the $\mathbb{Q}$-basis $\{1, \beta, \beta^2\} \subseteq K$, for which $\rho(\beta)$ is the companion matrix associated with μ_β. This yields $N_K(a + b\beta + c\beta^2) = a^3 - 21abc + 7b^3 + 49c^3$, for $a, b, c \in \mathbb{Q}$. Letting $a, b, c \in \{0, 1, 2\}$ and $\omega := \frac{1}{3}(a + b\beta + c\beta^2) \in K$, checking $N_K(\omega) \in \mathbb{Q}$ for integrality, we find no non-zero solution. Hence we infer that $\mathcal{O} = \mathbb{Z}[\beta]$.

ii) We proceed to determine the class number of K: We have $r = 1$ and $s = 1$, yielding $M_{r,s} \sim 0.28$. Hence any ideal class contains an ideal of norm at most $m_K \sim 0.28 \cdot \sqrt{1323} \sim 10.29 < 11$. We have to consider $\mathcal{P}_K(p)$ for $p \in \{2, 3, 5, 7\}$:

For $p = 2$ we have $\mu_\beta = X^3 + 1 = (X + 1)(X^2 + X + 1) \in \mathbb{F}_2[X]$, hence $(2) = \mathfrak{p}_2\mathfrak{q}_2 \lhd \mathcal{O}$, where $\mathfrak{p}_2 := (2, \beta{+}1) = (2, \beta{-}1) \lhd \mathcal{O}$ and $\mathfrak{q}_2 := (2, \beta^2{+}\beta{+}1) \lhd \mathcal{O}$. Similarly, for $p = 5$ we have $\mu_\beta = X^3 - 2 = (X + 2)(X^2 - 2X - 1) \in \mathbb{F}_5[X]$, hence we have $(5) = \mathfrak{p}_5\mathfrak{q}_5 \lhd \mathcal{O}$, where $\mathfrak{p}_5 := (5, \beta{+}2) \lhd \mathcal{O}$ and $\mathfrak{q}_5 := (5, \beta^2 - 2\beta - 1) \lhd \mathcal{O}$.

For $p = 3$ we have $\mu_\lambda = X^3 - 1 = (X - 1)^3 \in \mathbb{F}_3[X]$, hence we have $(3) = \mathfrak{p}_3^3 \lhd \mathcal{O}$, where $\mathfrak{p}_3 := (3, \beta - 1) = (3, \beta + 2) \lhd \mathcal{O}$. Finally, for $p = 7$ we have $\mu_\beta = X^3 \in \mathbb{F}_7[X]$, hence we have $(7) = \mathfrak{p}_7^3 \lhd \mathcal{O}$, where $\mathfrak{p}_7 := (7, \beta) = (\beta) \lhd \mathcal{O}$ is principal.

Thus we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5 \rangle$, where $\mathfrak{q}_2 = \mathfrak{p}_2^{-1} \in \mathrm{Cl}_K$ and $\mathfrak{q}_5 = \mathfrak{p}_5^{-1} \in \mathrm{Cl}_K$, while $\mathfrak{p}_3^3 = 1 \in \mathrm{Cl}_K$. Since for any $\omega \in \mathcal{O}$ we have $N_K(\omega) \equiv \{0, \pm 1\} \pmod 7$, we conclude that $\mathfrak{p}_3$ is not principal, and thus has order 3 in Cl_K.

Since $N_K(\beta{-}1) = 6$ we have $\mathfrak{p}_2\mathfrak{p}_3 = (6, 2(\beta{-}1), 3(\beta{-}1), (\beta{-}1)) \subseteq (\beta{-}1) \lhd \mathcal{O}$, which since $N(\mathfrak{p}_2\mathfrak{p}_3) = 6$ entails equality, so that $\mathfrak{p}_2\mathfrak{p}_3 = 1 \in \mathrm{Cl}_K$. Similarly, since $N_K(\beta{+}2) = 15$ we have $\mathfrak{p}_3\mathfrak{p}_5 = (15, 3(\beta{+}2), 5(\beta{+}2), (\beta{+}2)^2) \subseteq (\beta{+}2) \lhd \mathcal{O}$, which since $N(\mathfrak{p}_3\mathfrak{p}_5) = 15$ entails equality, so that $\mathfrak{p}_3\mathfrak{p}_5 = 1 \in \mathrm{Cl}_K$. Hence in conclusion we have $\mathrm{Cl}_K = \langle \mathfrak{p}_3 \rangle \cong C_3$, thus $h_K = 3$. ♯

9 Unit groups

(9.1) Logarithmic embeddings. a) Let $n \in \mathbb{N}$, and let $r, s \in \mathbb{N}_0$ such that $r + 2s = n$. Recall that the geometric space $\mathbb{R}^n$ may be equipped with the structure of a commutative $\mathbb{Q}$-algebra, which is inherited from $\mathbb{R}^r \oplus \mathbb{C}^s$

Hence the regular action of $v = [x_1, \ldots, x_n] \in \mathbb{R}^n$, which is transported from $\mathbb{R}^r \oplus \mathbb{C}^s$ with component-wise multiplication, is given as the block diagonal matrix $\rho(v) = \mathrm{diag}[x_1, \ldots, x_r] \oplus \bigoplus_{j=1}^{s} \begin{bmatrix} x_{r+2j-1} & x_{r+2j} \\ -x_{r+2j} & x_{r+2j-1} \end{bmatrix} \in \mathbb{R}^{n \times n}$. Hence from this we obtain $\det(\rho(v)) = \prod_{i=1}^{r} x_i \cdot \prod_{j=1}^{s} (x_{r+2j-1}^2 + x_{r+2j}^2) = N_{r,s}(v)$.

b) The group of units of $\mathbb{R}^r \oplus \mathbb{C}^s$ equals $(\mathbb{R}^*)^r \oplus (\mathbb{C}^*)^s$. Hence the group of units $(\mathbb{R}^n)^*$ of $\mathbb{R}^n$, with respect to the above algebra structure, is the set of all $[x_1, \ldots, x_n] \in \mathbb{R}^n$ such that $x_i \neq 0$ for all $i \in \{1, \ldots, r\}$, and $[x_{r+2j-1}, x_{r+2j}] \neq [0, 0]$ for all $j \in \{1, \ldots, s\}$.

We consider the map $\mathcal{L}_{r,s} \colon (\mathbb{R}^n)^* \to \mathbb{R}^{r+s} \colon [x_1, \ldots, x_n] \mapsto [y_1, \ldots, y_{r+s}]$, where

$$\begin{array}{lcll} y_i & := & \ln(|x_i|), & \text{for } i \in \{1, \ldots, r\}, \\ y_{r+j} & := & \ln(x_{r+2j-1}^2 + x_{r+2j}^2), & \text{for } j \in \{1, \ldots, s\}. \end{array}$$

Then $\mathbb{R}^{r+s}$ is called the associated **logarithmic space**. Since $|\cdot| \colon \mathbb{C}^* \to \mathbb{R}_{>0}$ is multiplicative, and $\ln \colon (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ is a group homomorphism, we conclude that $\mathcal{L}_{r,s}$ is group homomorphism.

c) To take the map $N_{r,s}$ into account, let $\mathcal{H} \colon \mathbb{R}^{r+s} \to \mathbb{R} \colon [y_1, \ldots, y_{r+s}] \mapsto \sum_{k=1}^{r+s} y_k$, and $H := \ker(\mathcal{H}) \leq \mathbb{R}^{r+s}$; thus we have $\dim_{\mathbb{R}}(H) = r + s - 1$.

Then for any $v = [x_1, \ldots, x_n] \in (\mathbb{R}^n)^*$ we have $\ln(|N_{r,s}(v)|) = \ln\big(\prod_{i=1}^r |x_i| \cdot \prod_{j=1}^s (x_{r+2j-1}^2 + x_{r+2j}^2)\big) = \sum_{i=1}^r \ln(|x_i|) + \sum_{j=1}^s \ln(x_{r+2j-1}^2 + x_{r+2j}^2)$. Thus we infer that $\ln(|N_{r,s}(v)|) = \mathcal{H}(\mathcal{L}_{r,s}(v))$. In particular, we have $\mathcal{L}_{r,s}(v) \in H$ if and only if $|N_{r,s}(v)| = 1$.

(9.2) Groups of units. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, let $\sigma_1, \ldots, \sigma_r \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the real embeddings, and $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the conjugate pairs of the non-real ones, where $r, s \in \mathbb{N}_0$ such that $r + 2s = n$. Recall that $\alpha^\sigma \neq 0$ for all $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)$, whenever $\alpha \in K^*$.

Concatenating with the geometrical embedding $\mathcal{G}_{r,s}\colon K \to \mathbb{R}^n$ we get the **logarithmic map** $\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s}\colon K^* \to \mathbb{R}^{r+s}\colon \alpha \mapsto [y_1, \ldots, y_{r+s}]$ given by

$$\begin{array}{lcll} y_i & := & \ln(|\alpha^{\sigma_i}|), & \text{for } i \in \{1, \ldots, r\}, \\ y_{r+j} & := & \ln(\mathrm{Re}(\alpha^{\tau_j})^2 + \mathrm{Im}(\alpha^{\tau_j})^2), & \text{for } j \in \{1, \ldots, s\}. \end{array}$$

Since $\mathcal{G}_{r,s}$ is an embedding of algebras, we conclude that $\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s}\colon K^* \to \mathbb{R}^{r+s}$ is a group homomorphism; we have $\mathcal{L}_{r,s}(\mathcal{G}_{r,s}(\alpha)) \in H$ if and only if $|N_K(\alpha)| = 1$.

Theorem: Dirichlet's Unit Theorem. The group of units $\mathcal{O}^*$ is a finitely generated Abelian group of shape $A \times T(\mathcal{O}^*)$, where A is free of rank $r + s - 1$, and the torsion subgroup $T(\mathcal{O}^*)$ is finite cyclic.

Note that $T(\mathcal{O}^*)$ consists of the units of finite order, that is the complex roots of unity contained in K; in particular, we have $\{\pm 1\} \leq T(\mathcal{O}^*)$.

Proof. i) Restricting the group homomorphism $\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s}\colon K^* \to (\mathbb{R}^n)^* \to \mathbb{R}^{r+s}$, we get a monoid homomorphism $\mathcal{O} \setminus \{0\} \to \Lambda_{\mathcal{O}} \setminus \{0\} \to \mathbb{R}^{r+s}$, and restricting further we get a group homomorphism $\mathcal{O}^* \to \mathcal{G}_{r,s}(\mathcal{O}^*) \to \mathbb{R}^{r+s}$.

Next, the function $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ and its inverse $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ are both continuous. Hence if $M \subseteq \mathbb{R}$ is bounded, then its closure $\overline{M} \subseteq \mathbb{R}$ is compact, entailing that $\exp(\overline{M}) \subseteq \mathbb{R}_{>0}$ is compact as well, thus in particular $\exp(M) \subseteq \mathbb{R}_{>0}$ is bounded. Similarly, if $M \subseteq \mathbb{R}_{>0}$ is bounded such that $\overline{M} \subseteq \mathbb{R}_{>0}$ (that is $0 \notin \overline{M}$), then $\ln(\overline{M}) \subseteq \mathbb{R}$ is compact, thus in particular $\ln(M) \subseteq \mathbb{R}$ is bounded.

Hence, if $M \subseteq \mathbb{R}^{r+s}$ is a bounded then $\mathcal{L}_{r,s}^{-1}(M) \subseteq (\mathbb{R}^n)^*$ is bounded as well. Thus, since $\Lambda_{\mathcal{O}} \subseteq \mathbb{R}^n$ is a lattice, the intersection $\mathcal{L}_{r,s}^{-1}(M) \cap \Lambda_{\mathcal{O}}$ is finite. Hence any bounded subset of $\mathcal{L}_{r,s}(\Lambda_{\mathcal{O}} \setminus \{0\})$ is finite, implying that the additive subgroup $\Lambda_{\mathcal{O}^*} := \mathcal{L}_{r,s}(\mathcal{G}_{r,s}(\mathcal{O}^*)) \subseteq \mathbb{R}^{r+s}$ is a lattice; let $t := \mathrm{rk}_{\mathbb{Z}}(\Lambda_{\mathcal{O}^*}) \in \mathbb{N}_0$.

ii) We show that $T := \ker((\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s})|_{\mathcal{O}^*}) = T(\mathcal{O}^*)$: Since $T \subseteq \mathcal{L}_{r,s}^{-1}(\{0\})$, we conclude that $T \leq \mathcal{O}^*$ is finite, and hence by Artin's Theorem is cyclic. Moreover, it thus consists of elements of finite order, hence $T \leq T(\mathcal{O}^*)$.

To show the converse, note that for $\alpha \in \mathcal{O}^*$ we have $\alpha \in T$ if and only if $|\alpha^\sigma| = 1$ for all $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)$. Now, if $\alpha \in T(\mathcal{O}^*)$, then all its conjugates are roots of unity, thus have complex absolute value 1, entailing that $\alpha \in T$. ♯

Having this in place, we conclude that $\mathcal{O}^*/T(\mathcal{O}^*) \cong \Lambda_{\mathcal{O}^*}$, so that $\mathcal{O}^*/T(\mathcal{O}^*)$ is a free Abelian group of rank t. By the theory of finitely generated $\mathbb{Z}$-modules, we infer that $\mathcal{O}^* = A \times T(\mathcal{O}^*)$, where $A \cong \mathcal{O}^*/T(\mathcal{O}^*) \cong \Lambda_{\mathcal{O}^*}$.

Since for $\alpha \in \mathcal{O}^*$ we have $|N_K(\alpha)| = 1$, we infer that $\Lambda_{\mathcal{O}^*} \subseteq H \leq \mathbb{R}^{r+s}$, so that $t \leq r+s-1$. We show equality, by showing that there is a bounded subset of H whose $\Lambda_{\mathcal{O}^*}$-translates cover H:

iii) To this end, let $Z := \{v \in \mathbb{R}^n; |N_{r,s}(v)| = 1\}$. Then $Z \subseteq \mathbb{R}^n$ is closed, and we have $Z \subseteq (\mathbb{R}^n)^*$. Moreover, since $\mathcal{L}_{r,s} \colon (\mathbb{R}^n)^* \to \mathbb{R}^{r+s}$ is surjective, we have $\mathcal{L}_{r,s}(Z) = H$. (For the case $r = 2$ and $s = 0$ the set Z is depicted as the boundary of region A in Table 6.)

For $v \in Z$ and $\alpha \in \mathcal{O}^*$ we have $|N_{r,s}(v \cdot \mathcal{G}_{r,s}(\alpha))| = |N_{r,s}(v)| \cdot |N_{r,s}(\mathcal{G}_{r,s}(\alpha))| = |N_{r,s}(v)| \cdot |N_K(\alpha)| = 1$, thus $v \cdot \mathcal{G}_{r,s}(\alpha) \in Z$ as well. Hence, since $\mathcal{L}_{r,s}$ is a group homomorphism, mapping compact subsets of $(\mathbb{R}^n)^*$ to compact subsets of $\mathbb{R}^{r+s}$, it suffices to specify a compact subset $Y \subseteq Z$ such that $Z = \bigcup_{\alpha \in \mathcal{O}^*}(Y \cdot \mathcal{G}_{r,s}(\alpha))$:

iv) We consider the full lattice $\Lambda_{\mathcal{O}} \subseteq \mathbb{R}^n$, where $\mathrm{vol}(\Lambda_{\mathcal{O}}) = (\frac{1}{2})^s \cdot \sqrt{|\mathrm{disc}(K)|}$, and let $c_1, \ldots, c_{r+s} > 0$ such that $c := \prod_{k=1}^{r+s} c_k \geq (\frac{4}{\pi})^s \cdot \mathrm{vol}(\Lambda_{\mathcal{O}})$.

Let X be the set of all elements $w = [x_1, \ldots, x_n] \in \mathbb{R}^n$ such that $|x_i| \leq c_i$ for $i \in \{1, \ldots, r\}$, and $x_{r+2j-1}^2 + x_{r+2j}^2 \leq c_{r+j}$ for $i \in \{1, \ldots, r\}$. Hence for $w \in X$ we have $|N_{r,s}(w)| = \prod_{i=1}^{r} |x_i| \cdot \prod_{j=1}^{s} (x_{r+2j-1}^2 + x_{r+2j}^2) \leq \prod_{i=1}^{r} c_i \cdot \prod_{j=1}^{s} c_{r+j} = c$. Moreover, X is compact, convex, and centrally symmetric, such that $\mathrm{vol}(X) = 2^r \pi^s \cdot \prod_{i=1}^{r} c_i \cdot \prod_{j=1}^{s} c_{r+j} \geq 2^r \pi^s \cdot (\frac{4}{\pi})^s \cdot \mathrm{vol}(\Lambda_{\mathcal{O}}) = 2^n \cdot \mathrm{vol}(\Lambda_{\mathcal{O}})$. (For the case $r = 2$ and $s = 0$ the set X is depicted for $c_1 = c_2 = 1$ as region C in Table 6.)

Since there are only finitely many non-zero ideals of $\mathcal{O}$ having norm bounded above by c, considering only non-zero principal ideals entails that there are only finitely many pairwise non-associate non-zero elements $\omega_1, \ldots, \omega_m \in \mathcal{O}$ having absolute norm bounded above by c, for some $m \in \mathbb{N}_0$.

Let $Y := Z \cap \bigcup_{k=1}^{m}(X \cdot \mathcal{G}_{r,s}(\omega_k^{-1}))$. Since X is compact, we conclude that all the sets $X \cdot \mathcal{G}_{r,s}(\omega_k^{-1})$ are compact as well, and thus so are their (finite) union, and the intersection Y of the latter with the closed set Z.

v) Now let $v \in Z$. Then the set $\Lambda_{\mathcal{O}} \cdot v \subseteq \mathbb{R}^n$ is a full lattice again, where, using the regular representation ρ, we have $\mathrm{vol}(\Lambda_{\mathcal{O}} \cdot v) = |\det(\rho(v))| \cdot \mathrm{vol}(\Lambda_{\mathcal{O}}) = |N_{r,s}(v)| \cdot \mathrm{vol}(\Lambda_{\mathcal{O}}) = \mathrm{vol}(\Lambda_{\mathcal{O}})$. Hence by Minkowski's Theorem there is $0 \neq w \in (\Lambda_{\mathcal{O}} \cdot v) \cap X$. Thus there is $0 \neq \omega \in \mathcal{O}$ such that $\mathcal{G}_{r,s}(\omega) \cdot v = w \in X$. Then we have $|N_{r,s}(w)| = |N_{r,s}(\mathcal{G}_{r,s}(\omega))| \cdot |N_{r,s}(v)| = |N_K(\omega)| \leq c$.

Hence there is $\alpha \in \mathcal{O}^*$ such that $\omega = \omega_i \alpha$, for some $i \in \{1, \ldots, m\}$; in particular we have $m \geq 1$. Since $v \cdot \mathcal{G}_{r,s}(\alpha) \in Z$, and $v \cdot \mathcal{G}_{r,s}(\alpha) = w \cdot \mathcal{G}_{r,s}(\omega^{-1}) \cdot \mathcal{G}_{r,s}(\alpha) = w \cdot \mathcal{G}_{r,s}(\omega^{-1}\alpha) = w \cdot \mathcal{G}_{r,s}(\omega_i^{-1}) \in X \cdot \mathcal{G}_{r,s}(\omega_i^{-1})$, we infer that $v \cdot \mathcal{G}_{r,s}(\alpha) \in Y$. This shows that the $\mathcal{G}_{r,s}(\mathcal{O}^*)$-translates of Y cover Z. ♯

Corollary. The map $\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s}$ induces a short exact sequence of Abelian groups

$$\{1\} \to T(\mathcal{O}^*) \to \mathcal{O}^* \to \Lambda_{\mathcal{O}^*} \to \{0\}.$$

Corollary. The group $\mathcal{O}^*$ is finite, if and only if $K = \mathbb{Q}$, or $K = \mathbb{Q}(\sqrt{d})$ where $d < 0$ is square-free.

Proof. Finiteness of $\mathcal{O}^*$ is equivalent to $r = 1$ and $s = 0$, or $r = 0$ and $s = 1$. The former case amounts to $n = 1$, that is $K = \mathbb{Q}$. The latter case amounts to $n = 2$, where K does not have a real embedding. ♯

Corollary. An algebraic integer is a root of unity if and only if all its algebraic conjugates have complex absolute value 1.

We present an example showing that above it is not enough to assume that only the algebraic integer in question has complex absolute value 1:

Example. Let $\alpha := \sqrt[3]{2}$ and $\zeta := \zeta_3$, and let $K := \mathbb{Q}(\alpha, \zeta)$. Then K is Galois such that $\mathrm{Aut}_{\mathbb{Q}}(K) = \langle \sigma, \kappa \rangle \cong \mathcal{S}_3$, where $\sigma\colon \alpha \mapsto \zeta\alpha$ fixing ζ, and $\kappa := \overline{\ }$ is the restriction of complex conjugation.

From $X^3-1 = (X-1)(X^2+X+1) \in \mathbb{Z}[X]$ we get $(\alpha-1)(\alpha^2+\alpha+1) = \alpha^3-1 = 1$, showing $\alpha-1 \in \mathcal{O}_K^*$. Hence both $\zeta\alpha-1$ and $\zeta^2\alpha-1$ are units as well, thus so is $\epsilon := \frac{\zeta\alpha-1}{\zeta^2\alpha-1} \in \mathcal{O}_K^*$. The $\mathrm{Aut}_{\mathbb{Q}}(K)$-orbit of ϵ is $\{(\frac{\zeta\alpha-1}{\zeta^2\alpha-1})^{\pm 1}, (\frac{\zeta^2\alpha-1}{\alpha-1})^{\pm 1}, (\frac{\alpha-1}{\zeta\alpha-1})^{\pm 1}\}$. We have $|\zeta\alpha - 1| = |\zeta^2\alpha - 1| = \sqrt{(\zeta\alpha-1)(\zeta^2\alpha-1)} = \sqrt{2\alpha^2+\alpha+1} \sim 2.33$, while $\alpha - 1 \sim 0.26$. Hence we get $|\epsilon^{\pm 1}| = 1$, but its (four) algebraic conjugates have complex absolute value ~ 8.97 and ~ 0.11, respectively. ♯

(9.3) Regulators. Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, let $\sigma_1, \ldots, \sigma_r \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the real embeddings, let $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s \in \mathrm{Inj}_{\mathbb{Q}}(K)$ be the conjugate pairs of non-real embeddings, where $r, s \in \mathbb{N}_0$ such that $r+2s = n$, let $t := r + s - 1$, and let $\mathcal{O} := \mathcal{O}_K$ be the ring of integers of K.

A set $\mathcal{A} := \{\epsilon_1, \ldots, \epsilon_t\} \subseteq \mathcal{O}^*$ such that $\mathcal{L}_{r,s}(\mathcal{G}_{r,s}(\mathcal{A})) \subseteq \Lambda_{\mathcal{O}^*}$ is a $\mathbb{Z}$-basis, is called a set of **fundamental units**; this is equivalent to saying that $\mathcal{A}$ freely generates a complement for $T(\mathcal{O}^*)$ in $\mathcal{O}^*$.

The quantity $\mathrm{reg}_K = \mathrm{reg}_{\mathcal{O}^*} := \frac{\mathrm{vol}(\Lambda_{\mathcal{O}^*})}{\sqrt{r+s}} \in \mathbb{R}$ is called the **regulator** of K, where $0 < \mathrm{vol}(\Lambda_{\mathcal{O}^*}) \in \mathbb{R}$ is the t-dimensional volume of $\Lambda_{\mathcal{O}^*} \subseteq H \leq \mathbb{R}^{r+s}$.

Proposition. Letting $\{\epsilon_1, \ldots, \epsilon_{r+s-1}\} \subseteq \mathcal{O}^*$ be a set of fundamental units, the regulator of K is given as $\mathrm{reg}_K = |\det(\Delta^*)| \in \mathbb{R}$, where $\Delta^* \in \mathbb{R}^{t\times t}$ is any t-minor of the matrix

$$\Delta := \begin{bmatrix} \ln(|\epsilon_1^{\sigma_1}|) & \ldots & \ln(|\epsilon_1^{\sigma_r}|) & \ln(|\epsilon_1^{\tau_1}|^2) & \ldots & \ln(|\epsilon_1^{\tau_s}|^2) \\ \vdots & & \vdots & \vdots & & \vdots \\ \ln(|\epsilon_t^{\sigma_1}|) & \ldots & \ln(|\epsilon_t^{\sigma_r}|) & \ln(|\epsilon_t^{\tau_1}|^2) & \ldots & \ln(|\epsilon_t^{\tau_s}|^2) \end{bmatrix} \in \mathbb{R}^{t\times(r+s)},$$

where $|\cdot|$ denotes the real and complex absolute value, respectively.

Proof. Applying $\mathcal{L}_{r,s} \circ \mathcal{G}_{r,s}$ to the fundamental units yields the rows of Δ, which belong to the hyperplane $H = \ker(\mathcal{H}) \leq \mathbb{R}^{r+s}$. Letting $v := [1, \ldots, 1] \in \mathbb{R}^{r+s}$, we have $v \in H^\perp$ and $\|v\| = \sqrt{r+s}$. Hence letting $\widehat{\Delta} \in \mathbb{R}^{(r+s)\times(r+s)}$ be obtained from Δ by adding v as row $r+s$, we have $\mathrm{vol}(\Lambda_{\mathcal{O}^*}) = \frac{1}{\sqrt{r+s}} \cdot |\det(\widehat{\Delta})|$.

The columns of $\widehat{\Delta}$ sum up to $w := [0, \ldots, 0, r+s]^{\mathrm{tr}} \in \mathbb{R}^{(r+s)\times 1}$. Hence replacing any column of $\widehat{\Delta}$ by w shows that $|\det(\widehat{\Delta})| = (r+s) \cdot |\det(\Delta^*)|$, independently of the particular column chosen. This entails $\mathrm{vol}(\Lambda_{\mathcal{O}^*}) = \sqrt{r+s} \cdot |\det(\Delta^*)|$. ♯

Example. Let $K := \mathbb{Q}(\sqrt{2})$, hence $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$. Since $K \subseteq \mathbb{R}$ We have $T(\mathcal{O}^*) = \{\pm 1\}$. Moreover, we have $r = 2$ and $s = 0$, thus $\mathrm{rk}_{\mathbb{Z}}(\mathcal{O}^*/\{\pm 1\}) = 1$. We show that $\epsilon := 1 + \sqrt{2} \in \mathcal{O}$ is a fundamental unit; hence the regulator of K is $\mathrm{reg}_K = |\ln(|\epsilon|)| = \ln(1+\sqrt{2}) \sim 0.881374$:

We have $\mathcal{O}^* = \{\omega \in \mathcal{O}; |N(\omega)| = 1\}$, where for $\omega = a + b\sqrt{2} \in \mathcal{O}$ we have $N(\omega) = N(a+b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$. Thus we have to solve the **norm equation** $X^2 - 2Y^2 = \pm 1$ over $\mathbb{Z}$. Firstly, we have $N(\epsilon) = -1$, thus $\epsilon \in \mathcal{O}^*$, where $\epsilon > 1$.

Next, let $\omega \in \mathcal{O}^*$ such that $1 < \omega = a + b\sqrt{2} \leq \epsilon$. Letting $\overline{\omega} \in \mathcal{O}^*$ be the conjugate of ω, from $\omega\overline{\omega} = N(\omega) = \pm 1$ we get $-1 < \overline{\omega} < 1$, thus $0 < 2a = T(\omega) < 1 + \epsilon = 2 + \sqrt{2}$. Thus we have $a = 1$, entailing $b = 1$, hence $\omega = \epsilon$. ♯

IV Applications

10 Quadratic fields: ideals

(10.1) Quadratic number rings. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, let $\alpha := \sqrt{d} \in \mathbb{C}$, and let $K := \mathbb{Q}(\alpha)$ be the associated **quadratic (number) field**, where K is called **real** if $d > 0$, while it is called **imaginary** if $d < 0$.

Then K is Galois such that $\mathrm{Aut}_{\mathbb{Q}}(K) \cong C_2$, where the latter is generated by the conjugation map $\overline{\ }: \sqrt{d} \mapsto -\sqrt{d}$. Let $\mathcal{O}$ be the ring of integers of K, being called the associated **quadratic number ring**.

Theorem. i) If $d \not\equiv 1 \pmod 4$, then we have $\mathcal{O} = \mathbb{Z}[\alpha]$ and $\mathrm{disc}(\mathcal{O}) = 4d$.
ii) If $d \equiv 1 \pmod 4$, then we have $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(1+\alpha)]$ and $\mathrm{disc}(\mathcal{O}) = d$.

Proof. Let $\mathcal{O}' := \mathbb{Z}[\alpha] \subseteq \mathcal{O}$. Then $\{1, \alpha\} \subseteq \mathcal{O}'$ is a $\mathbb{Z}$-basis. Hence we have $\Delta = \begin{bmatrix} 1 & \alpha \\ 1 & -\alpha \end{bmatrix}$, thus $\mathrm{disc}(\mathcal{O}') = \det(\Delta)^2 = 4d$. Since d is square-free, we only have to check the elements $\frac{1}{2}(a+\alpha) \in K \setminus \mathbb{Q}$, where $a \in \{0, 1\}$, for integrality:

We have $N(\frac{\alpha}{2}) = -\frac{4}{d}$ and $N(\frac{1}{2}(1+\alpha)) = \frac{1}{4}(1-d)$. Hence if $d \not\equiv 1 \pmod 4$ we conclude that there are no further integral elements, entailing $\mathcal{O} = \mathcal{O}'$.

If $d \equiv 1 \pmod 4$, then for $\widehat{\alpha} := \frac{1}{2}(1+\alpha)$ the regular representation with respect to the $\mathbb{Q}$-basis $\{1, \alpha\} \subseteq K$ is given as $\rho(\widehat{\alpha}) = \frac{1}{2} \cdot \begin{bmatrix} 1 & 1 \\ d & 1 \end{bmatrix}$, hence we get $\mu_{\widehat{\alpha}} = \chi_{\widehat{\alpha}} = (X - \frac{1}{2})^2 - \frac{d}{4} = X^2 - X - \frac{d-1}{4} \in \mathbb{Z}[X]$, saying that $\widehat{\alpha}$ is integral. Thus we get $\mathcal{O} = \langle 1, \widehat{\alpha} \rangle_{\mathbb{Z}} = \mathbb{Z}[\widehat{\alpha}]$, where $[\mathcal{O} \colon \mathcal{O}'] = 2$ and hence $\operatorname{disc}(\mathcal{O}) = \frac{1}{4} \cdot \operatorname{disc}(\mathcal{O}') = d$. $\sharp$

(10.2) Theorem: Ramification in quadratic fields. Let still $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, let $\alpha := \sqrt{d} \in \mathbb{C}$ and $\widehat{\alpha} := \frac{1}{2}(1 + \alpha)$, let $K := \mathbb{Q}(\alpha)$, let $\mathcal{O}$ be its ring of integers, and let $p \in \mathbb{Z}$ be a prime. Then we have the following:

i) If $p \mid d$ (no matter whether $p = 2$ or odd), then $p\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p} = (p, \alpha) \lhd \mathcal{O}$.

ii) If $p = 2$ and d is odd, then we have (where in the second case $\mathfrak{p} \neq \overline{\mathfrak{p}}$)

$$2\mathcal{O} = \begin{cases} \mathfrak{p}^2, & \text{where } \mathfrak{p} := (2, 1 + \alpha) \lhd \mathcal{O}, \quad \text{if } d \equiv -1 \pmod 4; \\ \mathfrak{p}\overline{\mathfrak{p}}, & \text{where } \mathfrak{p} := (2, \widehat{\alpha}) \lhd \mathcal{O}, \quad \text{if } d \equiv 1 \pmod 8; \\ (2), & \quad \text{if } d \equiv -3 \pmod 8. \end{cases}$$

iii) If p is odd and $p \nmid d$, then we have (where in the first case $\mathfrak{p} \neq \overline{\mathfrak{p}}$)

$$p\mathcal{O} = \begin{cases} \mathfrak{p}\overline{\mathfrak{p}}, & \text{where } \mathfrak{p} := (p, c + \alpha) \lhd \mathcal{O}, \quad \text{if } c^2 \equiv d \pmod p; \\ (p), & \quad \text{if } d \text{ is not a square} \pmod p. \end{cases}$$

Proof. Let $r := |\mathcal{P}_K(p)|$, let $e := e(\mathfrak{q})$ for some (hence any) $\mathfrak{q} \in \mathcal{P}_K(p)$, and let $f := f(\mathfrak{q})$ for some (hence any) $\mathfrak{q} \in \mathcal{P}_K(p)$. By the fundamental equality there are three mutually exclusive possible cases: Either p is (completely) split, that is $r = 2$; or p is (completely) ramified, that is $e = 2$; or p is inert, that is $f = 2$.

Recall that $\mathcal{O} = \mathbb{Z}[\alpha]$ whenever $d \not\equiv 1 \pmod 4$, where $\mu_\alpha = X^2 - d \in \mathbb{Z}[X]$, while $\mathcal{O} = \mathbb{Z}[\widehat{\alpha}]$ whenever $d \equiv 1 \pmod 4$, where $\mu_{\widehat{\alpha}} = X^2 - X - \frac{d-1}{4} \in \mathbb{Z}[X]$. In the latter case we have $[\mathcal{O} \colon \mathbb{Z}[\alpha]] = 2$, so that $\operatorname{ann}_{\mathbb{Z}}(\mathcal{O} \colon \mathbb{Z}[\alpha]) = (2) \trianglelefteq \mathbb{Z}$. Hence to compute ramification, for any $p \neq 2$ we may consider the ring $\mathbb{Z}[\alpha]$.

i) Let first $p \mid d$. Then, if $p = 2$ we have d even, so that in any case we may consider the ring $\mathbb{Z}[\alpha]$. Then we have $X^2 - d = X^2 \in \mathbb{F}_p[X]$, which yields the prime divisor $\mathfrak{p} = (p, \alpha) \lhd \mathcal{O}$, such that $p\mathcal{O} = \mathfrak{p}^2$. (Alternatively, we just check that $\mathfrak{p}^2 = (p^2, p\alpha, d) \subseteq (p) \subseteq (p^2) + (d) \subseteq \mathfrak{p}^2 \lhd \mathcal{O}$, hence $\mathfrak{p}^2 = (p)$.)

ii) Hence we may now assume that $p \nmid d$. Let first $p := 2$.

For $d \equiv -1 \pmod 4$ we may consider the ring $\mathbb{Z}[\alpha]$, where we have $X^2 - d = (X + 1)^2 \in \mathbb{F}_2[X]$, which yields the prime divisor $\mathfrak{p} = (2, 1 + \alpha) \lhd \mathcal{O}$, such that $p\mathcal{O} = \mathfrak{p}^2$. (Alternatively, we check that $\mathfrak{p}^2 = (4, 2 + 2\alpha, (d+1) + 2\alpha) = (2) \lhd \mathcal{O}$.)

For $d \equiv 1 \pmod 4$ we have to consider the ring $\mathbb{Z}[\widehat{\alpha}]$:

For $d \equiv 1 \pmod 8$ we have $X^2 - X - \frac{d-1}{4} = X(X + 1) \in \mathbb{F}_2[X]$, yielding the distinct prime divisors $\mathfrak{p} = (2, \widehat{\alpha}) \lhd \mathcal{O}$ and $\overline{\mathfrak{p}} = (2, \widehat{\alpha} + 1) = (2, \overline{\widehat{\alpha}}) \lhd \mathcal{O}$, such that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$. (Alternatively, we just check that $\mathfrak{p}\overline{\mathfrak{p}} = (2, \widehat{\alpha})(2, \overline{\widehat{\alpha}}) = (4, 1 + \alpha, 1 - \alpha, N(\widehat{\alpha})) = (4, 2, 1 + \alpha, \frac{d-1}{4}) = (2) \lhd \mathcal{O}$.)

For $d \equiv -3 \pmod 8$ we have $X^2 - X - \frac{d-1}{4} = X^2 + X + 1 \in \mathbb{F}_2[X]$, which is irreducible. Hence $2\mathcal{O} \lhd \mathcal{O}$ is prime.

iii) Let still $p \nmid d$, but now let p be odd, so that we may consider the ring $\mathbb{Z}[\alpha]$.

Let first $d \in (\mathbb{F}_p^*)^2$, such that $p \mid c^2 - d$ for some $c \in \mathbb{Z} \setminus p\mathbb{Z}$. Then we have $X^2 - d = (X + c)(X - c) \in \mathbb{F}_p[X]$, which yields the distinct prime divisors $\mathfrak{p} = (p, c + \alpha) \lhd \mathcal{O}$ and $\overline{\mathfrak{p}} = (p, c - \alpha) \lhd \mathcal{O}$, such that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$. (Alternatively, we just check that $\mathfrak{p}\overline{\mathfrak{p}} = (p, c + \alpha)(p, c - \alpha) = (p^2, 2pc, p(c + \alpha), c^2 - d) \subseteq (p) \subseteq (p^2) + (2pc) \subseteq \mathfrak{p}\overline{\mathfrak{p}} \lhd \mathcal{O}$, hence $\mathfrak{p}\overline{\mathfrak{p}} = (p)$.)

Let now $d \notin (\mathbb{F}_p^*)^2$. Then $X^2 - d \in \mathbb{F}_p[X]$ is irreducible. Hence letting $\mathfrak{p} \lhd \mathcal{O}$ be a prime divisor of $p\mathcal{O}$, we infer that $\alpha \in \mathcal{O}/\mathfrak{p} =: F$ is a root of $\mu_\alpha \in F[X]$, hence $f = [F \colon \mathbb{F}_p] = 2$. Thus $p\mathcal{O} \lhd \mathcal{O}$ is prime. ♯

Example. For $p = 2$ and $d \equiv 1 \pmod 4$ the ring $\mathbb{Z}[\widehat{\alpha}]$ cannot be avoided, which also shows that the conductor condition in (5.8) cannot be dispensed of:

For $\alpha := \sqrt{-7}$ we have $X^2 + 7 = (X + 1)^2 \in \mathbb{F}_2[X]$, so that letting $\mathcal{O}' := \mathbb{Z}[\alpha]$ we get $2\mathcal{O}' = \mathfrak{q}_2^2$, where $\mathfrak{q}_2 := (2, 1 + \alpha) \lhd \mathcal{O}'$ is prime, while $2\mathcal{O} = \mathfrak{p}_2\overline{\mathfrak{p}}_2$, where $\mathfrak{p}_2 := (2, \widehat{\alpha}) = (\widehat{\alpha}) \lhd \mathcal{O}$ is prime; we have $\mathfrak{p}_2 \neq \overline{\mathfrak{p}}_2$, but $\mathfrak{p}_2 \cap \mathcal{O}' = \mathfrak{q}_2 = \overline{\mathfrak{q}}_2 = \overline{\mathfrak{p}}_2 \cap \mathcal{O}'$.

For $\alpha := \sqrt{-3}$ we have $X^2 + 3 = (X + 1)^2 \in \mathbb{F}_2[X]$, so that letting $\mathcal{O}' := \mathbb{Z}[\alpha]$ we get $2\mathcal{O}' = \mathfrak{q}_2^2$, where $\mathfrak{q}_2 := (2, 1 + \alpha) \lhd \mathcal{O}'$ is prime, while $2\mathcal{O} \lhd \mathcal{O}$ is prime; hence we have $\mathfrak{q}_2^2 = 2\mathcal{O}' \subset 2\mathcal{O} \cap \mathcal{O}' = \mathfrak{q}_2$.

Example: Gaussian numbers. For $d := -1$, we recover the results for $\mathcal{O} = \mathbb{Z}[i]$ in (5.5): An odd prime p is split if $-1 \in (\mathbb{Z}/(p))^*$ is a square, otherwise it is inert; 2 is ramified such that $2\mathcal{O} = (2, 1 + i)^2 = (1 + i)^2 \lhd \mathcal{O}$.

(10.3) Example: The quadratic field $\mathbb{Q}(\sqrt{-17})$. Let $\alpha := \sqrt{-17} \in \mathbb{C}$, let $K := \mathbb{Q}(\alpha)$ and let $\mathcal{O} := \mathcal{O}_K$. Then we get $(2) = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 := (2, 1 + \alpha) \lhd \mathcal{O}$, and $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$, where $\mathfrak{p}_3 := (3, 1 + \alpha) \lhd \mathcal{O}$ and $\overline{\mathfrak{p}}_3 := (3, 1 - \alpha) \lhd \mathcal{O}$.

Thus we get $(18) = (2) \cdot (3)^2 = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^2\overline{\mathfrak{p}}_3^2 \lhd \mathcal{O}$. Moreover, regrouping yields $\mathfrak{p}_3^2 = (9, 3(1+\alpha), 2(1+\alpha), (1+\alpha)^2) = (9, 1+\alpha)$, hence $\mathfrak{p}_2\mathfrak{p}_3^2 = (2, 1+\alpha)(9, 1+\alpha) = (18, 2(1 + \alpha), 9(1 + \alpha), (1 + \alpha)^2) = (1 + \alpha)$, and thus $\mathfrak{p}_2\overline{\mathfrak{p}}_3^2 = (1 - \alpha)$, giving rise to the decomposition $(18) = (1 + \alpha)(1 - \alpha) \lhd \mathcal{O}$.

Since $N(a + b\alpha) = (a + b\alpha)(a - b\alpha) = a^2 + 17b^2$, for $a, b \in \mathbb{Z}$, there is no element of $\mathcal{O}$ of norm 2 or 3. Thus from $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_3) = N(\overline{\mathfrak{p}}_3) = 3$ we infer that none of $\mathfrak{p}_2$ and $\mathfrak{p}_3$ and $\overline{\mathfrak{p}}_3$ is principal. Thus $\mathcal{O}$ is not factorial. (Actually, we will show in (10.4) below that K has class number $h_K = 4$.)

Indeed, the above gives rise to the (non-unique) factorizations $18 = 2 \cdot 3^2 = (1 + \alpha)(1 - \alpha) \in \mathcal{O}$, where the elements occurring are irreducible and pairwise non-associate, hence are not prime. (Note that the factorizations consist of a different number of factors, and multiplicities vary as well.)

(10.4) Class numbers. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be square-free, let $\alpha := \sqrt{d} \in \mathbb{C}$ and $\widehat{\alpha} := \frac{1}{2}(1+\alpha)$, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} = \mathcal{O}_d$ be its ring of integers. Then we have $\mathcal{O} = \mathbb{Z}[\alpha]$ such that $\mathrm{disc}(\mathcal{O}) = 4d$ if $d \not\equiv 1 \pmod 4$, and $\mathcal{O} = \mathbb{Z}[\widehat{\alpha}]$ such that $\mathrm{disc}(\mathcal{O}) = d$ if $d \equiv 1 \pmod 4$.

If $d > 0$ then K has only real embeddings, so that the Minkowski bound is $m_K = M_{2,0} \cdot \sqrt{\mathrm{disc}(\mathcal{O})}$, where $M_{2,0} = \frac{1}{2}$, thus $m_K = \sqrt{d}$ if $d \not\equiv 1 \pmod 4$, and $m_K \sim \frac{1}{2} \cdot \sqrt{d}$ if $d \equiv 1 \pmod 4$.

If $d < 0$ then K has no real embeddings, so that the Minkowski bound is $m_K = M_{0,1} \cdot \sqrt{|\mathrm{disc}(\mathcal{O})|}$, where $M_{0,1} = \frac{2}{\pi}$, thus $m_K \sim 1.28 \cdot \sqrt{|d|}$ if $d \not\equiv 1 \pmod 4$, and $m_K \sim 0.64 \cdot \sqrt{|d|}$ if $d \equiv 1 \pmod 4$.

Thus for smallish d the Minkowski bound is good enough to get down to a sufficiently small set of rational primes, over which a generating set of the class group can be found. A few examples of class numbers are given in Table 8, where $h_{\pm d}$ denotes the class number of $\mathcal{O}_{\pm d}$.

Example: Real quadratic fields. i) Let $d := 2$. Then any ideal class contains an ideal of norm at most $m_K = \sqrt{2} < 2$. Thus any ideal class contains (1), that is K has class number $h_K = 1$.

ii) Let $d := 10$. Then any ideal class contains an ideal of norm at most $m_K = \sqrt{10} < 4$. Thus we only have to consider $\mathcal{P}_K(p)$ for $p \in \{2,3\}$:

We have $\mathcal{P}_K(2) = \{\mathfrak{p}_2\}$, where $\mathfrak{p}_2 = (2,\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_2^2 = (2)$; and we have $\mathcal{P}_K(3) = \{\mathfrak{p}_3, \overline{\mathfrak{p}}_3\}$, where $\mathfrak{p}_3 = (3, 1+\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3)$. Thus we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2, \mathfrak{p}_3 \rangle$, where $\mathfrak{p}_2^2 = 1 \in \mathrm{Cl}_K$ and $\overline{\mathfrak{p}}_3 = \mathfrak{p}_3^{-1} \in \mathrm{Cl}_K$.

We show that $\mathfrak{p}_2$ is not principal: Assume to the contrary that there is $a + b\alpha \in \mathcal{O}$, where $a, b \in \mathbb{Z}$, such that $N(a+b\alpha) = a^2 - 10b^2 = \pm N(\mathfrak{p}_2) = \pm 2$; then we have $a^2 \equiv \pm 2 \pmod 5$, a contradiction.

We have $\mathfrak{p}_2\mathfrak{p}_3 = (2,\alpha)(3,1+\alpha) = (6, 2(1+\alpha), 3\alpha, 10+\alpha) = (6, 2-\alpha, 3\alpha) \lhd \mathcal{O}$; hence $(2-\alpha) \subseteq \mathfrak{p}_2\mathfrak{p}_3$, thus $N(\mathfrak{p}_2\mathfrak{p}_3) = 6 = |N_K(2-\alpha)|$ implies equality. Hence we have $\mathfrak{p}_3 = \mathfrak{p}_2^{-1} = \mathfrak{p}_2 \in \mathrm{Cl}_K$. Thus in conclusion we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle$, where $\mathfrak{p}_2 \in \mathrm{Cl}_K$ has order 2, hence $h_K = 2$. ♯

iii) Let $d := 14$. Then any ideal class contains an ideal of norm at most $m_K = \sqrt{14} < 4$. Thus we only have to consider $\mathcal{P}_K(p)$ for $p \in \{2,3\}$:

We have $\mathcal{P}_K(2) = \{\mathfrak{p}_2\}$, where $\mathfrak{p}_2 = (2,\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}^2 = (2)$; and we have $\mathcal{P}_K(3) = \{(3)\}$, that is 3 is inert, thus $(3) = 1 \in \mathrm{Cl}_K$. Hence we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle$, where $\mathfrak{p}_2^2 = 1 \in \mathrm{Cl}_K$. We have $(4-\alpha) \subseteq \mathfrak{p}_2$, thus $N(\mathfrak{p}_2) = 2 = |N_K(4-\alpha)|$ implies equality. Hence $\mathfrak{p}_2 = 1 \in \mathrm{Cl}_K$, thus $h_K = 1$. ♯

Example: Imaginary quadratic fields. i) For $d \in \{-1, -2\}$, any ideal class contains an ideal of norm at most $m_K \sim 1.28 \cdot \sqrt{2} \sim 1.8 < 2$; for $d := -3$, any ideal class contains an ideal of norm at most $m_K \sim 0.64 \cdot \sqrt{3} \sim 1.10 < 2$. Thus in these cases we have $h_K = 1$. (For $d = -1$ this is not surprising.)

ii) Let $d := -5$. Then any ideal class contains an ideal of norm at most $m_K \sim 1.28 \cdot \sqrt{5} \sim 2.85 < 3$. Thus we only have to consider $\mathcal{P}_K(2)$:

We have $\mathcal{P}_K(2) = \{\mathfrak{p}_2\}$, where $\mathfrak{p}_2 = (2, 1+\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_2^2 = (2)$, so that $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle$, where $\mathfrak{p}_2^2 = 1 \in \mathrm{Cl}_K$. Since there is no element $a + b\alpha \in \mathcal{O}$, where $a, b \in \mathbb{Z}$, such that $N(a+b\alpha) = a^2 + 5b^2 = 2 = N(\mathfrak{p}_2)$, we conclude that $\mathfrak{p}_2$ is not principal, so that $\mathfrak{p}_2 \in \mathrm{Cl}_K$ has order 2, thus $h_K = 2$. ♯

iii) Let $d := -17$. Then any ideal class contains an ideal of norm at most $m_K \sim 1.28 \cdot \sqrt{17} \sim 5.25 < 6$. Thus we only have to consider $\mathcal{P}_K(p)$ for $p \in \{2, 3, 5\}$:

We have $\mathcal{P}_K(2) = \{\mathfrak{p}_2\}$, where $\mathfrak{p}_2 = (2, 1+\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_2^2 = (2)$; next we have $\mathcal{P}_K(3) = \{\mathfrak{p}_3, \overline{\mathfrak{p}}_3\}$, where $\mathfrak{p}_3 = (3, 1+\alpha) \lhd \mathcal{O}$ and $\mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3)$; finally we have $\mathcal{P}_K(5) = \{(5)\}$, that is 5 is inert, so that $(5) = 1 \in \mathrm{Cl}_K$.

Thus we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2, \mathfrak{p}_3 \rangle$, where $\mathfrak{p}_2^2 = 1 \in \mathrm{Cl}_K$ and $\overline{\mathfrak{p}}_3 = \mathfrak{p}_3^{-1} \in \mathrm{Cl}_K$. Since for all $a + b\alpha \in \mathcal{O}$, where $a, b \in \mathbb{Z}$, we have $N(a+b\alpha) = a^2 + 17b^2 \neq 2 = N(\mathfrak{p}_2)$, we conclude that $\mathfrak{p}_2$ is not principal, so that $\mathfrak{p}_2 \in \mathrm{Cl}_K$ has order 2.

We have $\mathfrak{p}_3^2 = (9, 3(1+\alpha), -16 + 2\alpha) = (9, 1+\alpha) \lhd \mathcal{O}$. Since $\pm 3 \in \mathcal{O}$ are the only elements of norm $9 = N(\mathfrak{p}_3^2)$, but $\mathfrak{p}_3^2 \neq (3)$, we conclude that $\mathfrak{p}_3^2$ is not principal. Next, since $N(8-\alpha) = 81$ we have $\mathfrak{p}_3^4 = (81, 9(1+\alpha), -16 + 2\alpha) = (81, (\alpha-1)(8-\alpha), 2(8-\alpha)) \subseteq (8-\alpha) \lhd \mathcal{O}$, which since $N(\mathfrak{p}_3^4) = 81$ implies equality, thus $\mathfrak{p}_3 \in \mathrm{Cl}_K$ has order 4.

Finally, since $N(1+\alpha) = 18$ we have $\mathfrak{p}_2\mathfrak{p}_3^2 = (18, 2(1+\alpha), 9(1+\alpha), (1+\alpha)^2) = (1+\alpha) \lhd \mathcal{O}$, hence $\mathfrak{p}_2\mathfrak{p}_3^2 = 1 \in \mathrm{Cl}_K$, showing that $\mathfrak{p}_2 = \mathfrak{p}_2^{-1} = \mathfrak{p}_3^2 \in \mathrm{Cl}_K$. Thus we conclude that $\mathrm{Cl}_K = \langle \mathfrak{p}_3 \rangle \cong C_4$, hence $h_K = 4$. ♯

iv) Let $d := -19$. Then any ideal class contains an ideal of norm at most $m_K \sim 0.64 \cdot \sqrt{19} \sim 2.77 < 3$. Thus we only have to consider $\mathcal{P}_K(2)$: Since $\mathcal{P}_K(2) = \{(2)\}$, that is 2 is inert, from $(2) = 1 \in \mathrm{Cl}_K$ we conclude that $h_K = 1$.

v) Let $d := -23$. Then any ideal class contains an ideal of norm at most $m_K \sim 0.64 \cdot \sqrt{23} \sim 3.05 < 4$. Thus we only have to consider $\mathcal{P}_K(p)$ for $p \in \{2, 3\}$:

We have $\mathcal{P}_K(2) = \{\mathfrak{p}_2, \overline{\mathfrak{p}}_2\}$, where $\mathfrak{p}_2 = (2, \widehat{\alpha}) \lhd \mathcal{O}$ and $\mathfrak{p}_2\overline{\mathfrak{p}}_2 = (2)$; and we have $\mathcal{P}_K(3) = \{\mathfrak{p}_3, \overline{\mathfrak{p}}_3\}$, where $\mathfrak{p}_3 = (2, 1+\alpha) = (3, 2\widehat{\alpha}) \lhd \mathcal{O}$ and $\mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3)$. Thus we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2, \mathfrak{p}_3 \rangle$, where $\overline{\mathfrak{p}}_2 = \mathfrak{p}_2^{-1} \in \mathrm{Cl}_K$ and $\overline{\mathfrak{p}}_3 = \mathfrak{p}_3^{-1} \in \mathrm{Cl}_K$.

For $a + b\widehat{\alpha} \in \mathcal{O}$, where $a, b \in \mathbb{Z}$, we have $N(a+b\widehat{\alpha}) = (a + \frac{b}{2})^2 + 23 \cdot (\frac{b}{2})^2$; in particular we have $N(a + b\widehat{\alpha}) \neq 2$. Since $N(\widehat{\alpha}) = 6$ we have $\mathfrak{p}_2\mathfrak{p}_3 = (2, \widehat{\alpha})(3, 2\widehat{\alpha}) = (6, \widehat{\alpha}) = (\widehat{\alpha}) \lhd \mathcal{O}$, implying that $\mathfrak{p}_3 = \mathfrak{p}_2^{-1} \in \mathrm{Cl}_K$. Moreover, since $N(\mathfrak{p}_2) = 2$, we conclude that $\mathfrak{p}_2$ is not principal. Using $\widehat{\alpha}^2 = \widehat{\alpha} - 6$ and $N(2 - \widehat{\alpha}) = 8$ we get $\mathfrak{p}_2^3 = (4, 2\widehat{\alpha}, 2+\widehat{\alpha})(2, \widehat{\alpha}) = (4, 2+\widehat{\alpha})(2, \widehat{\alpha}) = (8, 4\widehat{\alpha}, 4+2\widehat{\alpha}, 2+3\widehat{\alpha}) = (8, 2-\widehat{\alpha}) = (2 - \widehat{\alpha}) \lhd \mathcal{O}$. Hence we have $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle$, where $\mathfrak{p}_2$ has order 3, thus $h_K = 3$. ♯

(10.5) Remark: Trivial class group. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, let $K := \mathbb{Q}(\sqrt{d})$, and let $\mathcal{O}_d$ be its ring of integers. We consider the class number problem for quadratic fields, that is we wonder which of them have trivial class

Table 8: Class numbers of quadratic fields.

d	h_d	h_{-d}	d	h_d	h_{-d}	d	h_d	h_{-d}	d	h_d	h_{-d}
1		1	29	1	6	57	1	4	83	1	3
2	1	1	30	2	4	58	2	2	85	2	4
3	1	1	31	1	3	59	1	3	86	1	10
5	1	2	33	1	4	61	1	6	87	2	6
6	1	2	34	2	4	62	1	8	89	1	12
7	1	1	35	2	2	65	2	8	91	2	2
10	2	2	37	1	2	66	2	8	93	1	4
11	1	1	38	1	6	67	1	1	94	1	8
13	1	2	39	2	4	69	1	8	95	2	8
14	1	4	41	1	8	70	2	4	97	1	4
15	2	2	42	2	4	71	1	7	101	1	14
17	1	4	43	1	1	73	1	4	102	2	4
19	1	1	46	1	4	74	2	10	103	1	5
21	1	4	47	1	5	77	1	8	105	2	8
22	1	2	51	2	2	78	2	4	106	2	6
23	1	3	53	1	6	79	3	5	107	1	3
26	2	6	55	2	4	82	4	4	109	1	6

group, or equivalently are factorial. To this end, we again distinguish the cases $d < 0$ and $d > 0$:

a) For $d < 0$, the following deep theorem was conjectured by Gauss [1798]: (For the 'if' direction see Exercise (15.2), and the 'only if' direction is checked for $d \geq -30$ and $d \equiv -1 \pmod 4$ in Exercises (15.5) and (15.8), respectively):

Theorem: [Heegner, 1952; Stark, 1967]**.** The ring $\mathcal{O}_d$ has trivial class group if and only if $d \in \{-1, -2, -3, -7, -11\} \dot\cup \{-19, -43, -67, -163\}$, where the first bunch are the values for which $\mathcal{O}_d$ is Euclidean; see (10.6). ♯

Indeed, for any $h \in \mathbb{N}$ there are only finitely many imaginary quadratic fields having class number h [Goldfield–Gross–Zagier, 1983].

b) In contrast, for $d > 0$ it is still an open problem which rings $\mathcal{O}_d$ have trivial class group, where it is even unknown whether there are infinitely many of them. (Non-factoriality is checked for the cases $d \in \{10, 15, 26, 30\}$, that is all the ones such that $d \leq 30$, in Exercise (15.5).)

(10.6) Remark: Euclidean fields. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, let $K := \mathbb{Q}(\sqrt{d})$, and let $\mathcal{O}_d$ be its ring of integers. We wonder which of the rings $\mathcal{O}_d$ are Euclidean, where in particular $\mathcal{O}_d$ is said to be Euclidean with respect to

the absolute norm map if it has degree map $\delta\colon \mathcal{O}_d \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |N(z)|$; note that the multiplicativity of the norm map implies monotonicity, hence in this case we only have to check for quotient and remainder. We again distinguish the cases $d < 0$ and $d > 0$:

a) For $d < 0$, it is not too difficult to see that for $d \leq -13$ the ring $\mathcal{O}_d$ is not Euclidean with respect to any degree map, see Exercise (15.1). Moreover, it is shown there that $\mathcal{O}_d$ is Euclidean with respect to the absolute norm map for $d \in \{-1, -2, -3, -7, -11\}$. Since for $d \in \{-5, -6, -10\}$ we have already seen in (10.5) that $\mathcal{O}_d$ is not factorial, let alone Euclidean, we get the following:

Theorem. The ring $\mathcal{O}_d$ is Euclidean if and only if it is so with respect to the absolute norm map, which holds if and only if $d \in \{-1, -2, -3, -7, -11\}$. ♯

b) For $d > 0$, it is shown in Exercise (15.1) that $\mathcal{O}_d$ is Euclidean with respect to the absolute norm map for $d \in \{2, 3, 5, 13\}$. Generalizing this method, it is not too difficult to see that for $d \in \{6, 7, 17, 21, 29\}$ the ring $\mathcal{O}_d$ also is Euclidean with respect to the absolute norm map (but still we do not prove this here).

Theorem: [Inkeri, 1949; Chatland–Davenport, 1950]**.** The ring $\mathcal{O}_d$ is Euclidean with respect to the absolute norm map if and only if

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73\}.$$

Actually, there are real quadratic fields which are Euclidean, but are not Euclidean with respect to the absolute norm map, the smallest example being $d = 14$ [Harper, 2004].

Moreover, Harper has shown that all real quadratic fields with trivial class group and discriminant at most 500 are actually Euclidean. Hence, contrary to the picture for imaginary quadratic fields it may be conjectured that a real quadratic field is factorial if and only if it is Euclidean.

11 Quadratic fields: units

(11.1) Units. a) Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, let $\alpha := \sqrt{d}$, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} = \mathcal{O}_d$ be its ring of integers.

Proposition. We have $T(\mathcal{O}^*) = \langle \zeta_4 \rangle = \{\pm 1, \pm i\}$ if $d = -1$, and $T(\mathcal{O}^*) = \langle \zeta_6 \rangle = \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}$ if $d = -3$, and $T(\mathcal{O}^*) = \langle \zeta_2 \rangle = \{\pm 1\}$ otherwise.

Proof. We have to determine the roots of unity contained in K: Since for Euler's totient function we have $\varphi(m) = 2$ if and only if $m \in \{3, 4, 6\}$, we conclude that $T(\mathcal{O}^*) \neq \{\pm 1\}$ if and only if $K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ or $K = \mathbb{Q}(\zeta_4)$.

In the former case, from $\zeta_6 = \frac{1}{2}(1 + \sqrt{-3})$ we get $K = \mathbb{Q}(\sqrt{-3})$ and $T(\mathcal{O}^*) = \langle \zeta_6 \rangle$. In the latter case, from $\zeta_4 = \sqrt{-1}$ we get $K = \mathbb{Q}(i)$ and $T(\mathcal{O}^*) = \langle \zeta_4 \rangle$. ♯

b) Letting $r \in \mathbb{N}_0$ and $s \in \mathbb{N}_0$ be the number of real and pairs of complex conjugate non-real embeddings of K, respectively, we have $r = 2$ and $s = 0$ for $d > 0$, and $r = 0$ and $s = 1$ for $d < 0$. Hence we have $\mathcal{O}^* = T(\mathcal{O}^*)$ for $d < 0$, while $\mathrm{rk}_{\mathbb{Z}}(\mathcal{O}^*/T(\mathcal{O}^*)) = 1$ for $d > 0$.

Thus in the latter case, where $T(\mathcal{O}^*) = \{\pm 1\}$, the remaining task is to determine a fundamental unit in $\mathcal{O}^*$, which is unique up to signs and taking inverses. In order to proceed, we need another classical concept:

(11.2) Continued fractions. We recall a few facts from the theory of continued fractions; for example, see [2, Chapter 5.3], [5, Chapter 10]:

Given $\rho \in \mathbb{R}$ such that $\rho \geq 0$, let

$$\mathrm{cf}[q_1, q_2, \ldots] = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots}}$$

be its **(regular) continued fraction expansion**, where $q_1 \in \mathbb{N}_0$ and $q_i \in \mathbb{N}$ for $i \geq 2$. This is obtained by letting $\rho_1 := \rho$, and then for $i \geq 1$ letting $q_i := \lfloor \rho_i \rfloor$, and if $\rho_i \neq q_i$ then $\rho_{i+1} := \frac{1}{\rho_i - q_i}$; if $\rho_i = q_i$ then we terminate.

a) We assume that $\rho \notin \mathbb{Q}$; equivalently ρ has an infinite continued fraction expansion. Truncating at position $i \in \mathbb{N}$ yields the i-th **convergent** $c_i = \frac{a_i}{b_i} := \mathrm{cf}[q_1, \ldots, q_i] \in \mathbb{Q}$, where $a_i, b_i \in \mathbb{N}_0$. Letting $C_i := \begin{bmatrix} a_{i-1} & b_{i-1} \\ a_i & b_i \end{bmatrix}$ and $Q_i := \begin{bmatrix} 0 & 1 \\ 1 & q_i \end{bmatrix}$, for $i \in \mathbb{N}$, and $C_0 = \begin{bmatrix} a_{-1} & b_{-1} \\ a_0 & b_0 \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, we have $C_i := Q_i \cdot C_{i-1}$.

In particular, the sequences $[a_1, a_2, \ldots]$ and $[b_2, b_3, \ldots]$ are strongly increasing, and we have $a_{i-1}b_i - a_i b_{i-1} = \det(C_i) = -\det(C_{i-1}) = (-1)^i \det(C_0) = (-1)^{i+1}$, which implies that $\gcd(a_i, b_i) = 1$ and $\frac{a_i}{b_i} - \frac{a_{i-1}}{b_{i-1}} = \frac{(-1)^i}{b_i b_{i-1}}$. It follows that $[c_1, c_2, \ldots]$ is a Cauchy sequence, so that $\lim_{i \to \infty} c_i$ exists, where indeed we have $\lim_{i \to \infty} c_i = \rho$. Actually, we have the following:

Theorem: Legendre's Theorem. Let $a \in \mathbb{N}_0$ and $b \in \mathbb{N}$ such that $\gcd(a, b) = 1$, and let $a' \in \{1, \ldots, b\}$ such that $aa' \equiv 1 \pmod{b}$. Then $\frac{a}{b} \in \mathbb{Q}$ is a convergent of ρ, for some $i \in \mathbb{N}$, if and only if $-\frac{1}{b(b+a')} < \rho - \frac{a}{b} < \frac{1}{b(2b-a')}$. ♯

In particular, if $|\rho - \frac{a}{b}| < \frac{1}{2b^2}$ then $\frac{a}{b} \in \mathbb{Q}$ is a convergent of ρ; and for $b = 1$ we get that a is a convergent of ρ if and only if $\rho - 1 < a < \rho + \frac{1}{2}$.

b) As far as periodicity of continued fraction expansions is concerned, we have the following (which does not generalize to higher degrees in any known way):

Theorem: [Euler, 1737; Lagrange, 1766]**.** The positive real number ρ has an (eventually) periodic infinite continued fraction expansion if and only if $\mathbb{Q}(\rho)$ is a (real) quadratic field.

Example. Let $\rho := \sqrt{2} \sim 1.4142136$. Then we get $p_1 := 1$ and $\rho_2 := \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 \sim 2.41$, thus $p_2 := 2$ and $\rho_3 := \frac{1}{(\sqrt{2}+1)-2} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 = \rho_2$; hence we get the periodic continued fraction expansion $\mathrm{cf}[1,\overline{2}] := [1,2,2,\ldots]$. Thus for the convergents $c_i = \frac{a_i}{b_i}$ for $i \in \mathbb{N}$, letting $a_0 = 1$ and $b_0 = 0$, we get $a_1 = 1$ and $b_1 = 1$, and for $i \geq 2$ we get recursively $a_i = a_{i-2} + 2a_{i-1}$ and $b_i = b_{i-2} + 2b_{i-1}$. A few convergents are given in Table 11; this numerically yields $[c_1, \ldots, c_3] = [1, 1.5, 1.4]$, and $[c_4, \ldots, c_{10}]$ are approximately given as

$$[1.4166667, 1.4137931, 1.4142857, 1.4142012, 1.4142157, 1.4142132, 1.4142136].$$

(11.3) Fundamental units in real quadratic fields. Let $1 \neq d \in \mathbb{N}$ be square-free, let $\alpha := \sqrt{d}$ and $K := \mathbb{Q}(\alpha)$, let $\bar{}$ be the non-trivial field automorphism of K, and let $N\colon K \to \mathbb{Q}\colon z = x+y\alpha \mapsto z\overline{z} = (x+y\alpha)(x-y\alpha) = x^2-dy^2$, where $x, y \in \mathbb{Q}$, be the norm map.

Let $\mathcal{O} = \mathcal{O}_d$ be the ring of integers of K, where $\mathcal{O}^* = \{\omega \in \mathcal{O}; N(\omega) = \pm 1\}$. Since for $\omega \in \mathcal{O}^*$ we have $\omega^{-1} = \frac{1}{N(\omega)} \cdot \overline{\omega} \in \mathcal{O}^*$, allowing for signs, and noting that $(x+y\alpha)(x'+y'\alpha) = (xx'+dyy') + (xy'+x'y)\alpha \in K$ for $x, y, x', y' \in \mathbb{Q}$, there is a unique fundamental unit $\epsilon = x + y\alpha \in \mathcal{O}^*$ such that $\epsilon > 1$, having any positive unit as a power; this amounts to saying that $x, y > 0$ are chosen minimal. Note that the trivial case $y = 0$ gives rise to $\{\pm 1\} = T(\mathcal{O}^*)$; and that, since $N\colon \mathcal{O}^* \to \{\pm 1\}$ is a group homomorphism, $1 \in N(\mathcal{O}^*)$, while the latter not necessarily contains -1.

Hence this amounts to solving a diophantine **norm equation**, by finding the **(positive) fundamental solution** $[x, y]$ where $x, y > 0$ are chosen minimal. We distinguish the cases $d \not\equiv 1 \pmod 4$, and $d \equiv 1 \pmod 4$:

i) Let $d \not\equiv 1 \pmod 4$, that is $d \equiv \{-1, 2\} \pmod 4$. Then we have $\mathcal{O} = \{a + b\alpha \in K; a, b \in \mathbb{Z}\}$. Hence we have to solve the diophantine norm equation $X^2 - dY^2 = \delta$ for $\delta \in \{\pm 1\}$, which for $\delta = 1$ is also called **Pell's equation**. In the case $\delta = 1$ there are infinitely many solutions, given by all or only the even powers of ϵ, depending on whether $N(\epsilon) = 1$ or $N(\epsilon) = -1$, respectively.

In the case $\delta = -1$, if $d \equiv -1 \pmod 4$ then d has a prime divisor $p \equiv -1 \pmod 4$, so that $a^2 - db^2 = -1$ implies that -1 is a square modulo p, a contradiction; if $d \equiv -2 \pmod 8$ then $a^2 - db^2 = -1$ implies that a is odd, and thus $2b^2 \equiv -2 \pmod 8$, entailing $b^2 \equiv -1 \pmod 4$, a contradiction. Hence we have solutions in this case possibly only if $d \equiv 2 \pmod 8$ (and if $d \equiv -1 \pmod 4$, which happens for the reduction of case ii) to this case).

• Thus we may simply proceed as follows: Running through $b \in \mathbb{N}$ successively, we just check whether $db^2 \pm 1 \in \mathbb{Z}$ is a square, and if so we return $[\sqrt{db^2 \pm 1}, b]$. But we can avoid sequential search, and can do better:

• From $a^2 - db^2 = \delta$ we get $\frac{a}{b} = \sqrt{d \pm \frac{1}{b^2}}$. Thus, since $\mathbb{R}_{>0} \to \mathbb{R}_{>0}\colon x \mapsto \sqrt{x}$ is strictly convex, having derivative $\mathbb{R}_{>0} \to \mathbb{R}_{>0}\colon x \mapsto \frac{1}{2\sqrt{x}}$, for $\delta = 1$ we get

Table 9: Fundamental units for $d \not\equiv 1 \pmod 4$.

d	N	a	b	reg $\sim$	d	N	a	b	reg $\sim$
2	-1	1	1	0.881	47	1	48	7	4.564
3	1	2	1	1.317	51	1	50	7	4.605
6	1	5	2	2.292	55	1	89	12	5.182
7	1	8	3	2.769	58	-1	99	13	5.288
10	-1	3	1	1.818	59	1	530	69	6.966
11	1	10	3	2.993	62	1	63	8	4.836
14	1	15	4	3.400	66	1	65	8	4.867
15	1	4	1	2.063	67	1	48842	5967	11.489
19	1	170	39	5.829	70	1	251	30	6.219
22	1	197	42	5.976	71	1	3480	413	8.848
23	1	24	5	3.871	74	-1	43	5	4.454
26	-1	5	1	2.312	78	1	53	6	4.663
30	1	11	2	3.089	79	1	80	9	5.075
31	1	1520	273	8.020	82	-1	9	1	2.893
34	1	35	6	4.248	83	1	82	9	5.100
35	1	6	1	2.478	86	1	10405	1122	9.943
38	1	37	6	4.304	87	1	28	3	4.025
39	1	25	4	3.912	91	1	1574	165	8.055
42	1	13	2	3.257	94	1	2143295	221064	15.271
43	1	3482	531	8.849	95	1	39	4	4.357
46	1	24335	3588	10.793	102	1	101	10	5.308

$\left|\alpha - \frac{a}{b}\right| = \sqrt{d + \frac{1}{b^2}} - \sqrt{d} < \frac{1}{2b^2} \cdot \frac{1}{\sqrt{d}} < \frac{1}{2b^2}$, while for $\delta = -1$ we get $\left|\alpha - \frac{a}{b}\right| = \sqrt{d} - \sqrt{d - \frac{1}{b^2}} < \frac{1}{2b^2} \cdot \frac{1}{\sqrt{d - \frac{1}{b^2}}} \leq \frac{1}{2b^2}$. Hence we conclude that any solution $[a, b]$ of the norm equation with $\delta \in \{\pm 1\}$ arises as a convergent $\frac{a}{b}$ of the continued fraction expansion of α. Conversely, since numerators and denominators of the convergents are increasing, in order to determine the fundamental solution we just have to compute the continued fraction expansion of α until we find a convergent $\frac{a}{b}$ such that $a^2 - db^2 \in \{\pm 1\}$.

A few fundamental units $\epsilon = a + b\alpha$ (determined computationally) are collected in Table 9, where $N = N(\epsilon) \in \{\pm 1\}$, and reg $= \ln(\epsilon) \in \mathbb{R}_{>0}$ is the regulator.

ii) Let $d \equiv 1 \pmod 4$. Then we have $\mathcal{O} = \{\frac{1}{2}(a + b\alpha) \in K; a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$. Hence we have to solve the diophantine norm equation $X^2 - dY^2 = \delta$ for $\delta \in \{\pm 4\}$. If $2 \mid ab$, then both a and b are even, so that this case reduces to the equation for $\delta \in \{\pm 1\}$ treated in case i); but note that we possibly have solutions for $\delta = -1$ in this case. Hence we may assume that $2 \nmid ab$. In this case, $a^2 - db^2 = \pm 4$ implies that $1 - d \equiv 4 \pmod 8$, thus we have solutions

possibly only if $d \equiv -3 \pmod 8$.

• Thus we may simply proceed as follows: Running through $b \in \mathbb{N}$ odd successively, we just check whether $db^2 - \delta \in \mathbb{Z}$ is a square, and if so we return $\frac{1}{2} \cdot [\sqrt{db^2 - \delta}, b]$. But again we can avoid sequential search, and can do better:

• From $a^2 - db^2 = \delta$ we get $\frac{a}{b} = \sqrt{d \pm \frac{4}{b^2}}$, thus for $\delta = 4$ and $d \notin \{5, 13\}$ we get $\left|\alpha - \frac{a}{b}\right| = \sqrt{d + \frac{4}{b^2}} - \sqrt{d} < \frac{1}{2b^2} \cdot \frac{4}{\sqrt{d}} \leq \frac{1}{2b^2}$, while for $\delta = -4$ and $d \notin \{5, 13\}$ we get $\left|\alpha - \frac{a}{b}\right| = \sqrt{d} - \sqrt{d - \frac{4}{b^2}} < \frac{1}{2b^2} \cdot \frac{4}{\sqrt{d - \frac{1}{b^2}}} \leq \frac{1}{2b^2} \cdot \frac{4}{\sqrt{d-1}} \leq \frac{1}{2b^2}$. Hence we conclude that, at least for $d \notin \{5, 13\}$, any solution $[a, b]$ of the norm equation with $\delta \in \{\pm 4\}$ also arises as a convergent $\frac{a}{b}$ of the continued fraction expansion of α. In conclusion, in order to determine the fundamental solution we just have to compute the continued fraction expansion of α until we find a convergent $\frac{a}{b}$ such that $a^2 - db^2 \in \{\pm 1, \pm 4\}$.

Actually, for $d = 13$ we have $\epsilon = \frac{1}{2}(3 + \alpha)$, where $\frac{3}{1}$ is the first convergent of the continued fraction expansion of $\alpha \sim 3.61$. But for $d = 5$ we have $\epsilon = \frac{1}{2}(1 + \alpha)$, where $\frac{1}{1}$ is not a convergent of the continued fraction expansion of $\alpha \sim 2.24$.

A few fundamental units (determined computationally) are collected in Table 10, where $\epsilon = a + b\alpha$ if $N = N(\epsilon) \in \{\pm 1\}$, and $\epsilon = \frac{1}{2}(a + b\alpha)$ if $N = N(\epsilon) \in \{\pm 4\}$; moreover, $\mathrm{reg} = \ln(\epsilon) \in \mathbb{R}_{>0}$ denotes the regulator.

(11.4) Example: Units in $\mathbb{Z}[\sqrt{2}]$. a) Let $d = 2$, let $\alpha := \sqrt{2}$, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} := \mathcal{O}_K$. Hence we have the fundamental unit $\epsilon := 1 + \alpha \in \mathcal{O}^*$ such that $\epsilon > 1$, which is associated with the first convergent $c_1 = 1$ of α; see (11.2). For the convergents $c_i = \frac{a_i}{b_i}$, for $i \in \mathbb{N}$, letting $a_0 = 1$ and $b_0 = 0$, we have $a_1 = 1$ and $b_1 = 1$, so that $C_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Letting $Q = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$, for $i \geq 1$ we get $C_i = Q^{i-1} \cdot C_1$ (giving rise to the two-step recursion between the a_i's and the b_i's separately mentioned earlier). Letting $P := C_1^{-1} Q C_1 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}$, we get $C_i = C_1 \cdot P^{i-1} = C_{i-1} \cdot P$, leading to the (one-step) recursion $a_i = a_{i-1} + 2b_{i-1}$ and $b_i = a_{i-1} + b_{i-1}$, for $i \geq 1$; in particular, the a_i are all odd.

Thus we have $a_i + b_i\alpha = (a_{i-1} + b_{i-1}\alpha)(1 + \alpha) = \epsilon^i \in \mathcal{O}^*$ for $i \geq 1$, where $N(\epsilon) = -1$. This shows that all convergents are actually solutions of the norm equation $X^2 - 2Y^2 = \pm 1$, so that the solutions of the latter are precisely the convergents of α; a few powers of ϵ are given in Table 11;

b) We present an application of these observations:

Proposition. Let $s_n := \frac{n(n+1)}{2}$ be the n-th **triangular number**, for $n \in \mathbb{N}$. Then $\{s_n \in \mathbb{N}; s_n \text{ is a square}\}$ is in natural bijection with $\{\epsilon^i \in \mathcal{O}^*; i \in \mathbb{N}\}$. In particular, there are infinitely many squares amongst the triangular numbers.

Table 10: Fundamental units for $d \equiv 1 \pmod 4$.

d	N	a	b	reg $\sim$
5	-4	1	1	0.481
13	-4	3	1	1.195
17	-1	4	1	2.095
21	4	5	1	1.567
29	-4	5	1	1.647
33	1	23	4	3.828
37	-1	6	1	2.492
41	-1	32	5	4.159
53	-4	7	1	1.966
57	1	151	20	5.710
61	-4	39	5	3.664
65	-1	8	1	2.776
69	4	25	3	3.217
73	-1	1068	125	7.667
77	4	9	1	2.185
85	-4	9	1	2.209
89	-1	500	53	6.908
93	4	29	3	3.366
97	-1	5604	569	9.324
101	-1	10	1	2.998

d	N	a	b	reg $\sim$
105	1	41	4	4.407
109	-4	261	25	5.565
113	-1	776	73	7.347
129	1	16855	1484	10.426
133	4	173	15	5.153
137	-1	1744	149	8.157
141	1	95	8	5.247
145	-1	12	1	3.180
149	-4	61	5	4.111
157	-4	213	17	5.361
161	1	11775	928	10.067
165	4	13	1	2.559
173	-4	13	1	2.571
177	1	62423	4692	11.735
181	-4	1305	97	7.174
185	-1	68	5	4.913
193	-1	1764132	126985	15.076
197	-1	14	1	3.333
201	1	515095	36332	13.845
205	4	43	3	3.761

Proof. Let n be odd such that $n(n \pm 1) = 2s^2$ for some $s \in \mathbb{N}$. Then we have $n = m^2$ for some $m \in \mathbb{N}$ such that $m \mid s$; let $l \in \mathbb{N}$ such that $ml = s$. We get $m^2 - 2l^2 = n - \frac{2s^2}{n} = \mp 1$, thus $\frac{m}{l} = \frac{n}{s}$ is the i-th convergent of α, where i is odd if the right hand side is -1, while i is even if the right hand side is 1.

Conversely, given $c_i = \frac{m}{l}$ for some $i \in \mathbb{N}$, then m is odd, and letting $n := m^2$ and $s := ml$ we get $(-1)^i = m^2 - 2l^2 = n - \frac{2s^2}{n}$, hence $n(n \pm 1) = 2s^2$, where n is odd, and the '+' case holds if i is odd, while the '$-$' case holds if i is even. ♯

(11.5) Example: Archimedes's Problema Bovinum. We present a larger example, showing the efficiency of the continued fraction approach, which comes up in the solution of **cattle problem of Archimedes**, see Exercise (15.37):

Let $d := 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 = 4729494$ and $\widehat{d} := d \cdot (2 \cdot 4657)^2 = 410286423278424$. We look for the fundamental solution of Pell's equation for $\widehat{d}$. To this end, since $\widehat{d}$ is not square-free, we first consider Pell's equation for d:

Computationally we find that the continued fraction expansion of $\sqrt{d}$ is periodic

Table 11: Units in $\mathbb{Z}[\sqrt{2}]$ and triangular numbers.

i	a_i	b_i	n	$s = \sqrt{s_n}$
0	1	0	0	0
1	1	1	1	1
2	3	2	8	6
3	7	5	49	35
4	17	12	288	204
5	41	29	1681	1189
6	99	70	9800	6930
7	239	169	57121	40391
8	577	408	332928	235416
9	1393	985	1940449	1372105
10	3363	2378	11309768	7997214
11	8119	5741	65918161	46611179
12	19601	13860	384199200	271669860
13	47321	33461	2239277041	1583407981
14	114243	80782	13051463048	9228778026
15	275807	195025	76069501249	53789260175

---

of period length 92, from position $i = 2$ on, and reads

$$\mathrm{cf}[2174; \overline{1, 2, 1, 5, 2, 25, 3, 1, 1, 1, 1, 1, 1, 15, 1, 2, 16, 1, 2, 1, 1, 8, 6, 1, 21, 1, 1, 3, 1,}$$
$$\overline{1, 1, 2, 2, 6, 1, 1, 5, 1, 17, 1, 1, 47, 3, 1, 1, 6, 1, 1, 3, 47, 1, 1, 17, 1, 5, 1, 1, 6, 2, 2, 1,}$$
$$\overline{1, 1, 3, 1, 1, 21, 1, 6, 8, 1, 1, 2, 1, 16, 2, 1, 15, 1, 1, 1, 1, 1, 1, 3, 25, 2, 5, 1, 2, 1, 4348}].$$

It turns out that the 92-nd convergent of $\sqrt{d}$ equals

$$c_{92} = \frac{a_{92}}{b_{92}} = \frac{1099319867328297349798662328214335439010880 49}{505494852343150330744778197355404089863 40},$$

which is the first one such that $N_{\mathbb{Q}(\sqrt{d})}(a_{92} + b_{92}\sqrt{d}) = \pm 1$, where actually the '+' sign holds. Thus we conclude that $\epsilon := a_{92} + b_{92}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is the fundamental unit fulfilling $\epsilon > 1$; we have $a_{92} \sim 1.1 \cdot 10^{44}$ and $b_{92} \sim 5.05 \cdot 10^{40}$. The solutions $[\widehat{a}, \widehat{b}] \in \mathbb{Z}^2$ of $X^2 - \widehat{d}Y^2 = X^2 - d \cdot (2 \cdot 4657 \cdot Y)^2 = 1$ are in bijection with the solutions $[a, b]$ of $X^2 - dY^2 = 1$ by $\widehat{a} = a$ and $(2 \cdot 4657) \cdot \widehat{b} = b$ Thus we look for the smallest power $\epsilon^k = a + b\sqrt{d}$, for some $k \in \mathbb{N}$, such that $(2 \cdot 4657) \mid b$; note that we have not yet seen that such a solution exists at all:

It turns out that $k = 2329$, where $a \sim 3.765 \cdot 10^{103272}$ and $b \sim 1.7 \cdot 10^{103269}$, so that $\widehat{b} \sim 1.86 \cdot 10^{103265}$ (where we do not print out these figures explicitly). ♯

12 Cyclotomic fields: algebra

(12.1) Cyclotomic fields. For $m \in \mathbb{N}$ let $\zeta_m := \exp(\frac{2\pi i}{m}) \in \mathbb{C}$ be a primitive m-th root of unity; actually this is a particular choice which is algebraically irrelevant, but not so analytically.

The associated minimum polynomial over $\mathbb{Q}$ is the m-th **cyclotomic polynomial** $\mu_{\zeta_m} := \Phi_m \in \mathbb{Z}[X]$. It splits as $\Phi_m = \prod_{k \in (\mathbb{Z}/(m))^*}(X - \zeta_m^k) \in \mathbb{C}[X]$, that is its roots are all the primitive m-th roots of unity, where the latter are precisely the generators of μ_m. In particular, we have $\deg(\Phi_m) = \varphi(m)$, where the latter is **Euler's totient function**.

Let $\mathbb{Q}(\zeta_m)$ be the associated **cyclotomic field**, which is Galois over $\mathbb{Q}$ of degree $[\mathbb{Q}(\zeta_m)\colon \mathbb{Q}] = \varphi(m)$. We have $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \cong (\mathbb{Z}/(m))^*$, where the field automorphism associated with $k \in (\mathbb{Z}/(m))^*$ is given by $\sigma_k\colon \zeta \mapsto \zeta^k$; in particular σ_{-1} coincides with complex conjugation.

Let $\mathcal{O}_m := \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ be the ring of integers of $\mathbb{Q}(\zeta_m)$. Since $\Phi_m \in \mathbb{Z}[X]$ we have $\mathbb{Z}[\zeta_m] \subseteq \mathcal{O}_m$. We proceed to show that we actually have equality, where we first consider the prime power case, which is interesting in itself:

(12.2) The prime power case. Let first $q := p^\nu \in \mathbb{N}$, where $p \in \mathcal{P}_{\mathbb{Z}}$ and $\nu \in \mathbb{N}$, let $K_q := \mathbb{Q}(\zeta_q)$, and let $\mathcal{O}_q := \mathcal{O}_{K_q}$; hence $n := [K_q\colon \mathbb{Q}] = \varphi(q) = p^{\nu-1}(p-1)$.

Proposition. Then $(1-\zeta_q) \lhd \mathcal{O}_q$ is prime such that $N(1-\zeta_q) = p$, and we have $p\mathcal{O}_q = (1-\zeta_q)^n \lhd \mathcal{O}_q$; in other words p is completely ramified in K_q.

Proof. Letting $q' := p^{\nu-1} \in \mathbb{N}$ we have $\Phi_q = \frac{X^q-1}{X^{q'}-1} = \sum_{i=0}^{p-1} X^{iq'} \in \mathbb{Z}[X]$. Thus evaluating at $X \mapsto 1$ yields $p = \Phi_q(1) = \prod_{k \in (\mathbb{Z}/(q))^*}(1-\zeta_q^k) = N(1-\zeta_q)$. Hence in particular $(1-\zeta_q) \lhd \mathcal{O}_q$ is prime.

Moreover, for $k \in (\mathbb{Z}/(q))^*$, where we may assume that $k \in \{0, \ldots, q-1\}$, we get $1-\zeta_q^k = (1-\zeta_q) \cdot \sum_{i=0}^{k-1} \zeta_q^i \in \mathcal{O}_q$, thus $(1-\zeta_q) \mid (1-\zeta_q^k)$. By symmetry, we also have $(1-\zeta_q^k) \mid (1-\zeta_q)$, entailing that $(1-\zeta_q) \sim (1-\zeta_q^k) \in \mathcal{O}_q$. Hence we infer that $p\mathcal{O}_q = \prod_{k \in (\mathbb{Z}/(q))^*}(1-\zeta_q) = (1-\zeta_q)^{\varphi(q)} \lhd \mathcal{O}_q$. ♯

Theorem. We have $\mathcal{O}_q = \mathbb{Z}[\zeta_q]$, having discriminant $\mathrm{disc}(\mathcal{O}_q) = \epsilon \cdot p^\delta$, where $\delta := p^{\nu-1}(\nu p - \nu - 1)$ and $\epsilon := (-1)^{\binom{\varphi(q)}{2}}$.

In particular, $\mathrm{disc}(\mathcal{O}_q) \mid p^{\nu p^{\nu-1}(p-1)} = q^{\varphi(q)}$, and $\mathrm{disc}(\mathcal{O}_p) = (-1)^{\binom{p-1}{2}} \cdot p^{p-2}$.

Proof. i) We first determine $\mathrm{disc}(\mathbb{Z}[\zeta_q]) = \mathrm{disc}(\zeta_q)$: To this end, differentiating the equation $X^q - 1 = \Phi_q \cdot (X^{q'} - 1) \in \mathbb{Z}[X]$, where $q' := p^{\nu-1}$, we get $qX^{q-1} = (\partial\Phi_q) \cdot (X^{q'} - 1) + q'\Phi_q \cdot X^{q'-1} \in \mathbb{Z}[X]$. Evaluating at $X \mapsto \zeta_q$ yields $q\zeta_q^{-1} = (\partial\Phi_q)(\zeta_q) \cdot (\zeta_q^{q'} - 1) \in K_q$, that is $(\partial\Phi_q)(\zeta_q) = \frac{-q\zeta_q^{-1}}{1-\zeta_p} \in K_q$.

We have $N(-q) = (-q)^n$ and $N(\zeta_q) = (-1)^n \cdot \Phi_q(0) = (-1)^n$, hence we get $N(-q\zeta_q^{-1}) = q^n$. Moreover, for the case $\nu = 1$, where $[K_p\colon \mathbb{Q}] = p-1$, we get $N(1-\zeta_p) = (N_{\mathbb{Q}(\zeta_p)}(1-\zeta_p))^{q'} = p^{q'}$. Thus we obtain $\operatorname{disc}(\zeta_q) = (-1)^{\binom{n}{2}} \cdot N((\partial\Phi_q)(\zeta_q)) = (-1)^{\binom{n}{2}} \cdot \frac{q^n}{p^{q'}} = (-1)^{\binom{n}{2}} \cdot p^{\nu n - q'}$, where $\epsilon := (-1)^{\binom{n}{2}} = (-1)^{\binom{\varphi(q)}{2}}$ and $\delta := \nu n - q' = \nu p^{\nu-1}(p-1) - p^{\nu-1} = p^{\nu-1}(\nu p - \nu - 1)$.

ii) Since $p\mathcal{O}_q = (1-\zeta_q)^n \lhd \mathcal{O}_q$ is completely ramified, we have $\mathcal{O}_q/(1-\zeta_q) \cong \mathbb{Z}/p\mathbb{Z}$ as rings. We show that $\langle 1, \zeta_q, \ldots, \zeta_q^{k-1}\rangle_{\mathbb{Z}} + (1-\zeta_q)^k\mathcal{O}_q = \mathcal{O}_q$ as Abelian groups, for all $k \in \mathbb{N}$: (Note that the left hand summand stabilizes for $k \geq n$, while the right hand summand gets strictly smaller for increasing k.)

For $k = 1$ we indeed have $\mathbb{Z} + (1-\zeta_q)\mathcal{O}_q = \mathcal{O}_q$. For $k \geq 2$, by induction we have $(1-\zeta_q)\mathcal{O}_q = (1-\zeta_q)\cdot\langle 1, \zeta_q, \ldots, \zeta_q^{k-2}\rangle_{\mathbb{Z}} + (1-\zeta_q)^k\mathcal{O}_q$, hence $\mathcal{O}_q = \mathbb{Z} + (1-\zeta_q)\mathcal{O}_q = \mathbb{Z} + (1-\zeta_q)\cdot\langle 1, \zeta_q, \ldots, \zeta_q^{k-2}\rangle_{\mathbb{Z}} + (1-\zeta_q)^k\mathcal{O}_q = \langle 1, \zeta_q, \ldots, \zeta_q^{k-1}\rangle_{\mathbb{Z}} + (1-\zeta_q)^k\mathcal{O}_q$.

Now we have $\operatorname{disc}(\mathbb{Z}[\zeta_q]) = [\mathcal{O}_q\colon \mathbb{Z}[\zeta_q]]^2 \cdot \operatorname{disc}(\mathcal{O}_q)$, so that $[\mathcal{O}_q\colon \mathbb{Z}[\zeta_q]] \mid p^\delta$, hence $p^\delta\mathcal{O}_q \subseteq \mathbb{Z}[\zeta_q] \subseteq \mathcal{O}_q$. Thus for $k := n\delta$, since $(1-\zeta_q)^n\mathcal{O}_q = p\mathcal{O}_q$, we get $\mathbb{Z}[\zeta_q] \subseteq \mathcal{O}_q = \langle 1, \zeta_q, \ldots, \zeta_q^{n\delta-1}\rangle_{\mathbb{Z}} + p^\delta\mathcal{O}_q \subseteq \mathbb{Z}[\zeta_q]$, hence $\mathcal{O}_q = \mathbb{Z}[\zeta_q]$. ♯

(12.3) The general case. Let $m = \prod_{i=1}^r p_i^{\nu_i} \in \mathbb{N}$, where $\{p_1, \ldots, p_r\} \subseteq \mathcal{P}_\mathbb{Z}$ are pairwise distinct, and $\nu_1, \ldots, \nu_r \in \mathbb{N}$, for some $r \in \mathbb{N}_0$, let $K_m := \mathbb{Q}(\zeta_m)$, and let $\mathcal{O}_m := \mathcal{O}_{K_m}$.

Theorem. We have $\mathcal{O}_m = \mathbb{Z}[\zeta_m]$, having discriminant $\operatorname{disc}(\mathcal{O}_m) \mid m^{\varphi(m)}$.

Proof. Letting $q_i := p_i^{\nu_i}$ and $m_i := \frac{m}{q_i}$, we have $\zeta_{q_i} = \zeta_m^{m_i}$, so that $K_{q_i} \subseteq K_m$, where $\operatorname{disc}(K_{q_i}) \mid q_i^{\varphi(q_i)}$. Conversely, since $\prod_{i=1}^r \zeta_{q_i}$ is a primitive m-th root of unity, we infer that $K_m \subseteq \prod_{i=1}^r K_{q_i}$, hence equality holds. Since Euler's totient function is multiplicative with respect to coprime arguments, we indeed have $[K_m\colon \mathbb{Q}] = \varphi(m) = \prod_{i=1}^r \varphi(q_i) = \prod_{i=1}^r [K_{q_i}\colon \mathbb{Q}]$.

Since the discriminants of the K_{q_i} are pairwise coprime, by (3.8) we conclude that $\mathbb{Z}[\zeta_m] \subseteq \mathcal{O}_m = \prod_{i=1}^r \mathcal{O}_{q_i} = \prod_{i=1}^r \mathbb{Z}[\zeta_{q_i}] \subseteq \mathbb{Z}[\zeta_m]$, hence equality holds. We have $K_{m_i} = \prod_{j\neq i} K_{q_j}$, which entails $\operatorname{disc}(\mathcal{O}_m) = \prod_{i=1}^r \operatorname{disc}(\mathcal{O}_{q_i})^{[K_{m_i}\colon \mathbb{Q}]} \mid \prod_{i=1}^r q_i^{\varphi(q_i)\cdot\prod_{j\neq i}\varphi(q_j)} = (\prod_{i=1}^r q_i)^{\varphi(m)} = m^{\varphi(m)}$. ♯

(12.4) Ramification. Let $m = \prod_{p\in\mathcal{P}_\mathbb{Z}} p^{\nu_p} \in \mathbb{N}$, where $\nu_p \in \mathbb{N}_0$, let $K_m := \mathbb{Q}(\zeta_m)$, and let $\mathcal{O}_m := \mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$.

For $p \in \mathcal{P}_\mathbb{Z}$ let $q := p^{\nu_p}$ and $s := \frac{m}{q}$. Since q and s are coprime, we have $\mathbb{Z}/(m) \cong \mathbb{Z}/(q) \oplus \mathbb{Z}/(s)$, implying $\operatorname{Aut}_\mathbb{Q}(K_m) \cong (\mathbb{Z}/(m))^* \cong (\mathbb{Z}/(q))^* \times (\mathbb{Z}/(s))^* \cong \operatorname{Aut}_\mathbb{Q}(K_q) \times \operatorname{Aut}_\mathbb{Q}(K_s)$; in particular we have $\varphi(m) = \varphi(q)\varphi(s)$. Hence we have $K_m = K_qK_s$ such that $K_q \cap K_s = \mathbb{Q}$.

Theorem. Let $\mathfrak{p} \in \mathcal{P}_{K_m}(p)$. Then we have $e(\mathfrak{p}) = \varphi(p^{\nu_p})$, and $f(\mathfrak{p}) \in \mathbb{N}$ is minimal such that $p^{f(\mathfrak{p})} \equiv 1 \pmod{\frac{m}{p^{\nu_p}}}$.

Proof. Let $\Phi_m \in \mathbb{Z}[X]$ be the m-th cyclotomic polynomial. Then, letting $\overline{\ }\colon \mathcal{O}_m \to \mathcal{O}_m/\mathfrak{p}$ denote the natural epimorphism, $\overline{\Phi}_m \in \mathbb{F}_p[X]$ has irreducible divisors of the same degree $f(\mathfrak{p}) := [\mathcal{O}_m/\mathfrak{p}\colon \mathbb{F}_p]$, all occurring with the same multiplicity $e(\mathfrak{p})$. Hence we have $|\mathcal{P}_{K_m}(p)| \cdot e(\mathfrak{p}) \cdot f(\mathfrak{p}) = \varphi(m)$.

i) We first consider K_q: Let $\mathfrak{q} := \mathfrak{p} \cap \mathcal{O}_q \lhd \mathcal{O}_q$. We have already seen that p is completely ramified in $\mathcal{O}_q$, so that $p\mathcal{O}_q = \mathfrak{q}^{\varphi(q)}$ where $\mathfrak{q} = (\zeta_q - 1) \lhd \mathcal{O}_q$; hence $\mathcal{P}_{K_q}(p) = \{\mathfrak{q}\}$ and $e(\mathfrak{q}) = \varphi(q)$ and $f(\mathfrak{q}) = 1$.

ii) We now consider K_s: Let $\mathfrak{s} := \mathfrak{p} \cap \mathcal{O}_s \lhd \mathcal{O}_s$. From $\gcd(X^s - 1, \partial(X^s - 1)) = \gcd(X^s - 1, sX^{s-1}) \in \mathbb{F}_p[X]$ being constant we infer that $X^s - 1 \in \mathbb{F}_p[X]$ is square-free. In particular, $\overline{\Phi}_s \in \mathbb{F}_p[X]$ is square-free as well, so that p is unramified in $\mathcal{O}_s$, that is $e(\mathfrak{s}) = 1$. (Alternatively, this also follows from $\operatorname{disc}(\mathcal{O}_s) \mid s^{\varphi(s)}$ and $p \nmid s$.)

We have $F := \mathcal{O}_s/\mathfrak{s} = \mathbb{Z}[\zeta_s]/\mathfrak{s} = \mathbb{F}_p(\overline{\zeta}_s) \cong \mathbb{F}_p[X]/(\mu_{\overline{\zeta}_s})$, where $\mu_{\overline{\zeta}_s} \in \mathbb{F}_p[X]$ is the minimum polynomial of $\overline{\zeta}_s$ over $\mathbb{F}_p$. Since $\overline{\zeta}_s \in F$ is a root of $\overline{\Phi}_s \in \mathbb{F}_p[X] \subseteq F[X]$, where the latter splits over $\mathbb{F}_p$ into irreducible factors of degree $f(\mathfrak{s})$, we get $\mu_{\overline{\zeta}_s} \mid \overline{\Phi}_s \in \mathbb{F}_p[X]$, implying that $f(\mathfrak{s}) = [F\colon \mathbb{F}_p] = \deg(\mu_{\overline{\zeta}_s})$. Moreover, since $X^s - 1 \in F[X]$ splits completely and square-freely, the natural map $\langle \zeta_s \rangle \to \langle \overline{\zeta}_s \rangle$ is a group isomorphism, that is $\overline{\zeta}_s$ is a primitive s-th root of unity.

The field extension $\mathbb{F}_p \subseteq F$ is Galois such that $\operatorname{Aut}_{\mathbb{F}_p}(F) = \langle \varphi_p \rangle \cong C_{f(\mathfrak{s})}$, where φ_p is the Frobenius automorphism. Thus $f := f(\mathfrak{s}) \in \mathbb{N}$ is minimal such that $\overline{\zeta}_s = (\overline{\zeta}_s)^{\varphi_p^f} = \overline{\zeta}_s^{\,p^f}$, that is $\overline{\zeta}_s^{\,p^f - 1} = 1$, or equivalently, since $\overline{\zeta}_s$ is a primitive s-th root of unity, we have $s \mid p^f - 1$. Thus $f(\mathfrak{s})$ is the order of $p \in (\mathbb{Z}/(s))^*$, and we have $|\mathcal{P}_{K_s}(p)| \cdot f(\mathfrak{s}) = \varphi(s)$; note that indeed $f(\mathfrak{s}) \mid |(\mathbb{Z}/(s))^*| = \varphi(s)$.

iii) In combination, by multiplicativity of ramification indices and inertia degrees, and recalling that the elements of $\mathcal{P}_{K_m}(p)$ are all conjugate, we have $e(\mathfrak{q}) \mid e(\mathfrak{p})$, as well as $f(\mathfrak{s}) \mid f(\mathfrak{p})$ and $|\mathcal{P}_{K_s}(p)| \mid |\mathcal{P}_{K_m}(p)|$. This yields $\varphi(m) = \varphi(s) \cdot \varphi(q) = |\mathcal{P}_{K_s}(p)| \cdot f(\mathfrak{s}) \cdot e(\mathfrak{q}) \mid |\mathcal{P}_{K_m}(p)| \cdot f(\mathfrak{p}) \cdot e(\mathfrak{p}) = \varphi(m)$, entailing equality $e(\mathfrak{p}) = e(\mathfrak{q}) = \varphi(q)$ and $f(\mathfrak{p}) = f(\mathfrak{s})$. ♯

Corollary. We have $I_\mathfrak{p} = K_s$ and $D_\mathfrak{p} = \operatorname{Fix}_{K_s}(\widehat{\varphi}_p)$.

Proof. By the characterization of inertia fields, from $e(\mathfrak{s}) = 1$ we conclude that $K_s \subseteq I_\mathfrak{p}$, where from $e(\mathfrak{p}) = [K_m\colon I_\mathfrak{p}] \mid [K_m\colon K_s] = \frac{\varphi(m)}{\varphi(s)} = \varphi(q) = e(\mathfrak{p})$ we infer that equality $I_\mathfrak{p} = K_s$ holds.

Thus, letting $G := (\mathbb{Z}/(m))^* \cong \operatorname{Aut}_\mathbb{Q}(K_m)$, since $K_s = \operatorname{Fix}_{K_m}(G^0_\mathfrak{p})$ we conclude that the inertia group is $G^0_\mathfrak{p} = (\mathbb{Z}/(q))^*$, where $\operatorname{Aut}_\mathbb{Q}(K_s) \cong G/G^0_\mathfrak{p} \cong (\mathbb{Z}/(s))^*$.

Now $\widehat{\varphi}_p := p + (s) \in (\mathbb{Z}/(s))^*$ induces the Frobenius automorphism φ_p on $\mathcal{O}_m/\mathfrak{p} \cong \mathcal{O}_s/\mathfrak{s}$; note that since p is unramified in K_s the Frobenius lift $\widehat{\varphi}_p$ is uniquely defined. Hence the decomposition group is $G_\mathfrak{p} = G^0_\mathfrak{p} \times \langle \widehat{\varphi}_p \rangle$ and the decomposition field is $D_\mathfrak{p} = \operatorname{Fix}_{K_m}(G_\mathfrak{p}) = \operatorname{Fix}_{K_s}(\widehat{\varphi}_p)$. ♯

(12.5) Quadratic residues. a) Let $p \in \mathcal{P}_{\mathbb{Z}}$ be odd. Then $a \in \mathbb{Z}$ such that $p \nmid a$ is called a **quadratic residue** modulo p, if there is $b \in \mathbb{Z}$ such that $a = b^2 \in (\mathbb{Z}/(p))^*$, otherwise it is called a **quadratic non-residue**. Let $\mathcal{Q}_p := \{a \in (\mathbb{Z}/(p))^*; a \in \mathbb{Z} \text{ quadratic residue}\}$ and $\mathcal{N}_p := \{a \in (\mathbb{Z}/(p))^*; a \in \mathbb{Z} \text{ quadratic non-residue}\}$ be the sets of **squares** and **non-squares**, respectively.

For $a \in \mathbb{Z}$ such that $p \nmid a$ the **Legendre symbol** is defined as $\left(\frac{a}{p}\right) := 1$ if $a \in \mathcal{Q}_p$, and $\left(\frac{a}{p}\right) := -1$ if $a \in \mathcal{N}_p$; in particular $\left(\frac{a}{p}\right)$ only depends on the congruence class of a modulo p. Since $(\mathbb{Z}/(p))^* = \langle \rho \rangle \cong C_{p-1}$, the Legendre symbol $\left(\frac{\cdot}{p}\right)$ coincides with the natural group epimorphism $(\mathbb{Z}/(p))^* \to \{\pm 1\}$ given by $\rho \mapsto -1$. Hence $\mathcal{Q}_p = \ker(\left(\frac{\cdot}{p}\right)) \leq (\mathbb{Z}/(p))^*$ is the unique subgroup of index 2, consisting of the elements of $(\mathbb{Z}/(p))^*$ of order dividing $\frac{p-1}{2}$.

Proposition: Euler criterion. We have $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Proof. If $\left(\frac{a}{p}\right) = 1$, then $a^{\frac{p-1}{2}} = 1 \in (\mathbb{Z}/(p))^*$. If $\left(\frac{a}{p}\right) = -1$, then $a^{p-1} = 1 \in (\mathbb{Z}/(p))^*$ implies $a^{\frac{p-1}{2}} = -1 \in (\mathbb{Z}/(p))^*$, being the unique element of order 2. ♯

Corollary: First supplement to the Quadratic Reciprocity Law. We have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, that is $-1 \in \mathcal{Q}_p$ if and only if $p \equiv 1 \pmod{4}$.

b) In order to compute Legendre symbols, using multiplicativity it suffices to be able to determine $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, as well as $\left(\frac{l}{p}\right)$, where $l \in \mathcal{P}_{\mathbb{Z}}$ is odd such that $l \neq p$. We have already dealt with the case $\left(\frac{-1}{p}\right)$, in terms of p.

To proceed, we observe that the Legendre symbols $\left(\frac{2}{p}\right)$ and $\left(\frac{l}{p}\right)$ relate to the ramification of primes in quadratic fields as follows, giving a description in terms of the 'numerator' 2 and l, respectively:

Corollary. If $d \in \mathbb{Z} \setminus \{0, 1\}$ is square-free such that $p \nmid d$, then $\left(\frac{d}{p}\right) = 1$ if and only if p splits in the quadratic field $\mathbb{Q}(\sqrt{d})$.

The content of the Quadratic Reciprocity Law is to describe $\left(\frac{2}{p}\right)$ and $\left(\frac{l}{p}\right)$ similarly, but now 'reciprocally' in terms of the 'denominator' p:

(12.6) Reciprocity. Let $p \in \mathcal{P}_{\mathbb{Z}}$ be odd, and let $K := \mathbb{Q}(\zeta_p)$.

We have $\mathrm{Aut}_{\mathbb{Q}}(K) \cong G := (\mathbb{Z}/(p))^* = \langle \rho \rangle \cong C_{p-1}$. Hence for any $s \in \mathbb{N}$ dividing $p-1$ there is a unique subgroup $G^{(s)} = \langle \rho^s \rangle \leq G$ of index s; then $G^{(s)} \cong C_{\frac{p-1}{s}}$

consists of the elements of G of order dividing $\frac{p-1}{s}$, or equivalently being s-th powers; in particular, we have $G^{(2)} = \mathcal{Q}_p$, being the subgroup of squares. Moreover, for $t \mid (p-1)$ we have $t \mid s$ if and only if $G^{(s)} \leq G^{(t)}$.

Thus K has a unique subfield $K^{(s)} = \mathrm{Fix}_K(G^{(s)})$ of degree $[K^{(s)}\colon \mathbb{Q}] = s$. In particular, $K^{(2)}$ is the unique quadratic subfield of K. Moreover, for $t \mid (p-1)$ we have $t \mid s$ if and only if $K^{(t)} \subseteq K^{(s)}$.

Theorem. Let $l \in \mathcal{P}_\mathbb{Z}$ such that $l \neq p$. Then the following are equivalent:
i) $l \in (\mathbb{Z}/(p))^*$ is an s-th power; **ii)** $s \mid |\mathcal{P}_K(l)|$; **iii)** l splits completely in $K^{(s)}$.

Proof. Let $r := |\mathcal{P}_K(l)|$, and let $f := f(\mathfrak{q})$, for any $\mathfrak{q} \in \mathcal{P}_K(l)$. Then f equals the order of $l \in (\mathbb{Z}/(p))^* = G$, and since l is unramified in K we have $rf = p-1$. Moreover, we have $I_\mathfrak{q} = K$, and thus $D_\mathfrak{q} \subseteq K$ is the unique subfield of index f, that is of degree $\frac{p-1}{f} = r$ over $\mathbb{Q}$, hence we have $D_\mathfrak{q} = K^{(r)}$.

Now l is a s-th power in G if and only if f divides $\frac{p-1}{s} = \frac{rf}{s}$, or equivalently $s \mid r$, that is $K^{(s)} \subseteq K^{(r)} = D_\mathfrak{q}$. By the characterization of decomposition fields, and G being Abelian, this is to say that l splits completely in $K^{(s)}$. ♯

(12.7) Quadratic reciprocity. Let $p \in \mathcal{P}_\mathbb{Z}$ be odd, let $K := \mathbb{Q}(\zeta_p)$, let $G := (\mathbb{Z}/(p))^*$, and let $l \in \mathcal{P}_\mathbb{Z}$ such that $l \neq p$. We are going to describe whether or not $l \in \mathcal{Q}_p \leq G$, which is equivalent to asking whether or not l splits (completely) in the unique quadratic subfield $K^{(2)}$ of K. In order to describe $K^{(2)}$, let $p^* := \left(\frac{-1}{p}\right) \cdot p = (-1)^{\frac{p-1}{2}} \cdot p$, that is $p^* = \pm p$ for $p \equiv \pm 1 \pmod 4$.

Proposition. The field $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.

Proof. Let $\zeta := \zeta_p$, and let $D := K^{(2)} = \mathrm{Fix}_K(\mathcal{Q}_p)$; hence $D \subseteq K$ is Galois such that $\mathrm{Aut}_D(K) \cong \mathcal{Q}_p$, and $\mathbb{Q} \subseteq D$ is Galois such that $\mathrm{Aut}_\mathbb{Q}(D) \cong G/\mathcal{Q}_p \cong C_2$.

We consider the **Gaussian sum** $\beta := T_{K/D}(\zeta) = \sum_{k \in \mathcal{Q}_p} \zeta^k \in D$. The non-trivial $\mathrm{Aut}_\mathbb{Q}(D)$-conjugate of β is $\beta' := \beta^{\sigma_a} = \sum_{k \in \mathcal{Q}_p} \zeta^{ak} = \sum_{k \in \mathcal{N}_p} \zeta^k \in D$, for any $a \in \mathcal{N}_p$. Let $\gamma := \beta - \beta' = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k \in D$. Since $\{\zeta, \ldots, \zeta^{p-1}\} = \zeta \cdot \{1, \zeta, \ldots, \zeta^{p-2}\} \subseteq K$ is a $\mathbb{Q}$-basis, we have $\gamma \neq 0$. Moreover, we have $\gamma^{\sigma_a} = \beta' - \beta = -\gamma$, for any $a \in \mathcal{N}_p$. Hence $D = \mathbb{Q}(\gamma) = \mathbb{Q}(\beta) \subseteq K$, where the minimum polynomial of γ is given as $\mu_\gamma = (X-\gamma)(X+\gamma) = X^2 - \gamma^2 \in \mathbb{Z}[X]$.

From $\gamma^2 = \big(\sum_{k=1}^{p-1} \left(\frac{k^{-1}}{p}\right) \zeta^k\big) \cdot \big(\sum_{l=1}^{p-1} \left(\frac{-l}{p}\right) \zeta^{-l}\big) = \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{k^{-1}(-l)}{p}\right) \zeta^{k-l}$, letting $j := k^{-1}l \in (\mathbb{Z}/(p))^*$, we get $\left(\frac{-1}{p}\right) \gamma^2 = \sum_{j=1}^{p-1} \big(\left(\frac{j}{p}\right) \cdot \sum_{k=1}^{p-1} \zeta^{k(1-j)}\big) = (p-1) + \sum_{j=2}^{p-1} \big(\left(\frac{j}{p}\right) \cdot \sum_{k=1}^{p-1} \zeta^k\big) = (p-1) + T(\zeta) \cdot \sum_{j=2}^{p-1} \left(\frac{j}{p}\right)$. We have $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = |\mathcal{Q}_p| - |\mathcal{N}_p| = 0$, and $\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$ yields $T(\zeta) = -1$, thus $\frac{p-1}{2} \cdot \gamma^2 = \left(\frac{-1}{p}\right) \gamma^2 = (p-1) - (-1) = p$ (showing again that $\gamma \neq 0$). ♯

Hence we have $\{\pm\gamma\} = \{\pm\sqrt{p^*}\}$, where these cases cannot be told apart algebraically, but analytical tools are required to decide which case actually holds. Moreover, this also reveals β and β': From $\beta+\beta' = T(\zeta) = -1$ and $\beta-\beta' = \gamma = \pm\sqrt{p^*}$ we get $\beta = \frac{1}{2}(-1+\gamma) = \frac{1}{2}(-1\pm\sqrt{p^*})$ and $\beta' = \frac{1}{2}(-1-\gamma) = \frac{1}{2}(-1\mp\sqrt{p^*})$.

(12.8) Quadratic Reciprocity Law [Gauss, 1796]**.** Let $p \in \mathcal{P}_\mathbb{Z}$ be odd.

Corollary. Let $l \in \mathcal{P}_\mathbb{Z}$ be odd such that $l \neq p$. Then $\left(\frac{l}{p}\right) \cdot \left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}$.

Proof. We have $\left(\frac{l}{p}\right) = 1$, that is $l \in \mathcal{Q}_p \leq (\mathbb{Z}/(p))^*$, if and only if l splits in $\mathbb{Q}(\sqrt{p^*})$. The latter is the case if and only if $p^* \in \mathcal{Q}_l \leq (\mathbb{Z}/(l))^*$, that is $\left(\frac{p^*}{l}\right) = 1$. This yields $\left(\frac{l}{p}\right) = \left(\frac{p^*}{l}\right) = \left(\frac{-1}{l}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{l}\right)$. ♯

Corollary: Second supplement to the Quadratic Reciprocity Law.
i) The prime p is split in $\mathbb{Q}(\sqrt{2})$, if and only if the prime 2 is split in $\mathbb{Q}(\sqrt{p^*})$.
ii) We have $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, that is $2 \in \mathcal{Q}_p$ if and only if $p \equiv \pm 1 \pmod 8$.

Proof. i) The prime p is split in $\mathbb{Q}(\sqrt{2})$, if and only if $2 \in \mathcal{Q}_p \leq (\mathbb{Z}/(p))^*$, that is $\left(\frac{2}{p}\right) = 1$, which holds if and only if 2 splits in $\mathbb{Q}(\sqrt{p^*})$.

ii) The prime 2 splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if $p^* \equiv 1 \pmod 8$.

Hence, if $p \equiv 1 \pmod 4$, that is $p^* = p$, this is equivalent to $p \equiv 1 \pmod 8$; this says that $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{p+1}{2}\cdot\frac{p-1}{4}} = (-1)^{\frac{p^2-1}{8}}$.

Similarly, if $p \equiv -1 \pmod 4$, that is $p^* = -p$, this is equivalent to $p \equiv -1 \pmod 8$; this says that $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{p-1}{2}\cdot\frac{p+1}{4}} = (-1)^{\frac{p^2-1}{8}}$.

In any case $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, and $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$. ♯

(12.9) Example: The 23-rd cyclotomic field. We present an example of a cyclotomic field whose ring of integers is not factorial (actually the 'smallest' one, see (13.1)): Let $\zeta := \zeta_{23} \in \mathbb{C}$, let $K := \mathbb{Q}(\zeta)$, and let $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[\zeta]$.

We have $\mathrm{Aut}_\mathbb{Q}(K) \cong G := (\mathbb{Z}/(23))^* = \langle 5\rangle \cong C_{22} \cong C_2 \times C_{11}$. Hence $\mathcal{Q}_{23} = \langle 5^2\rangle = \langle 2\rangle$ is the unique subgroup of index 2, while $\langle -1\rangle$ is the unique subgroup of order 2, so that $G = \{-1\} \times \mathcal{Q}_{23}$. Thus K has a unique subfield $K^{(11)} := \mathrm{Fix}_K(\langle -1\rangle) = K \cap \mathbb{R}$ of index 2, being called its **real** subfield, and a unique quadratic subfield $D := K^{(2)} = \mathrm{Fix}_K(\mathcal{Q}_{23}) = \mathbb{Q}(\sqrt{-23})$.

We have (although this does not matter algebraically) $\gamma = \sqrt{-23} = i\cdot\sqrt{23}$, hence $\beta = T_{K/D}(\zeta) = \sum_{i\in\mathcal{Q}_{23}} \zeta^i = \frac{1}{2}(-1+\sqrt{-23})$ and $\overline{\beta} = \frac{1}{2}(-1-\sqrt{-23})$. Moreover,

we have $\mathcal{O}_D = \mathbb{Z}[\beta]$, and for $a, b \in \mathbb{Z}$ we get $N_D(a+b\beta) = (a+b\beta)(a+b\overline{\beta}) = a^2 + ab(\beta+\overline{\beta}) + b^2\beta\overline{\beta} = a^2 - ab + 6b^2 = (a-\frac{b}{2})^2 + 23\cdot(\frac{b}{2})^2$.

Having this in place, we now proceed to show (in two ways) that $\mathcal{O}$ is not a principal ideal domain, and thus is not factorial:

i) We determine the ramification of 2 in K: Letting $\mathfrak{p} \in \mathcal{P}_K(2)$, we have $e(\mathfrak{p}) = \varphi(1) = 1$ and $I_\mathfrak{p} = K$. Hence we have $D_\mathfrak{p} = \mathrm{Fix}_K(\widehat{\varphi}_2)$. Now $2 \in (\mathbb{Z}/(23))^*$ has order $f(\mathfrak{p}) = 11$, so that $[K\colon D_\mathfrak{p}] = 11$ implies $D_\mathfrak{p} = D$. Thus we get $|\mathcal{P}_K(2)| = 2$ and $\mathrm{Stab}_G(\mathfrak{p}) = \mathcal{Q}_{23}$. Since we have $-1 \notin \mathcal{Q}_{23}$, this entails $\mathcal{P}_K(2) = \{\mathfrak{p}, \overline{\mathfrak{p}}\}$.

In order to determine $\mathfrak{p}$, we observe that the cyclotomic polynomial $\Phi_{23} = \frac{X^{23}-1}{X-1} = \sum_{i=0}^{22} X^i \in \mathbb{Z}[X]$ splits as follows (as is seen computationally), again confirming $e(\mathfrak{p}) = 1$ and $f(\mathfrak{p}) = 11$:

$$(X^{11}+X^9+X^7+X^6+X^5+X+1)\cdot(X^{11}+X^{10}+X^6+X^5+X^4+X^2+1) \in \mathbb{F}_2[X].$$

Hence letting $\omega := 1+\zeta+\zeta^5+\zeta^6+\zeta^7+\zeta^9+\zeta^{11}$ and $\omega' := 1+\zeta^2+\zeta^4+\zeta^5+\zeta^6+\zeta^{10}+\zeta^{11}$, we may let $\mathfrak{p} := (2,\omega) \lhd \mathcal{O}$ and $\overline{\mathfrak{p}} := (2,\omega') \lhd \mathcal{O}$. (Actually, this shows that $2 \mid \omega\omega'$, while $2 \nmid \omega$ and $2 \nmid \omega'$.)

We derive a description of $\mathfrak{p}$ related to the subring $\mathcal{O}_D \subseteq \mathcal{O}$: We observe that 2 splits in D as $2\mathcal{O}_D = \mathfrak{q}\overline{\mathfrak{q}} \lhd \mathcal{O}_D$, where $\mathfrak{q} := (2,\beta) \lhd \mathcal{O}_D$ and $\overline{\mathfrak{q}} := (2,\overline{\beta}) \lhd \mathcal{O}_D$. Then, since $\mathfrak{q} \lhd \mathcal{O}_D$ is inert in K, we have $\{\mathfrak{p}, \overline{\mathfrak{p}}\} = \{\mathfrak{q}\mathcal{O}, \overline{\mathfrak{q}}\mathcal{O}\}$.

We show that $\mathfrak{q}\mathcal{O} = \mathfrak{p}$, by showing that $\beta \in \mathfrak{p}$: Going over to $\mathbb{F}_2[X]$ we have $\sum_{i\in\mathcal{Q}_{23}} X^i = (X^7+X^3+X)(X^{11}+X^9+X^7+X^6+X^5+X+1) \in \mathbb{F}_2[X]$, saying that $\beta - (\zeta^7+\zeta^3+\zeta)\cdot\omega \in 2\mathcal{O}$, thus $\beta \in \mathfrak{p}$.

By (10.4) we have $\mathrm{Cl}_D = \langle\mathfrak{q}\rangle \cong C_3$, where $\mathfrak{q}^3 = (\beta+2) \lhd \mathcal{O}_D$. Hence $\mathfrak{p}^3 = \mathfrak{q}^3\mathcal{O} = (\beta+2) \lhd \mathcal{O}$ is principal, so that $\mathfrak{p} \in \mathrm{Cl}_K$ has order dividing 3. We show that $\mathfrak{p} \lhd \mathcal{O}$ is not principal, entailing that $\mathfrak{p} \in \mathrm{Cl}_K$ has order 3: (Actually, we have $\mathrm{Cl}_K = \langle\mathfrak{p}\rangle$, see (13.1); moreover, this shows that $(2) \lhd \mathcal{O}$ is a maximal principal ideal, that is 2 is irreducible, and hence 2 is not a prime.)

Assume to the contrary that $\mathfrak{p} = (\pi) \lhd \mathcal{O}$, for some $\pi \in \mathcal{O}$. Then we have $\mathfrak{p}^{11} = \prod_{\sigma\in\mathcal{Q}_{23}} \mathfrak{p}^\sigma = \prod_{\sigma\in\mathcal{Q}_{23}} (\pi^\sigma) = (N_{K/D}(\pi)) \lhd \mathcal{O}$. Since $N_{K/D}(\pi) \in \mathcal{O}_D$, this entails $\mathfrak{q}^{11} = \mathfrak{p}^{11} \cap \mathcal{O}_D = N_{K/D}(\pi)\mathcal{O} \cap \mathcal{O}_D = N_{K/D}(\pi)\mathcal{O}_D \lhd \mathcal{O}_D$. Thus $\mathfrak{q} \in \mathrm{Cl}_D$ has order dividing 11, a contradiction. ♯

ii) Alternatively, let $\omega := 1-\zeta-\zeta^3 \in K$ (which we find by a random search, but this kind of example was already known to Kummer). Then we find that $N(\omega) = 6533 = 47\cdot139$. Hence $(\omega) \lhd \mathcal{O}$ is not prime, and thus has a factorization $(\omega) = \mathfrak{r}\mathfrak{s}$, where $\mathfrak{r}, \mathfrak{s} \lhd \mathcal{O}$ are prime such that $N(\mathfrak{r}) = 47$ and $N(\mathfrak{s}) = 139$. We show that $\mathfrak{r}$ is not principal:

Assume to the contrary that $\mathfrak{r} = (\rho) \lhd \mathcal{O}$, for some $\rho \in \mathcal{O}$ such that $N(\rho) = \pm 47$. Then we have $N(\rho) = N_D(N_{K/D}(\rho))$, and letting $N_{K/D}(\rho) = a+b\beta \in \mathcal{O}_D$, where $a, b \in \mathbb{Z}$, we get $\pm 47 = N(\rho) = N_D(a+b\beta) = (a-\frac{b}{2})^2 + 23\cdot(\frac{b}{2})^2$. Hence we conclude that $(2a-b)^2 + 23b^2 = 4\cdot47 = 188$, which by checking the cases $b \in$

$\{0,1,2\}$ yields a contradiction. (Similarly, $N(\rho) = 139$ yields a contradiction, while $N(\omega) = N_D(N_{K/D}(\omega)) = N_D(59 + 28\beta) = 45^2 + 14^2 \cdot 23 = 6533$.) ♯

13 Cyclotomic fields: geometry

(13.1) Class numbers. For $m \in \mathbb{N}$ let $K := \mathbb{Q}(\zeta_m)$, and let $\mathcal{O}_m := \mathbb{Z}[\zeta_m]$ be its ring of integers. From $\mathrm{Aut}_{\mathbb{Q}}(K) \cong (\mathbb{Z}/m\mathbb{Z})^*$, where the automorphism associated with $k \in (\mathbb{Z}/m\mathbb{Z})^*$ is given by $\zeta_m \mapsto \zeta_m^k$, we infer that K does not have any real embeddings, thus $r = 0$ and $s := \frac{\varphi(m)}{2}$. For $m \equiv 2 \pmod 4$ we have $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\frac{m}{2}})$, so that we may exclude these cases.

a) We consider the class number problem, that is the question which of the rings $\mathcal{O}_m$ has trivial class group: For $m = 1$ we have $\mathbb{Q}(\zeta_1) = \mathbb{Q}$; and $\mathbb{Q}(\zeta_m)$ is a quadratic number field if and only if $m \in \{3, 4\}$, namely $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, both cases having trivial class group. In general, a simple computational approach is as follows:

Letting $q \in \mathcal{P}_{\mathbb{Z}}$, for any $\mathfrak{q} \in \mathcal{P}_K(q)$ the inertia degree $f_q := f(\mathfrak{q}) \in \mathbb{N}$ equals the order of $q \in (\mathbb{Z}/(m_{q'}))^*$, where $m_{q'}$ denotes the q-prime part of m; hence f_q is found easily (computationally). Now it suffices to consider the primes q such that $N(\mathfrak{q}) = q^{f_q}$ does not exceed the Minkowski bound. In this case, recalling that $\mathbb{Q} \subseteq K$ is Galois, we infer that $\mathfrak{q}$ is principal as soon as we find an element $\omega_q \in \mathcal{O}$ such that $|N_K(\omega_q)| = q^{f_q} \cdot r$, where r is coprime to q and has only prime divisors (if any) already treated successfully before. To this end, we just run a random search through elements of $\mathcal{O}_m$ being sparse with respect to the $\mathbb{Z}$-generating set $\{1, \zeta_m, \ldots, \zeta_m^{m-1}\}$ and having non-zero coefficients $\{\pm 1\}$ only.

This works out for the cases m given in Table 12, where we also give the field degree $n = \varphi(m)$, the associated Minkowski bound m_K, and the prime powers q^f to be considered, or their number. For example, for the (smallest non-trivial) case $m = 11$ we find that $\omega_{23} := 1 + \zeta_{11} + \zeta_{11}^3 \in \mathcal{O}_{11}$ has absolute norm $|N_K(\omega_{23})| = 23$. This verifies the 'if' part of the following:

Theorem. The ring $\mathcal{O}_m$ has trivial class group if and only if

$$\begin{aligned} m \in\ & \{1,3,4,5,7,8,9,11,12,15\} \quad \dot\cup \\ & \{13,16,17,19,20,21,24,25,27,28,32,33,35,36,40,44,45,48,60,84\}, \end{aligned}$$

where the first bunch are the values for which $\mathcal{O}_m$ is Euclidean with respect to the absolute norm map. ♯

b) We consider the particularly interesting case $m = p \in \mathcal{P}_Z$: A few examples are given in Table 13, where h_p is the class number of $\mathcal{O}_p$, accompanied by its factorization. Those marked with an asterisk are the **irregular** primes, that is the primes p dividing the class number h_p; see (13.3). To determine these (and more) class numbers, fairly sophisticated techniques are needed (which we are not able to explain here in any detail), amongst other things employing the **analytical class number formula**.

Table 12: Cyclotomic fields with trivial class group.

m	n	$m_K \sim$	q^f
1	1	1	
3	2	1.2	
4	2	1.3	
5	4	1.7	
7	6	4.2	
8	4	2.5	2
9	6	4.5	3
11	10	59.0	$11, 23$
12	4	1.9	
13	12	306.5	$3^3, 13, 53, 79, 131, 157$
15	8	7.2	
16	8	25.9	$2, 17$
17	16	13254.1	$(\# = 104)$
19	18	105933.3	$(\# = 559)$
20	8	12.7	5
21	12	103.9	$2^6, 7, 43$
24	8	14.6	$2^2, 3^2$
25	20	443201.3	$(\# = 1865)$
27	18	77777.8	$(\# = 431)$
28	12	246.3	$2^3, 7^2, 13^2, 29, 113, 197$
32	16	33646.6	$(\# = 238)$
33	20	148856.0	$(\# = 698)$
35	24	4658732.1	$(\# = 13646)$
36	12	288.4	$2^6, 3^2, 37, 73, 109, 181$
40	16	8022.0	$(\# = 70)$
44	20	627278.0	$(\# = 2576)$
45	24	6389544.8	$(\# = 18273)$
48	16	10646.0	$(\# = 88)$
60	8	2538.2	$(\# = 29)$
84	24	7122380.5	$(\# = 20191)$

Still, we are able to treat the case $p := 23$: We have already seen in (12.9) that $3 \mid h_K$, where more precisely we have $(2) = \mathfrak{p}_2\overline{\mathfrak{p}}_2 \lhd \mathcal{O}_p$ and $\mathfrak{p}_2 \in \mathrm{Cl}_K$ has order 3. We proceed to show that $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle$, thus $h_K = 3$:

We have $|\mathrm{disc}(K)| = 23^{21} \sim 4 \cdot 10^{28}$, the relevant Minkowski constant is $M_{0,11} \sim 4.7 \cdot 10^{-8}$, which entails that any ideal class contains an ideal of norm at most $m_K = M_{0,11} \cdot \sqrt{23^{21}} \sim 9324406.5 < 9324407$. Thus we only have to consider the primes q such that $q^{f_q} < 9324407$, which leaves 28284 primes. We again proceed by using the technique described above, but now we consider the prime $q = 2$ as successfully treated right from the beginning; this ultimately shows that all prime ideals to be considered are indeed powers of $\mathfrak{p}_2$ in Cl_K. ♯

Table 13: Class numbers of cyclotomic fields.

	p	h_p	
	3	1	1
	5	1	1
	7	1	1
	11	1	1
	13	1	1
	17	1	1
	19	1	1
	23	3	3
	29	8	2^3
	31	9	3^2
$*$	37	37	37
	41	121	11^2
	43	211	211
	47	695	$5 \cdot 139$
	53	4889	4889
$*$	59	41241	$3 \cdot 59 \cdot 233$
	61	76301	$41 \cdot 1861$
$*$	67	853513	$67 \cdot 12739$
	71	3882809	$7^2 \cdot 79241$
	73	11957417	$89 \cdot 134353$
	79	100146415	$5 \cdot 53 \cdot 377911$
	83	838216959	$3 \cdot 279405653$
	89	13379363737	$113 \cdot 118401449$
	97	411322824001	$577 \cdot 3457 \cdot 206209$
$*$	101	3547404378125	$5^5 \cdot 101 \cdot 601 \cdot 18701$
$*$	103	9069094643165	$5 \cdot 103 \cdot 1021 \cdot 17247691$
	107	63434933542623	$3 \cdot 743 \cdot 9859 \cdot 2886593$

(13.2) Units. a) Let $m \in \mathbb{N}$ such that $m \not\equiv 2 \pmod 4$, let $K := \mathbb{Q}(\zeta_m)$, and let $\mathcal{O} := \mathcal{O}_m = \mathbb{Z}[\zeta_m]$ be its ring of integers.

Proposition. We have $T(\mathcal{O}^*) = \{\pm\zeta_m^i \in \mathcal{O}^*; i \in \mathbb{Z}\}$.

Proof. Note that $-\zeta_m$ is a primitive $(2m)$-th root of unity for m odd, while it is a primitive m-th root of unity for m even. Hence letting $T(\mathcal{O}^*) = \langle\zeta_k\rangle$, where $k \in \mathbb{N}$, we have $2m \mid k$ and $m \mid k$, respectively.

Moreover, we have $K = \mathbb{Q}(\zeta_k)$, entailing $\phi(m) = \phi(k)$. By the number-theoretic multiplicativity of Euler's totient function, since k is a multiple of m, the latter entails that either m is odd and $k = 2m$, or m is even and $k = m$. ♯

b) Since K does not have any real embeddings, but $\frac{\varphi(m)}{2}$ non-real ones, we have $\mathrm{rk}_{\mathbb{Z}}(\mathcal{O}^*/T(\mathcal{O}^*)) = \frac{\varphi(m)}{2} - 1$. Apart from that, not too much more can be said (here) about the general structure of $\mathcal{O}^*/T(\mathcal{O}^*)$ (which is the topic of **Iwasawa theory**). Alone, for the case of $m = p$ being prime we have the following:

Proposition: Kummer's Lemma. Let $p \in \mathcal{P}_{\mathbb{Z}}$ be odd. Then for any unit $\epsilon \in \mathcal{O}_p^*$ there are $r \in \mathcal{O}_p^* \cap \mathbb{R}$ and $k \in \mathbb{Z}$ such that $\epsilon = r\zeta_p^k \in \mathcal{O}_p^*$.

Proof. Let $\zeta := \zeta_p$, let $\mathcal{O} := \mathcal{O}_p$, let $G := \mathrm{Aut}_{\mathbb{Q}}(K) \cong (\mathbb{Z}/(p))^*$, and for $i \in (\mathbb{Z}/(p))^*$ let $\epsilon_i := \epsilon^{\sigma_i} \in \mathcal{O}^*$. Letting $^- \in G$ denote complex conjugation, the set $\{\epsilon_i\overline{\epsilon}_i^{-1} \in \mathcal{O}^*; i \in (\mathbb{Z}/(p))^*\}$ is G-stable, and consists of algebraic integers of complex absolute value 1. Thus we have $\epsilon\overline{\epsilon}^{-1} = \pm\zeta^l \in T(\mathcal{O}^*)$, for some $l \in \mathbb{Z}$. Since $2 \in (\mathbb{Z}/(p))^*$, applying σ_2 if necessary, we may assume that $l = 2k \in \mathbb{Z}$ is even, entailing $\omega := \zeta^{-k}\epsilon = \pm\zeta^k\overline{\epsilon} = \pm\overline{\zeta^{-k}\epsilon} = \pm\overline{\omega} \in \mathcal{O}^*$; that is either $\omega \in \mathbb{R}$, in which case we are done, or $\omega \in i\mathbb{R}$.

Hence assume that $\omega = -\overline{\omega}$. Then, letting $\mathfrak{p} := (1-\zeta) \lhd \mathcal{O}$ we have $(p) = \mathfrak{p}^{p-1} \lhd \mathcal{O}$, thus p is completely ramified in K. Hence we have $G_{\mathfrak{p}}^0 = G_{\mathfrak{p}} = G$, saying that $\mathfrak{p}$ is G-stable, and that G induces only the identity map on $\mathcal{O}/\mathfrak{p}$. Hence we have $\omega - \overline{\omega} = 2\omega \in \mathfrak{p}$, thus $2 \in \mathfrak{p}$, a contradiction. ♯

(13.3) Remark: Fermat's Last Theorem. We consider the **Fermat equation** $X^n + Y^n = Z^n$ for $1 \neq n \in \mathbb{N}$, whose **non-trivial** integral solutions $[x, y, z] \in (\mathbb{Z}\backslash\{0\})^3$ are looked for. It is immediate that we may restrict ourselves to **primitive** non-trivial solutions, that is such that additionally $\gcd(x, y, z) = 1$, or equivalently $\{x, y, z\}$ are pairwise coprime.

For $n = 2$, the (well-known) non-trivial integral solutions of the equation $X^2 + Y^2 = Z^2$ are called **Pythagorean triples**, the primitive ones being described in Exercise (15.11). From this, it follows (easily) that, for $n = 4$, there are no non-trivial integral solutions of the equation $X^4 + Y^4 = Z^4$; see Exercise (15.12).

In view of this, the question of solvability of the Fermat equation for general n is straightforwardly reduced to the case of n being an odd prime. For these cases we have the following, which has been conjectured by Fermat [1637]:

Theorem: Fermat's Conjecture [Wiles, Taylor–Wiles, 1995]**.**
For $p \in \mathcal{P}_{\mathbb{Z}}$ odd, the Fermat equation $X^p + Y^p = Z^p$ does not have any non-trivial integral solutions. ♯

The modern (successful) approach by Wiles goes back to the observation due to Frey [1986] and Ribet [1987] (independently), that the truth of Fermat's Conjecture follows from the (semi-stable case of) the **Shimura-Taniyama-Weil Conjecture** (on the modularity of L-series) for **elliptic curves**.

The classical (only partially successful) approach towards Fermat's Conjecture runs as follows: Let $p \in \mathcal{P}_{\mathbb{Z}}$ be odd, and let $[x, y, z]$ be a primitive non-trivial solution of the equation $X^p + Y^p + Z^p = 0$, where the latter is equivalent to the Fermat equation, but more symmetric. Then $[x, y, z]$ is said to be in **case I** if $p \nmid xyz$, while otherwise it is said to be in **case II**; note that in case II precisely one of $\{x, y, z\}$ is divisible by p.

Now the standard error made in 19-th century attempts to prove Fermat's Conjecture, most notably made by LAMÉ [1840], was to assume that the p-th cyclotomic field would be factorial, that is in modern wording would have class number $h_p = 1$. But KUMMER [1850], being aware of this, was able to show the truth of Fermat's Conjecture whenever p is a **regular** prime, that is p does not divide h_p. Otherwise p is called **irregular**; in Table 13 the irregular primes are marked by an asterisk.

Unfortunately, there are infinitely many irregular primes (which we are not able to show here), while it is not known whether there are infinitely many regular ones. Actually, KUMMER's proof for regular primes, generalizing from the case $h_p = 1$, in case I runs as follows:

(13.4) Theorem. Let $2 \neq p \in \mathcal{P}_{\mathbb{Z}}$ be a regular prime. Then the equation $X^p + Y^p + Z^p = 0$ does not have any integral solution $[x, y, z]$ such that $p \nmid xyz$.

Proof. i) Let $\zeta := \zeta_p \in \mathbb{C}$, let $K := \mathbb{Q}(\zeta)$, and let $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[\zeta]$, hence $\{\zeta, \ldots, \zeta^{p-1}\} \subseteq \mathcal{O}$ is an integral basis, and let $G := \mathrm{Aut}_{\mathbb{Q}}(K) \cong (\mathbb{Z}/(p))^*$.

We have $(p) = \mathfrak{p}^{p-1} \lhd \mathcal{O}$, where $\mathfrak{p} := (1 - \zeta) \lhd \mathcal{O}$, and where $G^0_{\mathfrak{p}} = G_{\mathfrak{p}} = G$, saying that $\mathfrak{p}$ is G-stable, and that G induces only the identity map on $\mathcal{O}/\mathfrak{p}$. Hence we have $\mathfrak{p} := (1 - \zeta^i) \lhd \mathcal{O}$, for all $i \in (\mathbb{Z}/(p))^*$. Moreover, letting $^- \in G$ denote complex conjugation, for any $\omega \in \mathcal{O}$ we have $\omega - \overline{\omega} \in \mathfrak{p}$, implying $(\omega - \overline{\omega})^p \in \mathfrak{p}^p \subseteq \mathfrak{p}^{p-1} = (p) \lhd \mathcal{O}$, entailing $\omega^p - \overline{\omega}^p \in p\mathcal{O}$, that is $\omega^p = \overline{\omega^p} \in \mathcal{O}/(p)$.

The basic observation relating Fermat's equation to cyclotomic fields is the following identity: We have $X^p - Y^p = Y^p \cdot ((\frac{X}{Y})^p - 1) = Y^p \cdot \prod_{i \in \mathbb{Z}/(p)} (\frac{X}{Y} - \zeta^i) = \prod_{i \in \mathbb{Z}/(p)} (X - \zeta^i Y) \in K(X, Y)$.

ii) Now assume there are pairwise coprime $x, y, z \in \mathbb{Z}$ such that $x^p + y^p + z^p = 0$ where $p \nmid xyz$. Then we have $\prod_{i \in \mathbb{Z}/(p)} (x + \zeta^i y) = x^p - (-y)^p = x^p + y^p = -z^p$.

Letting $\mathfrak{a}_i := (x + \zeta^i y) \trianglelefteq \mathcal{O}$, for $i \in \mathbb{Z}/(p)$, we have $\prod_{i \in \mathbb{Z}/(p)} \mathfrak{a}_i = (z)^p \trianglelefteq \mathcal{O}$; note that for any prime divisor $\mathfrak{q} \lhd \mathcal{O}$ of $\mathfrak{a}_i$ we have $z^p \in \prod_{i \in \mathbb{Z}/(p)} \mathfrak{a}_i \subseteq \mathfrak{q}$, thus $z \in \mathfrak{q}$.

We show that the $\mathfrak{a}_i$ are pairwise coprime ideals: Assume there is a prime ideal such that $\mathfrak{a}_i + \mathfrak{a}_j \subseteq \mathfrak{q} \lhd \mathcal{O}$ for some $i \neq j$. Then we have $(x + \zeta^i y) - (x + \zeta^j y) = \zeta^i (1 - \zeta^{j-i}) y \in \mathfrak{q}$, since $\zeta \in \mathcal{O}^*$ and $1 - \zeta^{j-i} \sim 1 - \zeta \in \mathcal{O}$ entailing that $(1 - \zeta) y \in \mathfrak{q}$. Since $\mathfrak{q}$ is prime, we have $y \in \mathfrak{q}$ or $1 - \zeta \in \mathfrak{q}$. If $y \in \mathfrak{q}$ then, since $z \in \mathfrak{q}$ and $y, z \in \mathbb{Z}$ are coprime, we conclude that $1 \in \mathfrak{q}$, a contradiction. If $1 - \zeta \in \mathfrak{q}$, then we have $\mathfrak{q} = (1 - \zeta) = \mathfrak{p}$, so that $z \in \mathfrak{q} \cap \mathbb{Z} = (p) \lhd \mathbb{Z}$, entailing $p \mid z$, a contradiction as well.

iii) Hence, by uniqueness of prime ideal factorization, we conclude that any of the ideals $\mathfrak{a}_i$ is a p-th power. In particular, there is $\mathfrak{a} \trianglelefteq \mathcal{O}$ such that $\mathfrak{a}_1 = (x + \zeta y) = \mathfrak{a}^p$. Thus $\mathfrak{a}^p$ is principal, that is $\mathfrak{a}^p = 1 \in \mathrm{Cl}_K$, from which since $p \nmid h_K$ we conclude that $\mathfrak{a} = 1 \in \mathrm{Cl}_K$, that is $\mathfrak{a}$ is principal. Hence letting $\mathfrak{a} = (\alpha) \trianglelefteq \mathcal{O}$, there is $\epsilon \in \mathcal{O}^*$ such that $x + \zeta y = \epsilon\alpha^p$. Using Kummer's Lemma there are $r \in \mathcal{O}^* \cap \mathbb{R}$ and $k \in \mathbb{Z}/(p)$ such that $\epsilon = r\zeta^k$. Hence we have $\zeta^{-k}(x+\zeta y) = r\alpha^p$, so that taking complex conjugates we get $\zeta^{-k}(x+\zeta y) = \zeta^k(x+\zeta^{-1}y) \in \mathcal{O}/(p)$.

iv) Assume that $k = 0 \in \mathbb{Z}/(p)$; then we have $x + \zeta y = x + \zeta^{-1}y \in \mathcal{O}/(p)$, thus $(\zeta - \zeta^{-1})y = \zeta^{-1}(\zeta^2 - 1)y \in p\mathcal{O}$. Hence, since $\zeta^2 - 1 \sim \zeta - 1 \in \mathcal{O}$, we have $(1 - \zeta)y \in (p) = \mathfrak{p}^{p-1}$, thus $y \in \mathfrak{p}^{p-2} \cap \mathbb{Z} = p\mathbb{Z}$, a contradiction. Similarly, assume that $k = 1 \in \mathbb{Z}/(p)$; then we have $\zeta^{-1}(x + \zeta y) = \zeta(x + \zeta^{-1}y) \in \mathcal{O}/(p)$, thus $(\zeta - \zeta^{-1})x \in p\mathcal{O}$, which now implies $x \in p\mathbb{Z}$, a contradiction. Thus we have $p \nmid k$ and $p \nmid (k - 1)$.

We have $\zeta^{-k}x + \zeta^{1-k}y - \zeta^k x - \zeta^{k-1}y \in p\mathcal{O}$. Assume that $\{\pm k, \pm(k-1)\} \subseteq (\mathbb{Z}/(p))^*$ are pairwise distinct; then since $\{\zeta^k, \zeta^{k-1}, \zeta^{-k}, \zeta^{1-k}, \}$ belong to an integral basis of $\mathcal{O}$ we infer that $p \mid x$ and $p \mid y$, a contradiction. Hence at least two of the latter elements coincide, thus we have $k = -k+1 \in \mathbb{Z}/(p)$, that is $2k = 1 \in \mathbb{Z}/(p)$. This yields $\zeta^{-k}(1 - \zeta)(x - y) \in p\mathcal{O}$, hence $(1 - \zeta)(x - y) \in (p) = \mathfrak{p}^{p-1}$, thus $x - y \in \mathfrak{p}^{p-2} \cap \mathbb{Z} = p\mathbb{Z}$, that is $x \equiv y \pmod{p}$.

v) By symmetry we infer that $y \equiv z \pmod{p}$ as well. This entails $x^p + y^p + z^p \equiv 3x^p \pmod{p}$. Since $p \nmid x$ we infer that $p = 3$. In the latter case, since $(\mathbb{Z}/(9))^*$ has order 6, the subgroup of cubes is $\{\pm 1\} \subseteq (\mathbb{Z}/(9))^*$, so that $x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{9}$, which is a final contradiction. ♯

Corollary. For the regular prime $p = 3$ any primitive non-trivial solution of the equation $X^3 + Y^3 + Z^3 = 0$ belongs to case II.

Actually, it is not too difficult (but still we do not present a proof here) to show the truth of Fermat's conjecture for $p = 3$, of course by making use of the (quadratic) cyclotomic field $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$.

V Exercises and references

14 Exercises: Theory

(14.1) Exercise: Wilson's Theorem [1770].
a) Show that $n \in \mathbb{Z}$, $n \geq 2$, is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.
b) For $p \in \mathcal{P}_{\mathbb{Z}}$ odd show that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

(14.2) Exercise: Primes in arithmetic progressions.
We consider an (easy) special case of **Dirichlet's Theorem [1837]** on primes in coprime residue classes:
a) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv -1 \pmod{4}$.
b) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod{4}$.

(14.3) Exercise: Discriminants.
Let $K \subseteq L$ be a separable finite extension of degree $n := [L\colon K]$, and let $\mathcal{S} := [z_1, \ldots, z_n]$ be an n-tuple of elements of L. Show that $\operatorname{disc}(\mathcal{S}) \neq 0$ if and only if $\mathcal{S}$ is K-linearly independent.

(14.4) Exercise: Discriminants.
Let R be integrally closed such that $K = \mathrm{Q}(R)$, let $K \subseteq L$ be a separable finite extension, and let $z \in L$ be integral over R such that $L = K(z)$.
a) For $f \in R[X]$ monic such that $f(z) = 0$, show that $\operatorname{disc}(z) \mid N_{L/K}((\partial f)(z))$.
b) Let $\mu_z \in R[X]$ be the minimum polynomial of z, and let $a \in R$ be a root of $\partial\mu_z$. Show that $\mu_z(a) \mid \operatorname{disc}(z) \in R$.

(14.5) Exercise: Resultants.
Let R be an integral domain, and $f = \sum_{i=0}^{n} f_i X^i \in R[X]$ and $g = \sum_{j=0}^{m} g_j X^j \in R[X]$, where $f_n, g_m \neq 0$. Then the associated **Sylvester matrix** is defined as

$$S(f,g) := \left[\begin{array}{ccccccc} f_n & f_{n-1} & \cdots & f_0 & & & \\ & f_n & \cdots & f_1 & f_0 & & \\ & & \ddots & & \ddots & \ddots & \\ & & & f_n & \cdots & \cdots & f_0 \\ \hline g_m & g_{m-1} & \cdots & g_0 & & & \\ & g_m & \cdots & g_1 & g_0 & & \\ & & \ddots & & \ddots & \ddots & \\ & & & g_m & \cdots & \cdots & g_0 \end{array}\right] \in R^{(n+m)\times(n+m)}.$$

where the upper and lower halves consist of m and n rows, respectively, and let $\operatorname{res}(f,g) := \det(S(f,g)) \in R$ be the **resultant** of f and g.

a) Let $K := \mathrm{Q}(R)$, let $\overline{K}$ be an algebraic closure of K, and let $f = f_n \cdot \prod_{i=1}^{n}(X-\alpha_i) \in \overline{K}[X]$ and $g = g_m \cdot \prod_{j=1}^{m}(X-\beta_j) \in \overline{K}[X]$. Show that $\operatorname{res}(f,g) = f_n^m \cdot \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} g_m^n \cdot \prod_{j=1}^{m} f(\beta_j) = f_n^m g_m^n \cdot \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$.

b) Let R be factorial. Show that $\gcd(f,g) \in R[X]$ is non-constant if and only if $\operatorname{res}(f,g) \neq 0 \in R$.

c) Let $f = X^n + \sum_{i=0}^{n-1} f_i X^i \in K[X]$ be irreducible and separable. Show that we have $\operatorname{disc}(f) = (-1)^{\binom{n}{2}} \cdot \operatorname{res}(f, \partial f) \in K$.

(14.6) Exercise: Integral bases.
Let R be a principal ideal domain, let $K := \mathrm{Q}(R)$ be its field of fractions, let $K \subseteq L$ be a separable finite extension of degree $n := [L\colon K]$, let S be the integral closure of R in L, and let $\alpha \in S$ be a primitive element of L over K.

a) Show that there are $f_0, \ldots, f_{n-1} \in R[X]$ monic of degree $\deg(f_i) = i$, and unique (up to associates) $d_0, \ldots, d_{n-1} \in R$, where $1 = d_0 \mid d_1 \mid d_2 \mid \cdots \mid d_{n-1}$, such that $\{\frac{f_i(\alpha)}{d_i}; i \in \{0, \ldots, n-1\}\}$ is an integral basis of L over K.

b) Show that $S/R[\alpha] \cong \bigoplus_{i=0}^{n-1} R/(d_i)$ as R-modules; conclude that $\operatorname{disc}(\alpha) = (\prod_{i=0}^{n-1} d_i)^2 \cdot \operatorname{disc}(S)$. (Recall that discriminants are only defined modulo $(R^*)^2$.)

c) For $i, j \in \{0, \ldots, n-1\}$ such that $i + j \leq n-1$, show that $d_i d_j \mid d_{i+j}$; conclude that $d_1^i \mid d_i$ and $d_1^{n(n-1)} \mid \operatorname{disc}(\alpha)$.

Hint for a). Let $U_k := \langle \frac{\alpha^i}{\operatorname{disc}(S)}; i \in \{0, \ldots, k\} \rangle_R$ for $k \in \{0, \ldots, n-1\}$. Show that $\{\frac{f_i(\alpha)}{d_i}; i \in \{0, \ldots, k\}\}$ is an R-basis of $S_k := U_k \cap S$, and that $\{r \in R; rS_k \subseteq R[\alpha]\} = (d_k) \trianglelefteq R$.

(14.7) Exercise: Integral bases.
Let K be an algebraic number field, and let $\mathcal{O}$ be its ring of integers. Running through all $\mathbb{Q}$-bases $\mathcal{B}$ of K being contained in $\mathcal{O}$, show that $\mathcal{B}$ is an integral basis if and only if $|\operatorname{disc}(\mathcal{B})|$ is minimal.

(14.8) Exercise: Stickelberger's Criterion.
Let K be an algebraic number field of degree $n := [K\colon \mathbb{Q}]$, let $\mathcal{O}$ be its ring of integers, and let $\mathcal{B} := \{\alpha_1, \ldots, \alpha_n\} \subseteq K$ be a $\mathbb{Q}$-basis being contained in $\mathcal{O}$; then $\operatorname{disc}(\mathcal{B}) \in \mathbb{Z}$. Show that $\operatorname{disc}(\mathcal{B}) \equiv \{0, 1\} \pmod 4$. In particular, derive **Stickelberger's Criterion** saying that $\operatorname{disc}(\mathcal{O}) \equiv \{0, 1\} \pmod 4$.

Hint. Use Laplace expansion to compute $\det(\Delta_{\mathcal{B}})$.

(14.9) Exercise: Noetherian rings.
Let R be a commutative ring. Show that the following are equivalent:
i) R is Noetherian, that is R fulfills the ascending chain condition.
ii) Any ideal of R is finitely generated.
iii) Any non-empty set of ideals of R has a maximal element.

(14.10) Exercise: Invertible ideals.
Let R be an integral domain, and let $\{0\} \neq I \trianglelefteq R$. Show the following:

a) If $\{0\} \neq J \trianglelefteq R$, then I and J are isomorphic as R-modules if and only if there are $0 \neq r, s \in R$ such that $rI = sJ$.
b) If I is invertible then it is finitely generated. Moreover, I is invertible if and only if it is a **projective** R-module (in the categorical sense).
c) The set of invertible ideals forms an Abelian monoid, which is free if and only if R is a principal ideal domain.

(14.11) Exercise: Dedekind domains.
Let R be a Dedekind domain. Show the following:
a) If R has only finitely many prime ideals, then R is a principal ideal domain.
b) If $\{0\} \neq \mathfrak{a} \trianglelefteq R$, then all ideals of $R/\mathfrak{a}$ are principal. (Thus if $\mathfrak{a}$ is a prime ideal then $R/\mathfrak{a}$ is a principal ideal domain.)

(14.12) Exercise: Conductors.
Let $K \subseteq L$ be an extension of algebraic number fields, and let $\mathfrak{a} \trianglelefteq \mathcal{O}_L$. Show that there is an integral primitive element α of L over K, such that $\mathfrak{a}$ and the conductor $\mathrm{ann}_{\mathcal{O}_L}(\mathcal{O}_L/\mathcal{O}_K[\alpha]) \trianglelefteq \mathcal{O}_L$ are coprime.

(14.13) Exercise: Ramification and resultants.
Let $K := \mathbb{Q}(\omega)$ be an algebraic number field, where $\omega \in \mathcal{O} = \mathcal{O}_K$, and let $p \in \mathcal{P}_{\mathbb{Z}}$ neither dividing $\mathrm{ann}_{\mathbb{Z}}(\mathcal{O}/\mathbb{Z}[\omega])$ nor $[K\colon \mathbb{Q}]$. Give an alternative proof using resultants to show that p is ramified in K if and only if $p \mid \mathrm{disc}(\mathcal{O})$.

(14.14) Exercise: Ramification.
Let $K \subseteq L$ and $K \subseteq M$ be extensions of algebraic number fields, and let $\mathfrak{p} \in \mathcal{P}_K$. Show that if $\mathfrak{p}$ splits completely (respectively, is unramified) in both L and M, then $\mathfrak{p}$ splits completely (respectively, is unramified) in LM.

Conclude that $\mathfrak{p}$ splits completely (respectively, is unramified) in L if and only if $\mathfrak{p}$ splits completely (respectively, is unramified) in the normal closure of L.

(14.15) Exercise: Schmidt's Theorem.
Let $K \subseteq L$ be algebraic number fields such that $[L\colon K]$ is a prime and the normal closure of L has solvable K-automorphism group, and let $\mathfrak{p} \in \mathcal{P}_K$ be unramified in L, possessing prime divisors $\mathfrak{q} \neq \mathfrak{q}' \in \mathcal{P}_L(\mathfrak{p})$ such that $f_K(\mathfrak{q}) = f_K(\mathfrak{q}') = 1$.

Show **Schmidt's Theorem**, saying that $\mathfrak{p}$ is completely split in L.

Hint. Use **Galois's Theorem**, saying that any non-trivial element of a transitive permutation group of prime degree fixes at most one point.

(14.16) Exercise: Galois ramification.
Let $K \subseteq L$ be a Galois extension of algebraic number fields, and $G := \mathrm{Aut}_K(L)$.

a) Assume that G is non-cyclic. Show that there are only finitely many prime ideals in K which are non-split in L.

b) Let $\mathfrak{q} \in \mathcal{P}_L$ such that $D_\mathfrak{q}$ is normal in G. For any intermediate field $K \subseteq M \subseteq L$ show that $M \subseteq D_\mathfrak{q}$ if and only if $\mathfrak{p}$ splits completely in M.

(14.17) Exercise: Galois ramification.
Let $K \subseteq L$ be a Galois extension of algebraic number fields, let $G := \mathrm{Aut}_K(L)$, and let $\mathfrak{p} \in \mathcal{P}_K$. Show the following:
a) If $\mathfrak{p}$ is inert in L, then G is cyclic.
b) If $\mathfrak{p}$ is completely ramified in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G is cyclic of prime order. Likewise, if in all intermediate fields $K \subseteq M \subset L$ there is only a single prime lying over $\mathfrak{p}$, but not so in L, then G is cyclic of prime order.
c) If $\mathfrak{p}$ is unramified in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has a unique smallest non-trivial subgroup H. Likewise, if $\mathfrak{p}$ splits completely in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has a unique smallest non-trivial subgroup H.
d) If $\mathfrak{p}$ is inert in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has prime power order.

Hint for d). If a finite group G has a unique smallest non-trivial subgroup H, then G has prime power order, and H is a central subgroup of prime order.

(14.18) Exercise: Biquadratic fields.
Let $K \neq L$ be quadratic algebraic number fields, and let $p \in \mathcal{P}_\mathbb{Z}$.
a) Show that p might be completely ramified in K and L, but not so in KL. Likewise, show that in both K and L there might be only a single prime lying over p, but not so in KL.
b) Show that p might be unramified in K and L, but not so in KL. Likewise, show that p might split completely in K and L, but not so in KL.
c) Show that p might be inert in K and L, but not so in KL. Likewise, show that p might be pure in K and L, but not so in KL.
d) Still, if p is inert in *all* quadratic subfields of KL, what happens in KL?
e) Letting $\mathfrak{p} \in \mathcal{P}_{KL}(p)$, provide examples for $[e(\mathfrak{p}), f(\mathfrak{p})] \in \{[1,2],[2,1],[2,2]\}$.

(14.19) Exercise: Full lattices.
Let $V \neq \{0\}$ be an Euclidean $\mathbb{R}$-vector space, and let $\Lambda \subseteq V$ be a lattice. Show that Λ is a full lattice if and only if the quotient group V/Λ, equipped with the quotient topology, is compact.

(14.20) Exercise: Fundamental domains.
Let $n \in \mathbb{N}$, let $\Lambda \subseteq \mathbb{Z}^n \subseteq \mathbb{R}^n$ be a full sublattice, and let $\mathcal{F} \subseteq \mathbb{R}^n$ be a fundamental domain for Λ. Show that $\mathrm{vol}(\Lambda) = |\mathcal{F} \cap \mathbb{Z}^n|$.

(14.21) Exercise: Minkowski's Theorem.
We consider the Euclidean space $\mathbb{R}^{2n}$, where $n \in \mathbb{N}$. Show that the limit $\lim_{r\to\infty} \frac{|B_r(0)\cap\mathbb{Z}^{2n}|}{r}$ exists, and compute its value.

(14.22) Exercise: Minkowski's Lattice Point Theorem.
Let V be an Euclidean $\mathbb{R}$-vector space such that $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$, and let $\Lambda \subseteq V$ be a full lattice. Show that the volume bound in Minkowski's theorem cannot be improved in general, by exhibiting a convex and centrally symmetric subset $X \subseteq V$ such that $\mathrm{vol}(X) = 2^n \cdot \mathrm{vol}(\Lambda)$, but $\Lambda \cap X = \{0\}$.

(14.23) Exercise: Minkowski's Linear Form Theorem.
Let $A = [a_{ij}] \in \mathrm{GL}_n(\mathbb{R})$, where $n \in \mathbb{N}$, and for $j \in \{1, \ldots, n\}$ let $L_j \colon \mathbb{R}^n \to \mathbb{R} \colon [x_1, \ldots, x_n] \mapsto \sum_{i=1}^n x_i a_{ij}$, that is the $\mathbb{R}$-linear form given by the j-th column of A. Moreover, let $c_1, \ldots, c_n \in \mathbb{R}$ such that $c_j > 0$ and $\prod_{j=1}^n c_j > |\det(A)$.

Show **Minkowski's Linear Form Theorem** saying that there are $a_1, \ldots, a_n \in \mathbb{Z}$ such that $|L_j(a_1, \ldots, a_n)| < c_j$, for all $j \in \{1, \ldots, n\}$.

(14.24) Exercise: Minkowski's Discriminant Theorem.
Let K be an algebraic number field of degree $n := [K \colon \mathbb{Q}]$, having r real and s pairs of non-real embeddings. Give an alternative proof of Minkowski's Discriminant Theorem, avoiding Stirling's Formula, by showing directly that $\frac{1}{M_{r,s}^2} \geq \frac{\pi^n}{4}$.

Hint. Show that $\frac{n^n}{n!} \geq 2^{n-1}$ for $n \in \mathbb{N}$.

(14.25) Exercise: Real and non-real embeddings.
Let K be an algebraic number field. How can the number of real and of non-real embeddings of K (into the complex numbers $\mathbb{C}$) be determined from the minimum polynomial of a primitive element of K over $\mathbb{Q}$?

(14.26) Exercise: Totally real number fields.
Let K be an algebraic number field, such that all its embeddings into $\mathbb{C}$ are real, and let $\emptyset \neq S \subset \mathrm{Inj}_{\mathbb{Q}}(K)$. Show that there is a unit $\epsilon \in \mathcal{O}_K^*$ such that $0 < \epsilon^\sigma < 1$ for all $\sigma \in S$, and $1 < \epsilon^\sigma$ for all $\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K) \setminus S$.

(14.27) Exercise: Units in real subfields.
Let K be a Galois number field, let $K' := K \cap \mathbb{R}$.
a) Show that complex conjugation restricts to an automorphism of K, that $[K \colon K'] \leq 2$, and that K' is Galois if and only if K' has only real embeddings.
b) Show that the index $[\mathcal{O}_K^* \colon \mathcal{O}_{K'}^*]$ is finite if and only if complex conjugation is in the center of $\mathrm{Aut}_{\mathbb{Q}}(K)$.
c) Let K be the normal closure of a cubic field $\mathbb{Q}(\sqrt[3]{m})$. Show that $[\mathcal{O}_K^* \colon \mathcal{O}_{K'}^*]$ is infinite, and that there is a unit of infinite order in $\mathcal{O}_K^*$ having complex absolute value 1.

(14.28) Exercise: Kummer's Lemma.
Let K be an algebraic number field, whose normal closure has Abelian automorphism group. Show that any unit $\epsilon \in \mathcal{O}_K^*$ can be written as $\epsilon = r\zeta \in \mathbb{C}$, where $r \in \mathbb{R}$ and $\zeta \in \mathbb{C}$ is a root of unity, and both r and ζ belong to K or a quadratic extension of K.

(14.29) Exercise: Finiteness of class groups.
This is an alternative approach to prove the finiteness of class groups of algebraic number fields, without using Minkowski's Theorem:

a) Let K be an algebraic number field, let $\mathcal{O} := \mathcal{O}_K$ be its ring of integers, let $\mathcal{B} \subseteq \mathcal{O}$ be an integral basis, and let $c_K := \prod_{\sigma \in \mathrm{Inj}_{\mathbb{Q}}(K)} (\sum_{\omega \in \mathcal{B}} \|\omega^\sigma\|) \in \mathbb{R}$. Show that for any ideal $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$ there is $0 \neq \alpha \in \mathfrak{a}$ such that $|N_K(\alpha)| \leq c_K \cdot N(\mathfrak{a})$.

b) Show that any ideal class of $\mathcal{O}$ contains an ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq c_K$. Compare c_K with the Minkowski bound $b_K = M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|}$, where r and s are the number of real and of non-real embeddings of K, respectively.

(14.30) Exercise: Finiteness of class groups.
This is a simplified approach to prove the finiteness of class groups of algebraic number fields, using Minkowski's Theorem but yielding a weaker bound:

a) Let K be an algebraic number field, let $\mathcal{O} := \mathcal{O}_K$ be its ring of integers, and let r and s be the number of real and of non-real embeddings of K, respectively. Show that any ideal $\{0\} \neq \mathfrak{a} \trianglelefteq \mathcal{O}$ possesses an element $0 \neq \alpha \in \mathfrak{a}$ such that $|N_K(\alpha)| \leq (\frac{2}{\pi})^s \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{a})$.

b) Conclude that any ideal class of $\mathcal{O}$ contains an ideal $\mathfrak{a}$ such that $N(\mathfrak{a}) \leq (\frac{2}{\pi})^s \cdot \sqrt{|\mathrm{disc}(K)|}$. Compare this with the Minkowski bound $M_{r,s} \cdot \sqrt{|\mathrm{disc}(K)|}$.

Hint for a). Use a subset of $\mathbb{R}^n$ consisting of the vectors $[x_1, \ldots, x_n]$ such that $|x_i| \leq c_i$ for $i \in \{1, \ldots, r\}$, and $x_{r+2j-1}^2 + x_{r+2j}^2 \leq c_{r+j}$ for $j \in \{1, \ldots, s\}$, where $c_1, \ldots, c_{r+s} \in \mathbb{R}$ such that $c_k > 0$ and $\prod_{k=1}^{r+s} c_k \geq (\frac{2}{\pi})^s \cdot \sqrt{|\mathrm{disc}(K)|} \cdot N(\mathfrak{a})$.

(14.31) Exercise: Four-squares theorem.
a) Show that an integer of shape $4^a \cdot (8k-1)$, where $a \in \mathbb{N}_0$ and $k \in \mathbb{N}$, cannot be written as a sum of three squares in $\mathbb{Z}$. (The converse also holds [Legendre, 1798], but we are not able to show this here.)
b) Show that if $p \in \mathcal{P}_{\mathbb{Z}}$ is odd, then $4p$ is a sum of four odd squares in $\mathbb{Z}$.

(14.32) Exercise: Legendre symbols.
Let $p \in \mathcal{P}_{\mathbb{Z}}$ be odd. Show that p can be written as $p = a^2 + 2b^2$, where $a, b \in \mathbb{Z}$, if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

(14.33) Exercise: Legendre symbols.
Let $0 \neq a \in \mathbb{Z}$. Show that
a) there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = 1$;
b) there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = -1$.

(14.34) Exercise: Quadratic polynomials.
a) For $a \in \mathbb{Z}$, show that any prime divisor p of $4a^2+1 \in \mathbb{Z}$ fulfills $p \equiv 1 \pmod 4$.
b) Show that any prime divisor p of $9a^2 + 3a + 1 \in \mathbb{Z}$ fulfills $p \equiv 1 \pmod 3$.

(14.35) Exercise: Primes in arithmetic progressions.
We consider another (easy) special case of **Dirichlet's Theorem [1837]** on primes in coprime residue classes:
a) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv -1 \pmod 3$.
b) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod 3$.

(14.36) Exercise: Primes in arithmetic progressions.
Show a (not so easy) special case of **Dirichlet's Theorem [1837]** on primes in coprime residue classes: For any $n \geq 2$ there are infinitely many primes $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod n$.

Hint. Assume to the contrary that there are only finitely many such primes, and let m be their product. Then choose $a \in \mathbb{Z}$ and $q \in \mathcal{P}_{\mathbb{Z}}$ such that $q \mid \Phi_n(anm)$.

(14.37) Exercise: Abelian Galois groups.
Show that for any finite Abelian group G there is a Galois algebraic number field K such that $\mathrm{Aut}_{\mathbb{Q}}(K) \cong G$.

Hint. Use Dirichlet's Theorem.

15 Exercises: Examples

(15.1) Exercise: Euclidean quadratic fields.
For $d \in \mathbb{Z} \setminus \{0, 1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$.
a) For $d \in \{-2, -1, 2, 3\} \dot\cup \{-11, -7, -3, 5, 13\}$ show that $\mathcal{O}_d$ is Euclidean with respect to the absolute norm map.
b) For $d \leq -13$ show that $\mathcal{O}_d$ is not Euclidean (for any degree map).

Hint for a). Generalize the method used for $\mathbb{Z}[i]$.

(15.2) Exercise: Factorial imaginary quadratic fields.
For $d \in \mathbb{Z} \setminus \{0, 1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Show that $\mathcal{O}_d$ is factorial, by showing that it has trivial class group, for

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

(15.3) Exercise: Factorial imaginary quadratic fields.
For $0 > d \in \mathbb{Z}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$.

a) If $\mathcal{O}_d$ has trivial class group, show the following:
i) We have $d \equiv 5 \pmod 8$, unless $d \in \{-1, -2, -7\}$.
ii) If $2 \neq p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \nmid d$ and $0 < -d < 4p$, then $\left(\frac{d}{p}\right) = -1$.
iii) If $d < -19$, then $d \equiv \{-43, -67, -163, -403, -547, -667\} \pmod{840}$.

b) Determine all $-2000 < d < 0$ such that $\mathcal{O}_d$ has trivial class group.

(15.4) Exercise: Factorial quadratic fields.
For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$, and assume that $\mathcal{O}_d$ has trivial class group. Show the following:
a) If $p \in \mathcal{P}_\mathbb{Z}$ is not inert, then there is $\alpha \in \mathcal{O}_d$ such that $|N(\alpha)| = p$.
b) If $2 \neq p \in \mathcal{P}_\mathbb{Z}$ is ramified, and $\alpha \in \mathcal{O}_d$ such that $p \nmid N(\alpha)$, then $\left(\frac{N(\alpha)}{p}\right) = 1$.
c) For $d < -2$ we have $d \equiv 1 \pmod 4$ and $-d \in \mathcal{P}_\mathbb{Z}$.
d) For $d > 1$ we have $d \in \mathcal{P}_\mathbb{Z}$, or $d = pq$ for $p, q \in \mathcal{P}_\mathbb{Z}$ such that $p, q \not\equiv 1 \pmod 4$.

Hint for c) and d). Use Dirichlet's Theorem, and consider Legendre symbols.

(15.5) Exercise: Non-factorial quadratic fields.
For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Show that $\mathcal{O}_d$ is not factorial for the following d (actually these are all cases for $|d| \leq 30$), by exhibiting elements having non-unique factorizations into irreducible elements:
i) $d \in \{-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30\}$.
ii) $d \in \{10, 15, 26, 30\}$.

(15.6) Exercise: Class numbers of quadratic fields.
For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$, let Cl_d be its class group, and let $h_d \in \mathbb{N}$ be its class number. Show the following:
i) If $d \in \{2, 3, 5, 6, 7, 173, 293, 437\}$, then $h_d = 1$.
ii) If $d \in \{-6, -10, 10\}$, then $h_d = 2$.
iii) If $d \in \{-23, -31, -83, -139, 223\}$, then $h_d = 3$.
iv) If $d \in \{-14, -39\}$, then $h_d = 4$, where Cl_d is cyclic.
v) If $d \in \{-21, -30\}$, then $h_d = 4$, where Cl_d is non-cyclic.
vi) If $d = -103$, then $h_d = 5$.

(15.7) Exercise: Class numbers of biquadratic fields.
Determine the ring of integers of the biquadratic field $K := \mathbb{Q}(\sqrt{2}, \sqrt{-3})$, and its class number. Compare with the class number of its quadratic subfields.

(15.8) Exercise: Non-factorial domains.
For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free let $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$, and let $R_d := \mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_d$; recall that $R_d = \mathcal{O}_d$ if and only if $d \not\equiv 1 \pmod 4$.
a) Let $d \leq -3$ be odd. Show that $2 \in R_d$ is irreducible but not prime.
b) Let $d \leq -5$ such that $d \equiv -1 \pmod 4$. Show that $d - 1$ and $2 + 2\sqrt{d}$ do not have a greatest common divisor in R_d.
c) Let $d := -3$. Show that there is a unique prime ideal $\mathfrak{p} \lhd R_{-3}$ containing (2), and show that $\mathfrak{p} \neq (2)$ and $\mathfrak{p}^2 = 2\mathfrak{p}$. Is (2) a product of prime ideals?

What do the above results imply for $\mathcal{O}_d$?

(15.9) Exercise: Factorization of ideals.
For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free let $\mathcal{O}_d$ and $\widehat{\mathcal{O}}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, respectively. Determine the factorization of the following ideals:

a) i) $(6) \trianglelefteq \mathcal{O}_{30}$, **ii)** $(6) \trianglelefteq \mathcal{O}_{-6}$, **iii)** $(14) \trianglelefteq \mathcal{O}_{-10}$, **iv)** $(30) \trianglelefteq \mathcal{O}_{-29}$.

b) i) $(6) \trianglelefteq \widehat{\mathcal{O}}_{-3}$, **ii)** $(14) \trianglelefteq \widehat{\mathcal{O}}_{-5}$

(15.10) Exercise: Primes as sums of two squares (GAP).
a) Write a GAP program implementing the (extended) Euclidean algorithm for the Gaussian integers $\mathbb{Z}[i]$. (Of course, any other computer algebra system may be used as well. As far as GAP is concerned, the Euclidean algorithm is readily available there, but you should implement it on your own, only building on GAP functions whose names do not contain capital letters.)

b) Write a GAP program which for a prime $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod 4$ computes its decomposition as a sum of two squares in $\mathbb{Z}$. (Think of an efficient method to compute a primitive 4-th root of unity modulo p.) Try your implementation for a few large primes p. How far do you get?

(15.11) Exercise: Pythagorean triples.
Show that the primitive positive integer solutions of the equation $X^2+Y^2 = Z^2$ are the triples $[x, y, z]$ and $[y, x, z]$ such that $x = u^2 - v^2$ and $y = 2uv$ and $z = u^2 + v^2$, for some $u, v \in \mathbb{Z}$ coprime such that $u > v \geq 1$ and $2 \mid uv$.

Hint. Use the ring $\mathbb{Z}[i]$.

(15.12) Exercise: Fermat equation.
Show that for $n = 4$ there are no non-trivial integral solutions of the Fermat equation $X^n + Y^n = Z^n$.

Hint. Consider a primitive solution $[x, y, u] \in \mathbb{N}^3$ of the equation $X^4+Y^4 = U^2$, where u is minimal, and use the classification of primitive Pythagorean triples.

(15.13) Exercise: Diophantine equations.
a) Show that $n = 0$ is the only integer such that $n^2 + 1$ is a cube.
b) Show that $n \in \{\pm 2, \pm 11\}$ are the only integers such that $n^2 + 4$ is a cube.
c) Show that there is no integer n such that $n^2 + 5$ is a cube.

Hint. In a) and b), use the ring $\mathbb{Z}[i]$, and in b) distinguish the cases n even and odd; in c), use the ring $\mathbb{Z}[\sqrt{-5}]$.

(15.14) Exercise: Diophantine equations.
Show **Fermat's Theorem**, saying that $n = 26$ is the only integer such that $n - 1$ is a square and $n + 1$ is a cube.

Hint. Use the ring $\mathbb{Z}[\sqrt{-2}]$.

(15.15) Exercise: Diophantine equations.
Show the **Ramanujan-Nagell Theorem**, saying that $n \in \pm\{1, 3, 5, 11, 181\}$ are the only integers such that $n^2 + 7$ is a 2-power.

Hint. Use the ring $\mathbb{Z}[\alpha]$, where $\alpha := \frac{1}{2}(1+\sqrt{-7})$, which by Exercise (15.1) is factorial, and recall that $N(\alpha) = 2$.

(15.16) Exercise: Lind-Reichardt equation.
a) Show that the diophantine equation $X^4 = 2Y^2 + 17$ has a solution modulo any prime $p \in \mathcal{P}_\mathbb{Z}$ such that $p \equiv \pm 1 \pmod 8$ or $p \equiv 3 \pmod 8$. What happens for $p \equiv -3 \pmod 8$?
b) Show that the equation $X^4 = 2Y^2 + 17Z^4$ has no non-trivial integral solution.

(15.17) Exercise: Rings of integers in cubic fields.
For $m \in \{3, 5, 6, 7\}$ let $K := \mathbb{Q}(\sqrt[3]{m})$. Determine the embeddings of K into $\mathbb{C}$, an integral basis of K, the ring of integers of K, and its discriminant.

(15.18) Exercise: Rings of integers in cubic fields.
a) Let $K := \mathbb{Q}(\sqrt[3]{175})$. Determine the embeddings of K into $\mathbb{C}$, an integral basis of K, the ring of integers $\mathcal{O} \subseteq K$, and its discriminant.
b) Show that K does not have an integral basis $\{1, \omega, \omega^2\}$ for any $\omega \in \mathcal{O}$.

Hint for a). Consider $\sqrt[3]{245} \in \mathbb{R}$ as well.

(15.19) Exercise: Rings of integers in cubic fields.
Let $\alpha \in \mathbb{R}$ such that $\alpha^3 = \alpha + 4$. Show that $\{1, \alpha, \frac{1}{2}\alpha(1+\alpha)\}$ is an integral basis of $\mathbb{Q}(\alpha)$, and determine its discriminant.

(15.20) Exercise: Rings of integers in cubic fields.
We consider **Dedekind's example** $K := \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{R}$ is such that $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$. Let $\mathcal{O}$ be the ring of integers of K.
a) Show that $\{1, \alpha, \frac{1}{2}\alpha(1+\alpha)\}$ is an integral basis of K, and determine the discriminants $\operatorname{disc}(\mathcal{O})$ and $\operatorname{disc}(\mathbb{Z}[\alpha])$.
b) Show that the prime 2 splits completely in K.
c) Show that the index $[\mathcal{O}\colon \mathbb{Z}[\omega]]$ is even, for any $\omega \in \mathcal{O} \setminus \mathbb{Z}$. Conclude that K does not have an integral basis consisting of powers of a single element.

(15.21) Exercise: Decomposition fields and inertia fields.
Let $K := \mathbb{Q}(\sqrt[3]{19})$ and $p := 3$.
a) Compute the normal closure $K \subseteq L \subseteq \mathbb{C}$, determine $\operatorname{Aut}_\mathbb{Q}(L)$ and the embeddings of K into $\mathbb{C}$, an integral basis of L, its ring of integers, and its discriminant.
b) Compute the factorization of p in K and in L, determine the associated decomposition and inertia fields, with respect to both $\mathbb{Q}$ and K, and compute the factorization of p in these intermediate fields.

(15.22) Exercise: Class numbers of cubic number fields.
a) For $m \in \{3, 5, 6, 17, 19\}$ let $K := \mathbb{Q}(\sqrt[3]{m})$, and let $\mathcal{O}_m$ be its rings of integers. Determine $\mathcal{O}_m$ for $m \in \{17, 19\}$ (recall $\mathcal{O}_m$ for $m \in \{3, 5, 6\}$ from Exercise (15.17)), and show that $\mathcal{O}_m$ has trivial class group.

b) Find the ring of integers of $\mathbb{Q}(\sqrt[3]{19})$, and show that it has class number 3.
c) Let $\alpha \in \mathbb{R}$ such that $\alpha^3 = \alpha + 1$, and let $\beta \in \mathbb{R}$ such that $\beta^3 = \beta + 7$. Show that both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ have trivial class group.

(15.23) Exercise: Units in cubic number fields.
a) Let K be a cubic number field having a unique real embedding, and $\mathcal{O} := \mathcal{O}_K$. Show that $\mathcal{O}^* = \pm\langle\epsilon\rangle$, where $\epsilon > 1$ is a uniquely defined fundamental unit.
b) Let $\rho \cdot \exp(\pm i\varphi) \in \mathbb{C}$ be the algebraic conjugates of ϵ, where $\rho > 0$ and $0 < \varphi < \pi$. Show that $\epsilon = \rho^{-2}$ and that $\mathrm{disc}(\epsilon) = -4\sin(\varphi)^2 \cdot (\rho^3 + \rho^{-3} - 2\cos(\varphi))$, and conclude that $|\mathrm{disc}(\epsilon)| < 4(\epsilon^3 + \epsilon^{-3} + 6)$.
c) Let $d := |\mathrm{disc}(\mathcal{O})|$. Show that $\epsilon^3 > \frac{d-28}{4}$, where for $d \geq 33$ even $\epsilon^3 > \frac{d-27}{4}$.

(15.24) Exercise: Units in cubic number fields.
a) For $m \in \{2, 3, 5, 6, 7\}$ let $K := \mathbb{Q}(\sqrt[3]{m})$. Determine the fundamental unit $\epsilon \in \mathcal{O}_K^*$ such that $\epsilon > 1$.
b) Let $\alpha \in \mathbb{R}$ such that $\alpha^3 + \alpha - 3 = 0$, and let $K := \mathbb{Q}(\alpha)$ Determine its ring of integers $\mathcal{O}$, show that K has only one real embedding, and determine the fundamental unit $\epsilon \in \mathcal{O}^*$ such that $\epsilon > 1$.
c) Let $\beta \in \mathbb{R}$ such that $\beta^3 - 2\beta - 3 = 0$, and let $K := \mathbb{Q}(\beta)$ Determine its ring of integers $\mathcal{O}$, show that K has only one real embedding, and determine the fundamental unit $\epsilon \in \mathcal{O}^*$ such that $\epsilon > 1$.

(15.25) Exercise: Factorization of ideals (partly GAP).
Let $\alpha \in \mathbb{R}$ such that $\alpha^5 = 5(\alpha + 1)$, let $K := \mathbb{Q}(\alpha)$, and let $\mathcal{O} := \mathcal{O}_K$.
a) Show that $\mathrm{disc}(\mathbb{Z}[\alpha]) = 3^2 \cdot 5^5 \cdot 41$, and that $\mathrm{ann}_{\mathbb{Z}}(\mathcal{O}/\mathbb{Z}[\alpha]) = (3) \trianglelefteq \mathbb{Z}$.
b) Using GAP, compute the factorization of $p\mathcal{O} \lhd \mathcal{O}$ for the rational primes $p \neq 3$ up to 10^4 (say). What do you observe for the inertia degrees occurring?

(15.26) Exercise: Norms in cyclotomic number fields.
Let $\zeta := \zeta_5 \in \mathbb{C}$, let $K := \mathbb{Q}(\zeta)$, and let $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[\zeta]$.
a) For any $\alpha \in \mathcal{O}$ show that $N(\alpha) = \frac{1}{4} \cdot (a^2 - 5b^2)$ for suitable $a, b \in \mathbb{Z}$. Conclude that the group of units of $\mathcal{O}$ is infinite.
b) Show that $N(a + b\zeta) = \sum_{i=0}^{4} (-1)^i a^i b^{4-i}$, for $a, b \in \mathbb{Z}$. Use this to calculate $N(\zeta + k)$ for $k \in \{-3, -2, 2, 3, 4\}$, and write the latter as products of irreducible elements of $\mathcal{O}$. Similarly, provide factorizations of 11, 31, and 61 in $\mathcal{O}$.

Hint for a). Use Gaussian sums.

(15.27) Exercise: Euclidean cyclotomic number fields.
For $m \in \mathbb{N}$ let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of unity, let $\mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field; then $\mathbb{Z}[\zeta_m]$ is its ring of integers.
a) Show that $\mathbb{Z}[\zeta_8]$ is Euclidean.
b) Show that $\mathbb{Z}[\zeta_5]$ is Euclidean.

(15.28) Exercise: Real subfields of cyclotomic fields.
Let $\zeta := \zeta_m \in \mathbb{C}$ be a primitive m-th root of unity, where $m \geq 3$, let $\omega := \zeta + \zeta^{-1}$, let $K := \mathbb{Q}(\omega)$ and let $\mathcal{O} := \mathcal{O}_K$.
a) Show that $K = \mathbb{Q}(\zeta) \cap \mathbb{R}$ and that $\mathcal{O} = \mathbb{Z}[\omega]$.
b) Let $m := p$ be an odd prime. Show that $\mathrm{disc}(\mathcal{O}) = p^{\frac{p-3}{2}}$.

Hint. Show that both the sets $\{\zeta^{-(k-1)}, \ldots, \zeta^{-1}, 1, \zeta, \ldots, \zeta^{k-1}\} \subseteq \mathbb{Q}(\zeta)$ and $\{1, \omega, \zeta, \zeta\omega, \ldots, \zeta^{k-1}, \zeta^{k-1}\omega\} \subseteq \mathbb{Q}(\zeta)$ are integral bases, where $k = \frac{\varphi(m)}{2}$.

(15.29) Exercise: Cyclotomic fields (partly GAP).
a) Let $r, e, f \in \mathbb{N}$. Show that there are rational primes $p, l \in \mathcal{P}_\mathbb{Z}$ such that $p \equiv 1 \pmod{e}$, and p splits into r distinct prime ideals in $\mathbb{Q}(\zeta_l)$, and such that $\mathbb{Q}(\zeta_l)$ has a subfield of degree rf. How does p split in this subfield?
b) Assuming the above setting, show that $\mathbb{Q}(\zeta_{pl})$ has a subfield in which p splits into r prime ideals, each having ramification index e and inertial degree f.
c) Write a GAP program which for $r, e, f \in \mathbb{N}$ computes rational primes p, l and a subfield of $\mathbb{Q}(\zeta_{pl})$ as above. Apply this in particular for $e := 2$, $f := 3$, $r := 5$.

(15.30) Exercise: Non-factorial cyclotomic number fields (GAP).
Show that the ring of integers of $\mathbb{Q}(\zeta_{31})$ is not factorial.

Hint. Use an element of small norm, and a suitable quadratic field.

(15.31) Exercise: Units in cyclotomic number fields.
Let $m \in \mathbb{N}$, let $K_m := \mathbb{Q}(\zeta_m)$ and $\mathcal{O}_m := \mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$, let $K'_m := \mathbb{Q}(\zeta_m) \cap \mathbb{R}$ and $\mathcal{O}'_m := \mathcal{O}_{K'_m} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$, see Exercise (15.28).
a) For $k \in (\mathbb{Z}/(m))^*$ show that $\frac{1-\zeta_m^k}{1-\zeta_m} \in \mathcal{O}_m^*$. (The subgroup of $\mathcal{O}_m^*$ generated by these elements is called the group of **cyclotomic units**.)
b) Let $p \in \mathcal{P}_\mathbb{Z}$. Show that $\mathcal{O}_p^* = \langle \zeta_p \rangle \times (\mathcal{O}'_p)^*$.
c) Now let $p := 5$. Determine K'_5 and $\mathcal{O}'_5$ and $(\mathcal{O}'_5)^*$, and show that we have $\mathcal{O}_5^* = \{\zeta_5^k \cdot (1 + \zeta_5)^n \in \mathcal{O}_5; k \in (\mathbb{Z}/(5))^*, n \in \mathbb{Z}\}$.

(15.32) Exercise: Class numbers of cyclotomic number fields.
For $p \in \{7, 11, 13\}$ let $\omega := \zeta_p + \zeta_p^{-1} \in \mathbb{C}$, let $K := \mathbb{Q}(\omega)$, and let $\mathcal{O} := \mathbb{Z}[\omega]$ be its ring of integers, see Exercise (15.28). Show that $\mathcal{O}$ has trivial class group.

(15.33) Exercise: Quadratic and cyclotomic fields.
a) Show that any quadratic field is a subfield of a suitable cyclotomic field.
b) Let $n \geq 3$ be odd. Describe the quadratic subfields of $\mathbb{Q}(\zeta_n)$.
c) Let $k \geq 3$. Describe the quadratic subfields of $\mathbb{Q}(\zeta_{2^k})$.

(15.34) Exercise: Ramification in function fields.
Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. We consider the plane curve $\{[t^2, t] \in \mathbb{F}^2; t \in \mathbb{F}\}$, having affine coordinate algebra $S := \mathbb{F}[X, Y]/(Y^2 - X)$. Letting $R := \mathbb{F}[X]$ and $K := \mathrm{Q}(R)$,

the projection morphism onto the first coordinate gives rise to the natural $\mathbb{F}$-algebra homomorphism $\pi\colon R \to S\colon X \mapsto \overline{X}$.

a) Show the following: The ring S is a univariate polynomial algebra; let $L := \mathrm{Q}(S)$. The map π is injective; hence we may consider R as a subalgebra of S.

The field extension $K \subseteq L$ is Galois; determine the degree $[L\colon K]$. The ring extension $R \subseteq S$ is finite, S is the integral closure of R in L, and S is a free R-module. Determine the trace R-bilinear form of S, and compute the discriminant $\mathrm{disc}_R(S) \in R/(\mathbb{F}^*)^2$ of S.

b) Determine the sets $\mathcal{P}_R$ and $\mathcal{P}_S$ of non-zero prime ideals of R and S, respectively, and show the following:

Both sets consist of maximal ideals. The sets $\mathcal{P}_S(\mathfrak{p}) := \{\mathfrak{q} \in \mathcal{P}_S; \mathfrak{q} \cap R = \mathfrak{p}\}$ for $\mathfrak{p} \in \mathcal{P}_R$, are non-empty and form a partition of $\mathcal{P}_S$. Actually, $\mathcal{P}_S(\mathfrak{p})$ consists of a single orbit under $\mathrm{Aut}_K(L)$, and we have $\mathfrak{p}S = (\prod_{\mathfrak{q}\in\mathcal{P}_S(\mathfrak{p})} \mathfrak{q})^{e_\mathfrak{p}} \lhd S$, for some $e_\mathfrak{p} \in \mathbb{N}$. What is the geometrical interpretation of the ramification index $e_\mathfrak{p}$? How does ramification relate to the discriminant $\mathrm{disc}_R(S)$?

Letting $\mathbb{E} := S/\mathfrak{q}$, then $\mathbb{E}$ is independent of the choice of $\mathfrak{q} \in \mathcal{P}_S(\mathfrak{p})$; determine the embedding $\mathbb{F} \subseteq \mathbb{E}$, and the degree $f_\mathfrak{p} := [\mathbb{E}\colon \mathbb{F}] \in \mathbb{N}$. We have $|\mathcal{P}_S(\mathfrak{p})| \cdot e_\mathfrak{p} \cdot f_\mathfrak{p} = [L\colon K]$. What is the geometrical interpretation of the inertia degree $f_\mathfrak{p}$? Determine the associated decomposition and inertia groups.

Hint for b). For $\mathbb{F} = \mathbb{C}$ distinguish the cases $x = 0$ and $x \neq 0$, while for $\mathbb{F} = \mathbb{R}$ distinguish the cases $x = 0$ and $x > 0$ and $x < 0$.

(15.35) Exercise: Values of polynomials.
Let $f := X^2 + aX + b \in \mathbb{Z}[X]$ be irreducible, let $\mathrm{im}(f)$ be the image of the polynomial function $f\colon \mathbb{Z} \to \mathbb{Z}$, let $\mathcal{P}_f \subseteq \mathcal{P}_\mathbb{Z}$ be the set of prime divisors of the elements of $\mathrm{im}(f)$, and let $\mathcal{P}_\delta \subseteq \mathcal{P}_\mathbb{Z}$ be the set of prime divisors of $\delta := \mathrm{disc}(f)$.

Show that $\mathcal{P}_f \setminus \mathcal{P}_\delta$ is the preimage of a subgroup of $(\mathbb{Z}/(\delta))^*$ of index 2.

(15.36) Exercise: Carmen de Hastingae Proelio.
All historians know that there is a great deal of mystery and uncertainty concerning the details of the ever-memorable battle [near Hastings] *on that fatal day, October 14, 1066. Here is the passage in question:*

The men of Harold stood well together, as their wont was, and formed sixty and one squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon war-hatchet would break his lance and cut through his coat of mail... When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle-cries 'Ut!', 'Olicrosse!', 'Godemitè!'.

What is the smallest possible number of men there could have been?

(15.37) Exercise: Archimedes's Problema Bovinum.
If thou art diligent and wise, O stranger, compute the number of cattle of the Sun, who once upon a time grazed on the fields of the Thrinacian isle of Sicily, divided into four herds of different colours, one milk white, another a glossy black, a third yellow and the last dappled. In each herd were bulls, mighty in number according to these proportions: Understand, stranger, that the white bulls were equal to a half and a third of the black together with the whole of the yellow, while the black were equal to the fourth part of the dappled and a fifth, together with, once more, the whole of the yellow. Observe further that the remaining bulls, the dappled, were equal to a sixth part of the white and a seventh, together with all of the yellow. These were the proportions of the cows: The white were precisely equal to the third part and a fourth of the whole herd of the black; while the black were equal to the fourth part once more of the dappled and with it a fifth part, when all, including the bulls, went to pasture together. Now the dappled in four parts were equal in number to a fifth part and a sixth of the yellow herd. Finally the yellow were in number equal to a sixth part and a seventh of the white herd. If thou canst accurately tell, O stranger, the number of cattle of the Sun, giving separately the number of well-fed bulls and again the number of females according to each colour, thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise.

But come, understand also all these conditions regarding the cattle of the Sun. When the white bulls mingled their number with the black, they stood firm, equal in depth and breadth, and the plains of Thrinacia, stretching far in all ways, were filled with their multitude. Again, when the yellow and the dappled bulls were gathered into one herd they stood in such a manner that their number, beginning from one, grew slowly greater till it completed a triangular figure, there being no bulls of other colours in their midst nor none of them lacking. If thou art able, O stranger, to find out all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.

Hint. The first part amounts to solving a system of diophantine linear equations, the second part leads to a Pell equation; anyway you better use GAP.

---

16 References

[1] E. Artin: Galois theory. Dover Publications, 1998.

[2] P. Bundschuh: Einführung in die Zahlentheorie. Springer-Lehrbuch, Springer, 2008.

[3] H. Cohen: A course in computational algebraic number theory. Grad. Texts in Math. 138, Springer, 1993.

[4] D. Eisenbud: Commutative algebra, with a view toward algebraic geometry. Graduate Texts in Mathematics 150, Springer, 1995.

[5] G. Hardy, E. Wright: An introduction to the theory of numbers. Oxford University Press, 2008.

[6] H. Koch: Zahlentheorie, Algebraische Zahlen und Funktionen. Vieweg Studium, Aufbaukurs Mathematik 72, 1997.

[7] D. Marcus: Number fields. Springer Universitext, Springer, 2018.

[8] H. Matsumura: Commutative ring theory. Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, 1987.

[9] H. Minkowski: Geometrie der Zahlen. Teubner, 1910.

[10] J. Neukirch: Algebraische Zahlentheorie. Springer, 1992.

[11] A. Schmidt: Einführung in die algebraische Zahlentheorie. Springer-Lehrbuch, Springer, 2007.

[12] I. Stewart, D. Tall: Algebraic number theory and Fermat's last theorem. Chapman & Hall, 2015.