Basic Algebraic Number Theory

Vítězslav Kala

April 4, 2026

Contents

Introduction

This is a working draft of lecture notes for the Master's course *Basic Algebraic Number Theory*. The course is a partial follow-up to Bachelor's courses *Number Theory* and *Introduction to Commutative Algebra*, for both of which there are Czech lecture notes:

- V. Kala, *Teorie čísel* [in Czech]
  https://www.karlin.mff.cuni.cz/~kala/files/TC25.pdf
- V. Kala, *Úvod do komutativní algebry* [in Czech]
  https://www.karlin.mff.cuni.cz/~kala/files/UKA25.pdf

I am very grateful to Matyáš Kafka for typing the very first draft on the basis of my lectures from Spring 2025, as well as to numerous other students for pointing out errors. Claude Opus 4.6 also did some proof-reading and corrections. *The current version is very far from perfect, so please do not hesitate to email me any corrections!*
The lectures themselves are based on several sources, primarily:

- A. Drápal, *Komutativní okruhy* [in Czech]
  http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf
- K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics 84 (Second Edition)
- J. Milne, *Algebraic Number Theory*,
  http://www.jmilne.org/math/CourseNotes/ant.html

1. Basics

1.1 Notation

Here is some notation that may differ from other courses at CUNI and that is consistently used throughout these notes (as it is standard in algebraic number theory):

- If we write $A \subset B$, we allow $A = B$. If we want to write that A is a proper subset of B, we write $A \subsetneq B$.
- $R^\times$ denotes the set of invertible elements of a ring R.
- If L, K are fields, we use the symbol L/K (read "L over K") to denote that L is a field extension of K.
- We use the symbol $\#$ to denote the number of elements in a set, e.g., $\#G$ is the number of elements of G.

Let us also recall the following standard notation that we'll use:
For a field K, we denote its *algebraic closure* by $\overline{K}$.
Let $L \supset K$ be a field extension and $\alpha \in L$ be algebraic over K. The monic *minimal polynomial* for α over K is denoted $m_{\alpha,K}(x) \in K[x]$. By a *conjugate* of α we mean a root of the minimal polynomial $m_{\alpha,K}(x)$.
I'll probably add a few more things here later.

1.2 Motivation

To motivate our interest in some of the topics we will study, we will outline a failed proof of Fermat's Last Theorem (or FLT for short).

Theorem 1.1 (Fermat's Last Theorem)**.** *For $n \geq 3$, the equation*

$$x^n + y^n = z^n$$

has no nonzero solutions in $\mathbb{Z}$.

"Proof":
Let $n \geq 3$ and assume towards contradiction that the triple (x, y, z) solves the equation. WLOG we can assume that x, y, z are coprime. We can rewrite the equation as:

$$y^n = z^n - x^n = (z - x)(z - \zeta_n x) \dots (z - \zeta_n^{n-1} x),$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$ denotes the primitive n-th root of unity. The rest of the proof is divided into the following steps.

Step A:
The terms $(z - x), (z - \zeta_n x), \dots, (z - \zeta_n^{n-1} x)$ are (essentially) coprime in $\mathbb{Z}[\zeta_n]$.

Step B:

We factor the terms into irreducibles

$$\begin{aligned} z - x &= \pi_1^{a_1} \dots \pi_k^{a_k} \\ z - \zeta_n x &= \rho_1^{b_1} \dots \rho_l^{b_l} \\ &\vdots \end{aligned}$$

Step A implies that π_i and ρ_j are pairwise distinct. Now we can rewrite the LHS like this

$$y^n = \pi_1^{na_1'} \dots \rho_1^{nb_1'} \dots$$

But then all the exponents on the RHS are divisible by n.

Step C:
Thus we can write

$$\begin{aligned} z - x &= \alpha^n \\ z - \zeta_n x &= \beta^n \\ &\vdots \end{aligned}$$

for some $\alpha, \beta, \dots \in \mathbb{Z}[\zeta_n]$.

Step D:
Our aim now is to write $\alpha, \beta, \dots$ in some basis and compare the coefficients to arrive at a contradiction.

Now it is important to note that this proof would not be a viable proof of Fermat's Last Theorem in general case, but if we address the problems in this proof, we can make it work in certain special cases (see Theorem 5.8).

Problems:

- First, it is useful to assume that n is an odd prime. Once the proof is done for primes, one easily proves the theorem for composite numbers. Let us denote this odd prime as p.
- Now we should distinguish the so-called 1st and 2nd case of FLT. The 1st case is when p does not divide xyz and the 2nd case is when it does.
- Since $\mathbb{Z}[\zeta_p]$ need not be a UFD in general, the factorization into irreducibles in Step B may not be unique. We should instead factor into prime ideals.
- After factoring into prime ideals, we will only get $z - x = A^p$ etc. for some ideal A in Step C. We need to introduce a "class group" which will be trivial iff $\mathbb{Z}[\zeta_p]$ is UFD. If we then limit ourselves to *regular primes*, i.e., those that do not divide the size of this class group, then we can replace the ideal A with an element (after considering invertible elements).

After solving these problems, we will be able to prove the 1st case of Fermat's Last Theorem for regular primes (see Theorem 5.8). This way the proof serves as a motivation for us to study the class group and other related topics.

1.3 Recap

In this section we state important definitions and theorems from the introductory Commutative Algebra course that we will need. All proofs and further details can be found in my lecture notes (in Czech only):
https://karlin.mff.cuni.cz/~kala/files/UKA25.pdf
We may also sometimes need to reference theorems or propositions, which can be found in this text. These will be marked by the number of the theorem preceded by "ÚKA", e.g., "ÚKA věta 1.1".

Definition. A *number field* K is a finite degree extension of $\mathbb{Q}$.

Theorem 1.2 (Primitive element theorem)**.** *Let K be a number field. Then there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.*

Definition. Let $K \supset \mathbb{Q}$ be a field. Then
a) Let $S \supset R$ be rings. We say that $\alpha \in S$ is *integral* over R if there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.
b) $\mathcal{O}_K$ denotes the ring of elements $\alpha \in K$ that are integral over $\mathbb{Z}$.

Theorem 1.3. *Let $S \supset R$ be rings. Then TFAE:*
a) $\alpha \in S$ is integral over R.
b) The minimal polynomial for α over R is monic.
c) $R[\alpha]$ is a finitely generated R-module.
d) There exists R' such that $R[\alpha] \subset R' \subset S$ and R' is a finitely generated R-module.

Definition. Let $D \in \mathbb{Z}$ be squarefree with $D \neq 0, 1$. A *quadratic field* is $K = \mathbb{Q}(\sqrt{D})$.

Theorem 1.4. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{for } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{for } D \equiv 1 \pmod 4 \end{cases}$$

Definition. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Then we have

$$K = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

and we define the *norm* as the map

$$\begin{aligned} N : K &\to \mathbb{Q} \\ a + b\sqrt{D} &\mapsto a^2 - b^2 D. \end{aligned}$$

and the *trace* as the map

$$\begin{aligned} \mathrm{Tr} : K &\to \mathbb{Q} \\ a + b\sqrt{D} &\mapsto 2a. \end{aligned}$$

2. Algebraic integers and ideals

2.1 Trace and norm

Definition. Let $L \supset K$ be a field extension of finite degree n. Let $e = \{e_1, \ldots, e_n\}$ denote a basis of the K-vector space L and let $\alpha \in L$.
a) We denote by $M_e(\alpha)$ the *matrix of multiplication by* α defined as

$$M_e(\alpha) = (a_{ij})_{1 \le i,j \le n}$$

where

$$\alpha \cdot e_j = \sum_{i=1}^{n} a_{ij} e_i \text{ with } a_{ij} \in K.$$

b) We define the *norm* as

$$N_{L/K}(\alpha) = \det(M_e(\alpha)) \in K.$$

c) We define the *trace* as

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(M_e(\alpha)) \in K.$$

d) We define the *characteristic polynomial for* α *in* L/K as

$$c_{\alpha,L/K}(x) := \det(xI - M_e(\alpha)) \in K[x].$$

Remark. *Let* $\alpha \in L$ *and* $c_{\alpha,L/K}(x) = \sum_{i=0}^{n} c_i x^i$. *Then*
a) $c_n = 1$
b) $c_0 = c_{\alpha,L/K}(0) = (-1)^n N_{L/K}(\alpha)$
c) $c_{n-1} = -\mathrm{Tr}_{L/K}(\alpha)$

Exercise. *Prove that the trace and norm are independent of the choice of basis for* L.

Example. Let $L = \mathbb{Q}(\sqrt{D})$ for some squarefree $D \neq 0, 1$ and $K = \mathbb{Q}$. A basis for L is $e = \{1, \sqrt{D}\}$. For $\alpha = a + b\sqrt{D} \in L$ we compute

$$\alpha \cdot 1 = a + b\sqrt{D}$$
$$\alpha \cdot \sqrt{D} = bD + a\sqrt{D}.$$

Thus

$$M_e(\alpha) = \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$
$$N_{L/K}(\alpha) = a^2 - b^2 D = \alpha\alpha'$$
$$\mathrm{Tr}_{L/K}(\alpha) = 2a = \alpha + \alpha'$$
$$c_\alpha(x) = x^2 - x\,\mathrm{Tr}(\alpha) + N(\alpha)$$

where $\alpha' = a - b\sqrt{D}$. Also if $\alpha \notin \mathbb{Q}$, then c_α is the minimal polynomial for α.

Proposition 2.1. *Let $L \supset K$ be a field extension of finite degree n and $\alpha \in L$. Let $m(x)$ be the minimal polynomial for α over K and $c(x)$ the characteristic polynomial for α in L/K. Then*
a) $c(x) = m^d(x)$ *where* $d = [L : K(\alpha)]$
b) $c(\alpha) = 0$
c) $N_{L/K}(\alpha) = (-1)^n c_0 = (-1)^n m_0^d = (N_{K(\alpha)/K}(\alpha))^d$
d) $\mathrm{Tr}_{L/K}(\alpha) = -c_{n-1} = d\,\mathrm{Tr}_{K(\alpha)/K}(\alpha)$

Proof. Parts b)–d) all follow from a), so it suffices to prove part a).

CASE 1: Assume $L = K(\alpha)$ for some $\alpha \in L$, then $d = 1$. We choose the basis $e = \{1, \alpha, \ldots, \alpha^{n-1}\}$ and compute the elements of $M_e(\alpha)$. We have

$$\begin{aligned} \alpha e_i &= \alpha^i = e_{i+1} \qquad \text{for } i < n \\ \alpha e_n &= \alpha^n = -m_{n-1}\alpha^{n-1} - \cdots - m_1\alpha - m_0 \end{aligned}$$

Now we can compute $c(x)$ by taking the determinant of the matrix

$$B := xI - M_e(\alpha) = \begin{pmatrix} x & 0 & 0 & \ldots & m_0 \\ -1 & x & 0 & \ldots & m_1 \\ 0 & -1 & x & \ddots & m_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & -1 & x + m_{n-1} \end{pmatrix}$$

which yields $c(x) = m(x)$ (left as an exercise).

CASE 2: Now let $d > 1$ and $\{e_1, \ldots, e_d\}$ be a basis for $L/K(\alpha)$ and $\{1, \alpha, \ldots, \alpha^{\frac{n}{d}-1}\}$ be a basis for $K(\alpha)/K$. As an exercise, show that $\{e_j\alpha^i\}$ is a basis for L/K. Then

$$\alpha e_j \alpha^i = e_j \alpha^{i+1}, \text{ and so}$$

$$xI - M(\alpha) = \begin{pmatrix} B & & & \\ & B & & \\ & & \ddots & \\ & & & B \end{pmatrix}_{d \times d}$$

Taking the determinant yields

$$c(x) = (\det(B))^d = m^d(x). \qquad \square$$

Recall. Let K be a field and let α be a separable element over K and $m(x) := m_{\alpha,K}(x)$. Then a K-homomorphism

$$\varphi : \ K(\alpha) \to \overline{K}$$

is uniquely determined by $\varphi(\alpha)$. Moreover $\varphi(\alpha)$ is a conjugate of α, i.e., it is a root of $m(x)$.
The separability of α is equivalent to m having no multiple roots, which happens iff the number of maps φ is equal to # of distinct roots of m, which is $\deg m = [K(\alpha) : K]$. This happens iff

$$m(x) = \prod_{\varphi} (x - \varphi(\alpha))$$

Proposition 2.2. *Let L/K be a finite separable extension and $\alpha \in L$, $c := c_{\alpha,L/K}$. Then*
a) $c(x) = \prod(x - \varphi(\alpha))$
b) $N_{L/K}(\alpha) = \prod \varphi(\alpha)$
c) $\mathrm{Tr}_{L/K}(\alpha) = \sum \varphi(\alpha)$
where the products and sums above run over all K-homomorphisms

$$\varphi : L \to \overline{L} = \overline{K}.$$

Proof. a) The restriction $\varphi|_{K(\alpha)}$ is uniquely determined by $\varphi(\alpha)$, which is a conjugate of α. Conversely, for a conjugate β there exists exactly one K-homomorphism

$$\begin{aligned} \psi: \ K(\alpha) &\to \overline{L} \\ \alpha &\mapsto \beta \end{aligned}$$

By ÚKA, důsledek 2.10, ψ has exactly $d = [L : K(\alpha)]$ extensions φ. By Proposition 2.1

$$\begin{aligned} c(x) &= m^d(x) \\ &= \left(\prod_{\psi: K(\alpha) \to \overline{K}} (x - \psi(\alpha)) \right)^d \\ &= \prod_{\varphi: L \to \overline{K}} (x - \varphi(\alpha)). \end{aligned}$$

The rest follows from part a) and Proposition 2.1. □

Exercise. *Show that $N_{L/K}(\alpha) \in K$ for all $\alpha \in L$ directly using the formula from Proposition 2.2b).*

Corollary 2.3. *a) The norm as a map $N : L^\times \to K^\times$ is a homomorphism, i.e.,*

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \text{for all } \alpha, \beta \in L^\times$$

b) The trace as a map $\mathrm{Tr} : L \to K$ is a group homomorphism, i.e.,

$$\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta) \quad \text{for all } \alpha, \beta \in L$$

Exercise. *Let $M \supset L \supset K$ be separable extensions of finite degree. Show that*
a) $N_{M/K} = N_{L/K} \circ N_{M/L}$
b) $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$
c) For $\alpha \in K$

$$\begin{aligned} N_{L/K}(\alpha) &= \alpha^n \\ \mathrm{Tr}_{L/K}(\alpha) &= n\alpha, \ \text{where } n = [L : K] \end{aligned}$$

2.2 Discriminant

Given a separable extension L/K of finite degree and a tuple of elements from L, we would like to know whether this tuple is a suitable basis for the K-vector space L. The following notion of discriminant will help us in doing so.

Definition. Let L/K be a separable extension of degree n and $\alpha_1, \ldots, \alpha_n \in L$. We define the *discriminant* as

$$\Delta(\alpha_1, \ldots, \alpha_n) := \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{1 \le i,j \le n} \in K.$$

Lemma 2.4. *Let L/K be a separable extension of degree n and let $\varphi_1, \ldots, \varphi_n$ be all the K-homomorphisms $L \to \overline{L}$ and $\alpha_1, \ldots, \alpha_n \in L$. If we denote $M = (\varphi_i(\alpha_j))_{1 \le i,j \le n}$, then*

$$M^T M = \left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{1 \le i,j \le n}.$$

and

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(M))^2.$$

The proof is left as an exercise (use Proposition 2.2).

Proposition 2.5. *Let $L = K(\gamma)$ be a separable extension of degree n over K. Then*

$$\Delta(1, \gamma, \dots, \gamma^{n-1}) = \left(\prod_{i<j} (\varphi_i(\gamma) - \varphi_j(\gamma)) \right)^2 = (-1)^{\binom{n}{2}} N_{L/K}(m'(\gamma)),$$

where m is the minimal polynomial for γ and φ_i's are all the K-homomorphisms $L \to \overline{L}$. Further,

$$\Delta(1, \dots, \gamma^{n-1}) \neq 0.$$

Proof. We set

$$M := \begin{pmatrix} 1 = \varphi_1(1) & \varphi_1(\gamma) & \dots & \varphi_1(\gamma)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 = \varphi_n(1) & \varphi_n(\gamma) & \dots & \varphi_n(\gamma)^{n-1} \end{pmatrix}$$

This is the well-known Vandermonde matrix, whose determinant equals

$$\det(M) = \prod_{i>j} (\varphi_i(\gamma) - \varphi_j(\gamma)).$$

The first equality then follows from Lemma 2.4.
Let us now show the second equality.

$$\begin{aligned} m(x) &= \prod (x - \varphi_i(\gamma)) \\ m'(x) &= (x - \varphi_2(\gamma))(x - \varphi_3(\gamma)) \dots (x - \varphi_n(\gamma)) + \\ &\quad + (x - \varphi_1(\gamma))(x - \varphi_3(\gamma)) \dots (x - \varphi_n(\gamma)) + \dots \\ m'(\varphi_i(\gamma)) &= \prod_{j, j \neq i} (\varphi_i(\gamma) - \varphi_j(\gamma)). \end{aligned}$$

Now by Proposition 2.2

$$\begin{aligned} N_{L/K}(m'(\gamma)) = \prod_i \varphi_i(m'(\gamma)) = \prod_i m'(\varphi_i(\gamma)) = \\ = \prod_{i,j, i \neq j} (\varphi_i(\gamma) - \varphi_j(\gamma)) = \\ = (-1)^{\binom{n}{2}} \prod_{i<j} (\varphi_i(\gamma) - \varphi_j(\gamma))^2. \end{aligned}$$

For the last part, note that φ's are distinct homomorphisms, and so $\varphi_i(\gamma) \neq \varphi_j(\gamma)$ for all $i \neq j$. Thus $\Delta(1, \dots, \gamma^{n-1}) \neq 0$. □

Corollary 2.6. *Let L/K be a separable extension of degree n.*
a) The map

$$\begin{aligned} B: \ L \times L &\to K \\ (\alpha, \beta) &\mapsto \mathrm{Tr}(\alpha\beta) \end{aligned}$$

is a symmetric bilinear form, which is also non-degenerate, i.e., for all $x \neq 0$ there exists y such that $B(x, y) \neq 0$.
b) Let $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in L$, $\beta_j = \sum p_{ij} \alpha_i$, $P = (p_{ij}) \in K^{n \times n}$. Then

$$\Delta(\beta_1, \dots, \beta_n) = (\det P)^2 \Delta(\alpha_1, \dots, \alpha_n)$$

c) $\alpha_1, \dots, \alpha_n$ is a basis for L over K iff $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$.

Proof. a) Since separable extensions are simple, we find $\gamma \in L$ such that $K(\gamma) = L$ and then we can take the basis $1, \gamma, \ldots, \gamma^{n-1}$ for L/K. Then

$$\Delta(1, \gamma, \ldots, \gamma^{n-1}) = \det(\mathrm{Tr}(\gamma^i \gamma^j)),$$

which is not zero by Proposition 2.5. The rest follows from the fact that a bilinear form B is non-degenerate iff $\det(B(e_i, e_j)) \neq 0$ for some (equivalently, any) basis e_i (exercise).
b) If H is a matrix of bilinear form in basis $\alpha_1, \ldots, \alpha_n$, then $P^T H P$ is the matrix in the basis $\beta_1, \ldots, \beta_n$. Then

$$\begin{aligned} \Delta(\alpha_1, \ldots, \alpha_n) &= \det(H) \\ \Delta(\beta_1, \ldots, \beta_n) &= \det(P^T H P) = (\det P)^2 \det H. \end{aligned}$$

c) Take $\beta_i := \gamma^{i-1}$ as a basis for $K(\gamma)/K$ and $\Delta(1, \gamma, \ldots, \gamma^{n-1}) \neq 0$. Conversely, if $\alpha_1, \ldots, \alpha_n$ is not a basis, then the matrix P is singular, hence by part b) we have $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. □

Exercise. *For $K := \mathbb{F}_2(x)$ and $L := K(\sqrt{x})$ consider the extension L/K. Show that then*

$$\mathrm{Tr}_{L/K}(\alpha) = 0 \quad \textit{for all } \alpha \in L.$$

2.3 Integral basis

From this section onward, let K be a number field and denote $n := [K : \mathbb{Q}]$. We will also consider ideals $I < \mathcal{O}_K$ to be nonzero, but we allow $I = \mathcal{O}_K$.
We are quite familiar with bases for K over $\mathbb{Q}$ and how to find them. In this section, we will explore the notion of a basis for $\mathcal{O}_K$ over $\mathbb{Z}$.

Lemma 2.7. *a) For every $\alpha \in K$ there exists a nonzero $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_K$.*
b) For an ideal $I < \mathcal{O}_K$, we have $I \cap \mathbb{Z} \neq \{0\}$.
c) If $\alpha \in \mathcal{O}_K$, then $N(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$.
d) If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Proof. a) Let

$$a_d \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0, \quad d \leq n,\ a_i \in \mathbb{Z},\ a_d \neq 0.$$

Then multiplying by a_d^{d-1} yields

$$(a_d\alpha)^d + a_{d-1}(a_d\alpha)^{d-1} + \cdots + a_d^{d-1} a_0 = 0.$$

Hence $a_d\alpha \in \mathcal{O}_K$.
b) Choose $0 \neq \alpha \in I \subset \mathcal{O}_K$ and write the minimal polynomial for α

$$\begin{aligned} 0 &= \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0, \quad d \leq n,\ a_i \in \mathbb{Z},\ a_0 \neq 0. \quad \text{Then} \\ a_0 &= -\alpha^d - a_{d-1}\alpha^{d-1} - \cdots - a_1\alpha \in I. \end{aligned}$$

c) We prove the statement for the norm; for the trace the proof is analogous. We have $N(\alpha) \in \mathbb{Q}$. The conjugates $\varphi_i(\alpha)$ all lie in $\mathcal{O}_{\overline{\mathbb{Q}}}$ because they share the minimal polynomial with α. By Proposition 2.2 $N(\alpha) = \prod \varphi_i(\alpha)$, therefore $N(\alpha) \in \mathbb{Q} \cap \mathcal{O}_{\overline{\mathbb{Q}}} = \mathbb{Z}$.
For an alternative proof, note that by Proposition 2.1, the trace and norm are coefficients of the characteristic polynomial, which is a power of the minimal polynomial. Hence they must lie in $\mathbb{Z}$.
d) Follows from the definition of discriminant, as we know that $\mathrm{Tr}(\alpha_i\alpha_j) \in \mathbb{Z}$. □

Lemma 2.8. *Every ideal $I < \mathcal{O}_K$ contains some basis for $K/\mathbb{Q}$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $K/\mathbb{Q}$. By Lemma 2.7a) we can find nonzero $m \in \mathbb{Z}$ such that $m\alpha_i \in \mathcal{O}_K$ for all $1 \leq i \leq n$. By Lemma 2.7b) we can choose nonzero $a \in I \cap \mathbb{Z}$. Then $\{am\alpha_i \mid 1 \leq i \leq n\}$ is still a basis for $K/\mathbb{Q}$ and $am\alpha_i \in I$, which concludes the proof. □

So far we know that the discriminant of a basis for $\mathcal{O}_K$ is nonzero and that it lies in $\mathbb{Z}$. Proposition 2.5 might suggest that it is also always positive, but the following example contradicts this conjecture.

Example. Let $K = \mathbb{Q}(i)$. We then have a basis $\{1, i\} =: \{\alpha_1, \alpha_2\}$. Now we compute its discriminant with the use of Proposition 2.5 for φ_1 being the identity and φ_2 the complex conjugation map.

$$\Delta(\alpha_1, \alpha_2) = (i - \bar{i})^2$$
$$\Delta(\alpha_1, \alpha_2) = -4$$

Definition. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $K/\mathbb{Q}$. We call it an *integral basis for* $I < \mathcal{O}_K$ if

$$I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

The value of $\Delta(\alpha_1, \ldots, \alpha_n)$ does not depend on the choice of basis and is called the *discriminant of the ideal* I and denoted by $\Delta(I)$. The number $\Delta(\mathcal{O}_K)$ is called the *discriminant of the field* K and is often denoted by Δ_K.

Proposition 2.9. *Let $I < \mathcal{O}_K$ and let $\alpha_1, \ldots, \alpha_n \in I$ be a basis for $K/\mathbb{Q}$ with $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal. Then it is an integral basis for I.*

Proof. $|\Delta(\alpha_1, \ldots, \alpha_n)| \in \mathbb{Z}^+$, so considering the minimal value makes sense. Let

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n \in I, \quad \text{where } c_i \in \mathbb{Q}.$$

Assume for contradiction that $c_i \notin \mathbb{Z}$ for some i. WLOG $c_1 \notin \mathbb{Z}$ and let

$$c_1 = \lfloor c_1 \rfloor + \{c_1\} \qquad \lfloor c_1 \rfloor \in \mathbb{Z}.$$

Consider the basis

$$\beta_1 := \alpha - \lfloor c_1 \rfloor \alpha_1, \beta_2 := \alpha_2, \ldots, \beta_n := \alpha_n.$$

We have

$$\beta_1 = \{c_1\}\alpha_1 + \cdots + c_n\alpha_n = \alpha - \lfloor c_1 \rfloor \alpha_1$$

and the transition matrix

$$\begin{pmatrix} \{c_1\} & c_2 & c_3 & \ldots & c_n \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & & \\ & & & & 1 \end{pmatrix}$$

Taking the determinant yields $\det = \{c_1\} \neq 0$. We have

$$|\Delta(\beta_1, \ldots, \beta_n)| = \{c_1\}^2 |\Delta(\alpha_1, \ldots, \alpha_n)| < |\Delta(\alpha_1, \ldots, \alpha_n)|,$$

which contradicts minimality, hence all $c_i \in \mathbb{Z}$ and

$$I \subset \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

The converse inclusion follows trivially. □

Exercise. *Prove the Stickelberger theorem:*
For all number fields K,

$$\Delta_K \equiv 0 \text{ or } 1 \mod 4.$$

Example. Let us use these results to find the integral basis of quadratic number fields.
Let $D \in \mathbb{Z}$ be squarefree with $D \neq 0, 1$. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field and let us search for an integral basis of $\mathcal{O}_K$.
The first guess is $1, \sqrt{D} \in \mathcal{O}_K$.
Then

$$\Delta(1, \sqrt{D}) = \left(\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}\right)^2 = 4D.$$

As D is squarefree, by Corollary 2.6b), we see that $\Delta_K = D$ or $4D$.
When $D \equiv 2, 3 \pmod 4$, the discriminant cannot be D, as it would contradict Stickelberger's theorem. Thus the discriminant is $4D$ in this case, and $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$.
When $D \equiv 1 \pmod 4$, we are inspired to look for an integral element that might give $\Delta_K = D$, i.e., that would have $\det P = 1/2$ in Corollary 2.6b), i.e., whose expression in terms of $1, \sqrt{D}$ would involve dividing by 2. One of the first choices is $\frac{1+\sqrt{D}}{2}$ which indeed lies in $\mathcal{O}_K$; and then $1, \frac{1+\sqrt{D}}{2}$ give a basis with discriminant D. Hence $\Delta_K = D$ and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ in this case.

Proposition 2.10. *$\mathcal{O}_K/I$ is finite for all $I < \mathcal{O}_K$. In particular, $\#\mathcal{O}_K/(a) = a^n$ for each $a \in \mathbb{Z}^+$.*

Proof. Let $a \in \mathbb{Z}^+$ and let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$. Then

$$\left\{\sum_{i=1}^{n} c_i\omega_i : 0 \leq c_i < a\right\}$$

is a set of representatives for $\mathcal{O}_K/(a)$. Hence $\mathcal{O}_K/(a)$ is finite with a^n elements.
For $I < \mathcal{O}_K$, hoose $a \in I \cap \mathbb{Z}^+$. Since $(a) \subset I$, we have a surjection

$$\begin{aligned} \mathcal{O}_K/(a) &\twoheadrightarrow \mathcal{O}_K/I \\ \alpha + (a) &\mapsto \alpha + I. \end{aligned}$$

As $\mathcal{O}_K/(a)$ is finite, $\mathcal{O}_K/I$ must be also finite. □

Definition. Let R be a domain and F its field of fractions. We say that R is integrally closed if whenever $\alpha \in F$ is integral over R, then $\alpha \in R$.
We say that a domain R is Dedekind if
a) R is noetherian,
b) Each prime ideal $P < R$ is maximal,
c) R is integrally closed.

Corollary 2.11. *$\mathcal{O}_K$ is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is integrally closed by definition: if an element of K is integral over $\mathcal{O}_K$, then it is also integral over $\mathbb{Z}$, so it lies in $\mathcal{O}_K$.
By Proposition 2.9, every ideal $I < \mathcal{O}_K$ is finitely generated, therefore $\mathcal{O}_K$ is noetherian.
Let $P < \mathcal{O}_K$ be a prime ideal. Then $\mathcal{O}_K/P$ is a domain, which is finite by Proposition 2.10. Since each finite domain is a field (exercise), P is maximal. □

2.4 Ideal cancellation

In this section, K is again a number field of degree n over $\mathbb{Q}$.

Notation. For a subset A of a ring R and an element $\beta \in R$, we denote

$$\beta A = \{\beta a \mid a \in A\}.$$

If A is an ideal, then $\beta A = (\beta)A$, where (β) denotes the principal ideal generated by β.

Lemma 2.12. *a) Let $A < \mathcal{O}_K$ and $\beta \in K$ be such that $\beta A \subset A$. Then $\beta \in \mathcal{O}_K$.*
b) Let $A, B < \mathcal{O}_K$ be such that $A = AB$. Then $B = \mathcal{O}_K$.

Proof. Take an integral basis $\alpha_1, \ldots, \alpha_n$ for the ideal A.
a) Consider the following system of linear equations for which α_i are a nonzero solution.

$$\beta\alpha_i = \sum a_{ij}\alpha_j \quad a_{ij} \in \mathbb{Z}.$$

By linear algebra $\det M = 0$, where

$$M = \begin{pmatrix} \beta - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & \beta - a_{22} & \ldots & -a_{2n} \\ \vdots & & \ddots & \vdots \\ & & & \beta - a_{nn} \end{pmatrix}$$

The determinant of M is a monic polynomial in β with $\mathbb{Z}$-coefficients, i.e., $0 = \det M = \beta^n + \ldots$, hence $\beta \in \mathcal{O}_K$.
b) Analogously we consider the following system of linear equations

$$\alpha_i = \sum b_{ij}\alpha_j \quad b_{ij} \in B.$$

with the matrix

$$\begin{pmatrix} 1 - b_{11} & -b_{12} & \ldots & -b_{1n} \\ -b_{21} & 1 - b_{22} & \ldots & -b_{2n} \\ \vdots & & \ddots & \vdots \\ & & & 1 - b_{nn} \end{pmatrix}$$

whose determinant is again 0. We can also write

$$\det = 0 = 1 + \heartsuit$$

where each term in $\heartsuit$ contains some b_{ij}, hence $\heartsuit \in B$ and hence also $1 \in B \implies B = \mathcal{O}_K$. □

Exercise. *Lemma 2.12 does not hold in general. Find examples of rings for which it does not hold.*

Proposition 2.13. *Let $A, B < \mathcal{O}_K$ and $\omega \in \mathcal{O}_K$ be such that $(\omega)A = BA$. Then $(\omega) = B$.*

Proof. Take $\beta \in B$. We have

$$(\omega)A \supset (\beta)A \implies \frac{\beta}{\omega}A \subset A.$$

Apriori, $\frac{\beta}{\omega}$ lies in K, but it follows by Lemma 2.12a) that $\frac{\beta}{\omega} \in \mathcal{O}_K$.
Hence

$$\omega^{-1}B = \left\{ \frac{\beta}{\omega} \middle| \ \beta \in B \right\} \subset \mathcal{O}_K;$$

it clearly is an ideal. We now have $A = (\omega^{-1}B)A$. By Lemma 2.12b), $\omega^{-1}B = \mathcal{O}_K$ and hence $(\omega) = B$. □

2.5 Ideal classes

Fix a number field K of degree n over $\mathbb{Q}$.

Definition. Let $A, B < \mathcal{O}_K$. We say that A and B are equivalent and write $A \sim B$ if there exist $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ such that $(\alpha)A = (\beta)B$. Classes of this equivalence are called *ideal classes. The class number of* K is defined as the number of ideal classes and denoted by h_K.

Remark. $h_K = 1 \iff \mathcal{O}_K$ *is PID* $\iff \mathcal{O}_K$ *is UFD.*
While the first equivalence is fairly obvious, the second is not: prove it as an exercise! (See ÚKA, věta 4.18.)

Proposition 2.14. *There is* $M \in \mathbb{Z}^+$ *(that depends on* K*) such that for all* $\alpha, \beta \in \mathcal{O}_K, \beta \neq 0$*, there are* $t \in \mathbb{Z}, 1 \leq t \leq M$ *and elements* $\omega, \delta \in \mathcal{O}_K$ *such that*

$$t\alpha = \omega\beta + \delta, \quad |N\delta| < |N\beta|.$$

Proof. Let $\gamma = \frac{\alpha}{\beta} \in K$. It suffices to show that there exist t and ω such that

$$|N(t\gamma - \omega)| < 1.$$

Before proving the proposition, let us do some preparation.
Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$. By $\omega_i^{(j)}$ denote the conjugates of ω_i; more precisely, fix the $\mathbb{Q}$-embeddings $\varphi_i : K \to \overline{\mathbb{Q}}$ and let $\omega_i^{(j)} = \varphi_j(\omega_i)$.
For a general element $\gamma \in K$ we have

$$\gamma = \sum_i c_i\omega_i, \text{ and so}$$

$$|N\gamma| = \left|\prod_j \left(\sum_i c_i\omega_i^{(j)}\right)\right| \leq \prod_j \sum_i |c_i| \cdot |\omega_i^{(j)}| \leq$$

$$\leq C(\max|c_i|)^n,$$

where

$$C = \prod_j \sum_i |\omega_i^{(j)}|.$$

Take $m \in \mathbb{Z}, m > \sqrt[n]{C}$, and let $M := m^n$.
For the purposes of the rest of the proof, we define the "integral" and "fractional" part of γ as follows

$$\lfloor\gamma\rfloor := \sum_i \lfloor c_i \rfloor \omega_i \in \mathcal{O}_K$$

$$\{\gamma\} := \sum_i \{c_i\}\omega_i.$$

Now $\gamma = \lfloor\gamma\rfloor + \{\gamma\}$ and we can consider the injective map

$$\varphi : K \hookrightarrow \mathbb{R}^n$$

$$\sum c_i\omega_i \mapsto (c_1, \ldots, c_n).$$

Note that $\varphi(\{\gamma\}) \in [0, 1)^n$.

Let's now return to $\gamma = \frac{\alpha}{\beta} \in K$ for the rest of the proof.

We divide the unit cube $[0,1]^n$ into $m^n = M$ small cubes of side $\frac{1}{m}$ and consider the points $\varphi(\{k\gamma\})$ for $1 \leq k \leq M+1$. Then there exist two such points that lie in the same small cube, say for $k < \ell$. Let $0 < t := \ell - k \leq M$.
We then have that $t\gamma = \omega + \varepsilon$ for $\omega \in \mathcal{O}_K$ and $\varepsilon \in K$ such that all coordinates of $\varphi(\varepsilon)$ lie in $(-\frac{1}{m}, \frac{1}{m})$. Thus

$$|N\varepsilon| < C\left(\frac{1}{m}\right)^n < 1. \qquad \square$$

Theorem 2.15. *Class number h_K is finite.*

Proof. Let us divide the proof into three steps.

Step 1. We'll show that for each $A < \mathcal{O}_K$ there is an ideal $B < \mathcal{O}_K$ such that $A \sim B$ and $M! \in B$ (where M is the constant from Proposition 2.14).
Take the element $\beta \in A, \beta \neq 0$, such that $|N(\beta)|$ is minimal. For each $\alpha \in A$ there is $t, 1 \leq t \leq M$ such that

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

However, the minimality of $|N(\beta)|$ implies that $t\alpha - \omega\beta = 0$, i.e., $t\alpha = \omega\beta \in (\beta)$.
As $t \mid M!$, we have $M!\alpha \in (\beta)$. This holds for all $\alpha \in A$, and so we have $M!A \subset (\beta)$.
Now let $B := \frac{1}{\beta}M!A < \mathcal{O}_K$. We have $(M!)A = (\beta)B$ and thus $A \sim B$. Furthermore, we have $\beta \in A$, and so $M! = \frac{1}{\beta}M!\beta \in B$.

Step 2. Let's now show that there are only finitely many ideals $B < \mathcal{O}_K$ such that $M! \in B$.
These ideals are precisely those that satisfy $(M!) \subset B$, and these correspond to ideals in $\mathcal{O}_K/(M!)$ by the correspondence theorem (a corollary of the second isomorphism theorem).
But $\mathcal{O}_K/(M!)$ is finite by Proposition 2.10, and so it has only finitely many ideals. Thus there are also only finitely many ideals B.

Step 3. By Steps 1. and 2., each ideal A is equivalent to one of finitely many possible ideals B. Thus there are only finitely many ideal equivalence classes. $\square$

Corollary 2.16. *For each ideal $A < \mathcal{O}_K$ there is $k, 1 \leq k \leq h_K$, such that A^k is principal.*

Proof. Consider the set $\{A^i \mid 1 \leq i \leq h_K + 1\}$. At least two of the ideals in this set are equivalent. Let $A^i \sim A^j$ with $i < j$ and let $\alpha, \beta \in \mathcal{O}_K$ be such that $(\alpha)A^i = (\beta)A^j$. We set $k := j - i$ and $B := A^k$ and show that B is principal. We have

$$(\alpha)A^i = (\beta)BA^i \implies \left(\frac{\alpha}{\beta}\right)A^i = BA^i \subset A^i \overset{2.12}{\implies} \frac{\alpha}{\beta} \in \mathcal{O}_K.$$

By Proposition 2.13 $(\frac{\alpha}{\beta}) = B$ is principal. $\square$

Corollary 2.17 (Ideal classes form a group)**.** *For $A < \mathcal{O}_K$ we denote by $[A]$ its ideal class. We can equip the ideal classes with group structure as follows:*

We define the group operation as

$$[A] \cdot [B] = [AB]$$

with the unit element $[\mathcal{O}_K]$ and the inverse element

$$[A]^{-1} := [A^{k-1}]$$

where k is such that A^k is principal (such k exists by Corollary 2.16). The resulting group is denoted by $\mathcal{C}\ell_K$.

Exercise. *Verify that $\mathcal{C}\ell_K$ is indeed a finite abelian group.*

2.6 Cancellation and unique factorization

Recall that we're fixing a number field K of degree n over $\mathbb{Q}$, and that by an "ideal", $A < \mathcal{O}_K$, we always mean a nonzero ideal.

Proposition 2.18. *Let $A, B, C < \mathcal{O}_K$.*
a) If $AB = AC$, then $B = C$.
b) $B \supset A$ iff $B \mid A$.

Proof. a) By Corollary 2.16, there is k such that $A^k = (\alpha)$. Then we have $A^k B = A^k C$, and so $(\alpha)B = (\alpha)C$. This implies $B = C$.
b) We show the implication "$\Rightarrow$", the other one is trivial. Again, there is l such that $B^l = (\beta)$. Thanks to $B \supset A$, we have $C := \frac{1}{\beta} B^{l-1} A < \mathcal{O}_K$. Then $BC = A$, as we wanted. □

Theorem 2.19. *Each ideal in $\mathcal{O}_K$ has a unique factorization into a product of prime ideals (up to order of the factors).*

Note that the factorization is unique just up to order of factors. In factorizations into irreducibles, one also needs to consider "up to multiplication by unit", but that doesn't play a role here, as units don't change the corresponding prime ideal.

Proof. **Existence.** Let A be a proper ideal and let P_1 be a maximal ideal (which is prime by Corollary 2.11) containing A. By Proposition 2.18 P_1 divides A, therefore there exists an ideal $A_1 < \mathcal{O}_K$ such that $P_1 A_1 = A$. If $A_1 = \mathcal{O}_K$, then we are done. Otherwise A_1 is a proper ideal, so we can iterate this process, obtaining

$$A \subset A_1 \subset A_2 \subset \dots$$

Since $\mathcal{O}_K$ is noetherian, there exists i such that $A_i = \mathcal{O}_K$, leading to $A = P_1 P_2 \dots P_i$.

Uniqueness. Let $P_1 \dots P_k = Q_1 \dots Q_l$. Thus

$$P_1 \mid Q_1 \dots Q_l \implies P_1 \supset Q_1 \dots Q_l.$$

As P_1 is prime, it must contain one of the factors on the right hand side, WLOG $P_1 \supset Q_1$. Since both are prime ideals and hence maximal (by Corollary 2.11), we get $P_1 = Q_1$. We can then cancel them using Proposition 2.18a), obtaining $P_2 \dots P_k = Q_2 \dots Q_l$. Continuing like this, we arrive at the two factorizations being equal. □

Definition. Let $P < \mathcal{O}_K$ be a prime ideal and $A < \mathcal{O}_K$ an ideal. We denote by $\operatorname{ord}_P A = v_P A$ the unique $t \in \mathbb{Z}_{\geq 0}$ such that $P^t \mid A$ and $P^{t+1} \nmid A$.

Remark. *Here are some basic properties of* ord*:*
a) $\operatorname{ord}_P AB = \operatorname{ord}_P A + \operatorname{ord}_P B$,
b) $A = \prod P^{\operatorname{ord}_P A}$ *(which is only formally an infinite product).*

2.7 Ideal group

We have already introduced the notion of ideal class group. In this section we will introduce the notion of ideal group. The set $\{I < \mathcal{O}_K \mid I \neq \{0\}\}$ is a commutative semigroup (or monoid).

We can obtain a group by considering formal fractions AB^{-1} (ordered pairs of ideals with equivalence defined as $AB^{-1} = (AC)(BC)^{-1}$, which is well-defined thanks to the cancellation property). This group is denoted by $\mathcal{I}_K$ and is called the *ideal group* of the field K.

We can view the formal fractions as subsets of K by recalling that there always exists a $k \in \mathbb{Z}^+$ such that B^k is principal (by Corollary 2.16). Let $B^k = (\beta)$. Then we have

$$AB^{-1} = \frac{AB^{k-1}}{(\beta)} = \frac{1}{\beta} AB^{k-1} \subset K.$$

Sets of this form are called *fractional ideals*. Alternatively they can be defined as finitely generated $\mathcal{O}_K$-submodules in K. As an exercise, you can show that these are equivalent definitions.

For each $I < \mathcal{O}_K$, we have $I = I\mathcal{O}_K^{-1}$ and thus $I \in \mathcal{I}_K$. Thanks to the cancellation property it follows that $I\mathcal{O}_K^{-1} = J\mathcal{O}_K^{-1} \iff I = J$.

Definition. The set $\{(\alpha)(\beta)^{-1} \mid \alpha, \beta \in \mathcal{O}_K \setminus \{0\}\}$ denoted by $\mathcal{P}_K$ is called the *group of principal fractional ideals* of the field K.

Exercise. *Show that*

$$\mathcal{I}_K / \mathcal{P}_K = \mathcal{C}\ell_K.$$

3. Prime ideals

3.1 Prime factorizations

We will now focus on the prime ideals and what they look like in $\mathcal{O}_K$. We always fix a number field K of degree $n = [K : \mathbb{Q}]$.

Let $P < \mathcal{O}_K$ be a prime ideal. $P \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$ and by Lemma 2.7 we have $P \cap \mathbb{Z} \neq \{0\}$. Since $\mathbb{Z}$ is a PID, $P \cap \mathbb{Z} = a\mathbb{Z}$ for some $a \in \mathbb{Z}^+$. It's an easy exercise that in fact $a = p$ is a prime number. This then means that there exists a unique prime number p such that $p \in P$, i.e., $P \mid (p)$. We would now like to factor all such $(p) = p\mathcal{O}_K$.

Definition. Let $P < \mathcal{O}_K$ be a prime ideal and $p \in P$ a prime number. We define the *ramification index* of P as

$$e := e\left(P/p\right) := \mathrm{ord}_P(p).$$

We also define the *inertia degree* of P as $f \geq 1$ such that

$$\#\mathcal{O}_K/P = p^f$$

and denote it by f or $f\left(P/p\right)$. Note that the definition makes sense, as $\mathcal{O}_K/P$ is a finite field of characteristic p, and so its size is indeed p^f for some f.

Theorem 3.1 (efg theorem)**.** *Let $p \in \mathbb{Z}$ be a prime number, $P_1, \ldots, P_g < \mathcal{O}_K$ all prime ideals containing p. Let e_i, f_i be their ramification indices and inertia degrees, i.e., $p = P_1^{e_1} \cdots P_g^{e_g}$. Then*

$$\sum_{i=1}^{g} e_i f_i = n = [K : \mathbb{Q}].$$

Moreover if $K/\mathbb{Q}$ is a Galois extension, then $e_1, \ldots, e_g =: e, f_1, \ldots, f_g =: f$ and $efg = n$.

Note that the efg theorem works for general number field extensions L/K as well. However this weaker version is slightly less technical.

Definition. Let $p \in \mathbb{Z}$ be a prime number and P_i, e_i, f_i, g as in the efg theorem. We say that
a) p *splits completely* in K if $g = n, e_i = f_i = 1$ for all i, i.e.,

$$(p) = P_1 \ldots P_n.$$

b) p is *inert* in K if $g = 1, e_1 = 1, f_1 = n$, i.e.,

$$(p) = P.$$

c) p *ramifies* in K if there exists an index i such that $e_i \geq 2$.

Later on we will prove that only finitely many prime numbers ramify, and that they can be characterized.
We need a bit of preparation before proving efg Theorem 3.1.

Proposition 3.2. *Let $P < \mathcal{O}_K$ be a prime ideal of inertia degree f. Then*

$$\#\mathcal{O}_K/P^k = p^{kf} \quad \text{for all } k \in \mathbb{Z}^+.$$

Proof. We proceed by induction on k.

For $k = 1$ the statement follows from the definition of f.

Now let $k > 1$. Viewing $\mathcal{O}_K/P^k$ as an additive group, it has a subgroup P^{k-1}/P^k. By the 2nd isomorphism theorem,

$$(\mathcal{O}_K/P^k)/(P^{k-1}/P^k) \simeq \mathcal{O}_K/P^{k-1}.$$

By the inductive hypothesis, we have

$$\#\mathcal{O}_K/P^{k-1} = p^{(k-1)f}.$$

Thus it remains to show that

$$\#P^{k-1}/P^k = p^f.$$

Because factorization into prime ideals is unique, we have $P^{k-1} \neq P^k$, and so we can choose $\alpha \in P^{k-1} \setminus P^k$. Since $(\alpha)+P^k \supset P^k$, by Proposition 2.18b) we have $(\alpha)+P^k \mid P^k$. By unique factorization (Theorem 2.19), P is the only prime dividing P^k, so $(\alpha) + P^k = P^l$ for some $l \leq k$. On the other hand, $\alpha \in P^{k-1}$ gives $P^{k-1} \supset (\alpha) + P^k = P^l$, hence $l \geq k-1$. Since $\alpha \notin P^k$, we must have $l = k-1$, i.e., $(\alpha) + P^k = P^{k-1}$.
Consider now the surjection

$$\begin{aligned} \varphi : \ \mathcal{O}_K &\twoheadrightarrow P^{k-1}/P^k \\ \gamma &\mapsto \gamma\alpha + P^k \end{aligned}$$

which is a group homomorphism. Let us determine its kernel:

$$\begin{aligned} &\gamma \in \operatorname{Ker}\varphi \iff \gamma\alpha \in P^k \iff \operatorname{ord}_P(\gamma\alpha) \geq k \iff \\ &k \leq \operatorname{ord}_P(\gamma\alpha) = \operatorname{ord}_P(\gamma) + \operatorname{ord}_P(\alpha) = \operatorname{ord}_P(\gamma) + k - 1. \end{aligned}$$

We have thus obtained

$$\gamma \in \operatorname{Ker}\varphi \iff \operatorname{ord}_P(\gamma) \geq 1 \iff \gamma \in P.$$

Hence $\operatorname{Ker}\varphi = P$. By the 1st isomorphism theorem,

$$\mathcal{O}_K/P \simeq P^{k-1}/P^k,$$

which concludes the proof. □

Recall. Recall the Chinese remainder theorem (CRT for short) whose proof can be found in ÚKA, tvrzení 1.21.

Let R be a (commutative) ring and $A_1, \ldots, A_g < R$ pairwise comaximal ideals, i.e., $A_i + A_j = R$ for all $i \neq j$. Then

$$\begin{aligned} R/A_1 \ldots A_g &\simeq R/A_1 \times \cdots \times R/A_g \quad \text{and} \\ A_1 \ldots A_g &= A_1 \cap \cdots \cap A_g. \end{aligned}$$

Proof of Theorem 3.1. Let $(p) = P_1^{e_1} \cdots P_g^{e_g}$. As an exercise, show that $P_i^{e_i}$ are pairwise comaximal. Then by CRT,

$$\mathcal{O}_K/(p) \simeq \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_g^{e_g}.$$

By Proposition 2.10, the size of LHS is

$$\#\mathcal{O}_K/(p) = p^n.$$

By Proposition 3.2 we have

$$\#RHS = \prod p^{e_i f_i} = p^{\sum e_i f_i}.$$

From the isomorphism it now follows that $n = \sum e_i f_i$.
It remains to prove the "Moreover" part, which will follow from Proposition 3.3 below. □

Definition. Let $K/\mathbb{Q}$ be a Galois extension, $A < \mathcal{O}_K$ an ideal and $\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$. Then we define

$$\sigma A := \{\sigma(\alpha) \mid \alpha \in A\} < \mathcal{O}_K.$$

Remark. *Note that the following holds:*
a) $\sigma\mathcal{O}_K = \mathcal{O}_K \implies \mathcal{O}_K/\sigma A = \sigma\mathcal{O}_K/\sigma A \simeq \mathcal{O}_K/A$.
b) For a prime ideal P, σP *is also a prime ideal.*

Proposition 3.3. *Let* $p \in \mathbb{Z}$ *be a prime number and* $P, Q < \mathcal{O}_K$ *prime ideals dividing* (p). *If* $K/\mathbb{Q}$ *is Galois, then there exists* $\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ *such that* $\sigma P = Q$; *in other words, the Galois group acts transitively on* $\{P_1, \ldots, P_g\}$.

Proof. For the purpose of this proof, let us denote $G := \mathrm{Gal}\left(K/\mathbb{Q}\right)$. Assume towards contradiction that $Q \notin \{\sigma P \mid \sigma \in G\}$. By CRT there exists $\alpha \in \mathcal{O}_K$ such that

$$\begin{aligned} \alpha &\equiv 0 \mod Q \\ \alpha &\equiv 1 \mod \sigma P \quad \text{for all } \sigma \in G. \end{aligned}$$

Now we have

$$N(\alpha) = \prod \sigma\alpha \in Q \cap \mathbb{Z} = (p).$$

Then

$$P \mid (p) \mid (N(\alpha)) = \prod(\sigma\alpha) \implies P \mid (\sigma\alpha)$$

for some σ. Thus $\sigma\alpha \in P$, which contradicts $\alpha \equiv 1 \mod \sigma^{-1}P$. □

Proof of Theorem 3.1, *"Moreover".* For each i there is some $\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ such that $\sigma P_1 = P_i$. Then

$$\mathcal{O}_K/P_1 \simeq \mathcal{O}_K/\sigma P_1 = \mathcal{O}_K/P_i,$$

and so $f_1 = f_i$.
Let us now apply σ to $(p) = P_1^{e_1} \cdots P_g^{e_g}$.
We have $p \in \mathbb{Z}$, and so $\sigma(p) = (p)$. Thus $(p) = (\sigma P_1)^{e_1} \cdots (\sigma P_g)^{e_g}$.
Here $\sigma P_1 = P_i$ occurs with exponent e_1, whereas in $(p) = P_1^{e_1} \cdots P_g^{e_g}$, it has exponent e_i. By unique factorization, we must have $e_1 = e_i$. □

3.2 Finding factors

How can we explicitly find the prime ideals dividing a given rational prime p?

Theorem 3.4 (Dedekind criterion)**.** *Let K be a number field such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α. Let $f \in \mathbb{Z}[x]$ denote the minimal polynomial for α and let p be a prime number.*
For $g \in \mathbb{Z}[x]$ we shall denote $\bar{g} \in \mathbb{F}_p[x]$ its reduction modulo p.
We let

$$\bar{f}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{e_i}$$

be the factorization into irreducibles over $\mathbb{F}_p$, where g_i are some fixed monic polynomials in $\mathbb{Z}[x]$. Then

$$p\mathcal{O}_K = \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i}$$

is the distinct prime ideal factorization.
Moreover

$$\mathcal{O}_K/(p, g_i(\alpha)) \simeq \mathbb{F}_p[x]/\bar{g}_i,$$

and so the inertia degree of $(p, g_i(\alpha))$ is $f_i = \deg g_i$.

The assumption $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α is strong and doesn't have to hold! However, in general the theorem holds for all primes p that do not divide the index $(\mathcal{O}_K : \mathbb{Z}[\alpha])$ (as a subgroup), with essentially the same proof – try it as an exercise.
For example, this can then be applied to determining the behavior of odd primes p in a quadratic field $\mathbb{Q}(\sqrt{D})$ using the polynomial $f(x) = x^2 - D$, even in the case $D \equiv 1 \pmod 4$.

Proof. Consider the isomorphism

$$\begin{aligned} \mathbb{Z}[x]/(f(x)) &\simeq \mathcal{O}_K = \mathbb{Z}[\alpha] \\ x + (f(x)) &\mapsto \alpha. \end{aligned}$$

Factoring mod p gives us

$$\begin{aligned} \mathbb{F}_p[x]/(\bar{f}(x)) &\simeq \mathcal{O}_K/(p) \\ x + (\bar{f}(x)) &\mapsto \alpha + (p). \end{aligned}$$

Now $\mathbb{F}_p[x]/(\bar{f})$ has maximal ideals $(\bar{g}_i) := (\bar{g}_i + (\bar{f}))$ for $i \in \{1, \ldots, r\}$. Now we have

$$\prod (\bar{g}_i)^{e_i} = 0 \equiv \bar{f}$$

and let us show that no smaller e_i's give 0.
The ideal $(\bar{g}_i)$ corresponds to $(g_i(\alpha) + (p)) < \mathcal{O}_K/(p)$ and this by the 2nd isomorphism theorem corresponds to $P_i := (p, g_i(\alpha)) < \mathcal{O}_K$. These P_i are all the prime ideals in $\mathcal{O}_K$ such that they contain (p). If we have

$$p\mathcal{O}_K = \prod P_i^{e_i'},$$

then the e_i' are characterized by the property

$$p\mathcal{O}_K \supset \prod P_i^{e_i'},$$

but they do not contain any product with smaller exponents. Under the correspondence, it corresponds to $\prod (\bar{g}_i)^{e_i}$, hence $e_i = e_i'$, which concludes the proof. □

Example. Consider the number field $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $f = x^2 + 5$ is the minimal polynomial for $\sqrt{-5}$.
For $p = 2$ we have

$$x^2 + 5 \equiv (x+1)^2 \mod 2$$
$$r = 1 \quad g_1 = x + 1 \in \mathbb{Z}[x] \quad e_1 = 2$$
$$2\mathcal{O}_K = (2) = (2, \sqrt{-5} + 1)^2 \implies 2 \text{ ramifies}$$

For $p = 3$ we have

$$x^2 + 5 \equiv (x+1)(x-1) \mod 3$$
$$3\mathcal{O}_K = (3) = (3, \sqrt{-5} + 1)(3, \sqrt{-5} - 1) \implies 3 \text{ splits completely}$$

For $p = 11$, $x^2 + 5$ is irreducible mod 11

$$11\mathcal{O}_K = (11) = (11, (\sqrt{-5})^2 + 5) = (11) \implies 11 \text{ is inert.}$$

Exercise. *a) In the example above, characterize the behavior of all p. (Hint: Try using Legendre symbols)*
b) Characterize the behavior of all p for general number field $\mathbb{Q}(\sqrt{D})$.
c) Use Theorem 3.4 *(when it applies) to verify Theorem* 3.1.

3.3 Ramification

Theorem 3.5. *Let p be a prime number. Then p ramifies in K if and only if* $p \mid \Delta_K$.

In order to prove this theorem, we first need to introduce a generalization of the discriminant.
We assume $A \subset B$ to be rings such that B is a free A-module of rank m, i.e.,

$$B \simeq A^m$$

as an A-module. Now for an element $\beta \in B$ we can define the map

$$B \to B$$
$$x \mapsto \beta x$$

which can be viewed as a linear map $A^m \to A^m$. We can then define $\mathrm{Tr}_{B/A}\,\beta$ as the trace of this linear map. More concretely, for an A-basis $e_1, \ldots, e_m \in B$ we have

$$\beta e_j = \sum a_{ij} e_i \quad \text{and}$$
$$\mathrm{Tr}_{B/A}\,\beta = \sum a_{ii} \in A.$$

Now given some $\beta_1, \ldots, \beta_m \in B$ we define

$$\Delta(\beta_1, \ldots, \beta_m) := \det(\mathrm{Tr}_{B/A}(\beta_i \beta_j)) \in A$$
$$\Delta(B/A) := (\Delta(e_1, \ldots, e_m)) < A.$$

We leave the proof of the following lemma as an exercise.

Lemma 3.6. *Let $B \supset A$ be rings such that B is a free A-module with a basis $e_1, \dots, e_m$. Let $I < A$ be an ideal.*
a) Then

$$\bar{e}_i := e_i + IB, \quad i \in \{1, \dots, m\}$$

is a basis for ${}^{B}/_{IB}$ as an ${}^{A}/_{I}$-module.
b)

$$\Delta(\bar{e}_i, \dots, \bar{e}_m) \equiv \Delta(e_1, \dots, e_m) \mod I.$$

c) If $B_i \supset A$ are rings that are free A-modules of finite ranks, then

$$\Delta\left(\Pi B_i/A\right) = \prod \Delta\left(B_i/A\right)$$

Definition. Let R be a ring and $\alpha \in R$. We say that α is *nilpotent* if $\alpha^r = 0$ for some $r \geq 1$.

Proof of Theorem 3.5. Let $p = P_1^{e_1} \cdots P_g^{e_g}$. By CRT we have

$$\mathcal{O}_K/(p) \simeq \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_g^{e_g}.$$

Let us now observe the following.

Lemma 3.7. *$\mathcal{O}_K/P_i^{e_i}$ contains a nonzero nilpotent element iff $e_i \geq 2$.*

Proof of Lemma 3.7. If $e_i = 1$, then P_i is a maximal ideal, so $\mathcal{O}_K/P_i$ is a field and hence does not contain any nonzero nilpotent elements.
Now if $e_i \geq 2$, then $\alpha \in P_i \setminus P_i^{e_i}$ is nilpotent. □

Now from Lemma 3.7 it follows that

$$\mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_g^{e_g}$$

contains a nonzero nilpotent element iff $e_i \geq 2$ for some i. In other words, it is sufficient for one of the factor rings to contain a nilpotent element.
Thanks to Lemma 3.6 we have

$$\begin{aligned}\Delta_K &= \Delta(\mathcal{O}_K/\mathbb{Z}) \\ &\equiv \Delta\left(\left(\mathcal{O}_K/(p)\right)/\mathbb{F}_p\right) \mod p \\ &= \prod \Delta\left(\left(\mathcal{O}_K/P_i^{e_i}\right)/\mathbb{F}_p\right) \mod p.\end{aligned}$$

If $e_i = 1$, then $\mathcal{O}_K/P_i$ is a field and $\left(\mathcal{O}_K/P_i\right)/\mathbb{F}_p$ is a separable field extension by ÚKA, důsledek 2.18, hence by Corollary 2.6c) we have

$$\Delta\left(\left(\mathcal{O}_K/P_i\right)/\mathbb{F}_p\right) \neq 0.$$

If all $e_i = 1$, then

$$\prod \Delta\left(\left(\mathcal{O}_K/P_i^{e_i}\right)/\mathbb{F}_p\right) \not\equiv 0 \mod p, \quad \text{and so} \quad p \nmid \Delta_K.$$

If $e_i \geq 2$ for some i, then $\mathcal{O}_K/(p)$ has a nilpotent element $\beta \neq 0$. We choose an $\mathbb{F}_p$-basis for $\mathcal{O}_K/(p)$

$$b_1 = \beta, b_2, \dots, b_f.$$

One can check that $\mathrm{Tr}(\beta b_i) = 0$ for all i, hence

$$\Delta\left(\left(\mathcal{O}_K/(p)\right)/\mathbb{F}_p\right) = \det(\mathrm{Tr}(b_i b_j)) = 0 \text{ in } \mathbb{F}_p.$$

Thus $p \mid \Delta_K$. □

4. Geometry of numbers

We continue with the setting that K is a number field of degree n over $\mathbb{Q}$. Recall that ideals are always assumed to be nonzero.

4.1 Ideal norm

Definition. For an ideal $I < \mathcal{O}_K$, we define its (*numerical*) *norm* as

$$\mathcal{N}I = \#\mathcal{O}_K/I.$$

One can also define $\mathcal{N}(0) = 0$.

Note that by Proposition 2.10, the norm $\mathcal{N}I$ is always finite and lies in $\mathbb{Z}^+$. Further,

$$\mathcal{N}(a\mathcal{O}_K) = |a|^n \quad \text{for all} \quad a \in \mathbb{Z}.$$

Note that $\mathcal{N}I = 0$ in the factor-ring $\mathcal{O}_K/I$, and so $I \mid \mathcal{N}I$.
We also have $\mathcal{N}I = 1$ iff $I = \mathcal{O}_K$.
Note that in ÚKA, sekce 4.6, we have defined the norm of an ideal in a quadratic number field as $g \in \mathbb{Z}^+$ such that $(g) = II'$, where I' is a conjugate ideal. In Proposition 4.2 below we will see that our new definition is more general.

Proposition 4.1. *a) Let $P < \mathcal{O}_K$ be a prime ideal and p the prime number contained in P. Then*

$$\mathcal{N}P = p^{f\left(P/(p)\right)}.$$

b) Let $I = \prod P_i^{r_i}$ for P_i prime ideals and $r_i \geq 1$. Then

$$\mathcal{N}I = \prod p_i^{f_i r_i},$$

where p_i is a prime number contained in P_i.
c) $\mathcal{N}(IJ) = \mathcal{N}(I) \cdot \mathcal{N}(J)$.
d) If $I \supset J$, then

$$\#I/J = \mathcal{N}(J)/\mathcal{N}(I) = \mathcal{N}(I^{-1}J).$$

Proof. a) This is the definition of the inertia degree f.
b) By CRT we have

$$\mathcal{O}_K/I \simeq \mathcal{O}_K/P_1^{r_1} \times \cdots \times \mathcal{O}_K/P_m^{r_m}.$$

By Proposition 3.2

$$\#\mathcal{O}_K/P_i^{r_i} = p_i^{r_i f_i},$$

which implies part b).
c) Factor I, J into prime ideals and use part b).

d) By 2nd isomorphism theorem

$$\begin{aligned}\big(\mathcal{O}_K/J\big)/\big(I/J\big) &\simeq \mathcal{O}_K/I, \quad \text{and so}\\ \#\mathcal{O}_K/J &= \#I/J \cdot \#\mathcal{O}_K/I. \quad \text{Thus}\\ \#I/J &= \mathcal{N}J/\mathcal{N}I = \mathcal{N}(I^{-1}J),\end{aligned}$$

where the last equality holds by part c). (Note that $I \mid J$, and so $I^{-1}J < \mathcal{O}_K$). □

Recall that for $\alpha \in \mathcal{O}_K$, we write $\alpha\mathcal{O}_K$ for the principal ideal (α); in particular $p\mathcal{O}_K = (p)$.

Proposition 4.2. *Assume that $K/\mathbb{Q}$ is Galois.*
a) Given a prime number p and prime ideal $P < \mathcal{O}_K$ such that $P \mid (p)$, let

$$p\mathcal{O}_K = (P_1 \dots P_g)^e.$$

Then

$$\mathcal{N}(P) \cdot \mathcal{O}_K \overset{(1)}{=} (P_1 \dots P_g)^{ef} \overset{(2)}{=} \prod_{\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)} \sigma P.$$

b) For each $I < \mathcal{O}_K$ we have

$$\mathcal{N}(I) \cdot \mathcal{O}_K = \prod_{\sigma \in \mathrm{Gal}\left(K/\mathbb{Q}\right)} \sigma I.$$

Proof. a) Since $\mathcal{N}P = p^f$, we have the equality of ideals

$$\mathcal{N}(P) \cdot \mathcal{O}_K = (p^f) = (p)^f = (P_1 \dots P_g)^{ef},$$

which shows the equation (1).
By Proposition 3.3 the Galois group $G := \mathrm{Gal}\left(K/\mathbb{Q}\right)$ acts transitively on $\{P_1, \dots, P_g\}$ and therefore the action has only one orbit of size g. This means that for all i the stabilizer

$$G_{P_i} = \{\sigma \in G \mid \sigma P_i = P_i\}$$

has size equal to

$$\frac{\#G}{\#\{\text{orbit of } P_i\}} = \frac{n}{g} \overset{3.1}{=} ef.$$

Thus (2) holds.
b) follows immediately from a) by consider the prime ideal factorization of I. □

Finally, we have the following result comparing the norm of an element with the ideal norm, that we'll prove a bit later.

Proposition 4.3. *For each $\beta \in \mathcal{O}_K$, we have $|N(\beta)| = \mathcal{N}(\beta\mathcal{O}_K)$.*

This proposition implies that the following diagram commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\beta \mapsto (\beta)} & \mathcal{I}_K \\ \Big\downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \Big\downarrow{\scriptstyle \mathcal{N}:\ \frac{I}{J} \mapsto \frac{\mathcal{N}I}{\mathcal{N}J}} \\ \mathbb{Q}^\times & \xrightarrow{|\cdot|} & \mathbb{Q}^+ (\simeq \mathcal{I}_\mathbb{Q}) \end{array}$$

4.2 Minkowski bound

One of the main goals of this chapter is the proof of the following key theorem. We'll prove it later, but let's start by formulating it and discussing some of its corollaries. However, first we need to discuss complex embeddings that play a role in the formulation of the theorem.

Complex embeddings.
Number field K is a finite extension of $\mathbb{Q}$, and so $\overline{K} = \overline{\mathbb{Q}}$. Moreover, it is natural to consider $\overline{\mathbb{Q}}$ as a subfield (consisting of all algebraic elements) of the algebraically closed field $\mathbb{C}$ (see ÚKA, tvrzení 2.8).
Further, $\mathbb{Q}$-homomorphisms of K into $\overline{\mathbb{Q}}$ are exactly the same as $\mathbb{Q}$-homomorphisms of K into $\mathbb{C}$ (as the image of K must consist of algebraic elements). Therefore it is more common to talk about embeddings of K into $\mathbb{C}$ (and we will do so from now on).
If we choose a primitive element $\alpha \in K$ (i.e., $K = \mathbb{Q}(\alpha)$), then an embedding $\sigma : K \hookrightarrow \mathbb{C}$ is uniquely determined by $\sigma(\alpha)$, which must be a root of the minimal polynomial m for α over $\mathbb{Q}$.
Some of these roots are real, corresponding to embeddings $\sigma : K \hookrightarrow \mathbb{R} \subset \mathbb{C}$. It's common to denote the number of real embeddings by r.
Some roots lie in $\mathbb{C} \setminus \mathbb{R}$, and these roots form pairs $\alpha, \overline{\alpha}$ (where $\overline{\alpha}$ denotes the complex conjugate). These correspond to pairs of conjugate embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$, and we denote their number by $2s$.
Finally, note that the $n = [K : \mathbb{Q}] = \deg m$ equals the total number of roots of m, and so $n = r + 2s$.

Theorem 4.4 (Minkowski bound)**.** *Let K be a number field of degree n and let $2s$ denote the number of embeddings $K \hookrightarrow \mathbb{C}$, whose image does not lie in $\mathbb{R}$. Then there exists a set of representatives for the class group $\mathcal{C}\ell_K$ consisting of ideals $I < \mathcal{O}_K$ such that*

$$\mathcal{N}I \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}.$$

Remark. *The term $\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s$ is called the Minkowski constant. The whole RHS is called the Minkowski bound and is often denoted B_K.*

Example. For $K := \mathbb{Q}(i)$ and an ideal $I < \mathcal{O}_K$, we can compute the Minkowski bound

$$\mathcal{N}(I) \leq B_K = 1.27\ldots,$$

hence $I = \mathcal{O}_K$ for all representatives of the ideal class group. Therefore the class group $\mathcal{C}\ell_K$ has only one element, and so $\mathcal{O}_K = \mathbb{Z}[i]$ is a PID.

Corollary 4.5. *There is no unramified field extension $K/\mathbb{Q}$, i.e., for each number field K there exists a prime number p that ramifies in K.*

Proof. Since $h_K \geq 1$ for each K, there exists an ideal $I < \mathcal{O}_K$ from Theorem 4.4 such that

$$1 \leq \mathcal{N}I \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}.$$

After rearranging we obtain

$$|\Delta_K|^{\frac{1}{2}} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s > 1,$$

where the last inequality is an analysis exercise.
Thus $|\Delta_K| \geq 2$, and so there exists a prime number p such that $p \mid \Delta_K$, which ramifies by Theorem 3.5. □

One can also talk about ramification for general extensions of number fields L/K, in which case it can happen that every prime ideal of K is unramified in L. The keyword (with fairly magical properties) is Hilbert class field.
Minkowski bound also implies an alternative proof of Theorem 2.15. However, this is circular reasoning given our proof of Theorem 2.15, as the finiteness of the class number was used in its proof. Nevertheless, the bound implied by Corollary 4.6 is better than the bound from Theorem 2.15.

Corollary 4.6. *Class number h_K is finite.*

Proof. Take an ideal $I < \mathcal{O}_K$ that satisfies Minkowski bound, and factor it into prime ideals

$$I = \prod P_i^{r_i} \implies B_K \geq \mathcal{N}I = \prod (\mathcal{N}P_i)^{r_i} \implies 2 \leq \mathcal{N}P_i \leq B_K \text{ and } r_i \leq \log_2 B_K.$$

Thus there are only finitely many candidates for P_i, and finitely many possibilities for r_i. Hence there are only finitely many possible representatives I, and so h_K is finite. □

Finding the class group $\mathcal{C}\ell_K$.
Minkowski bound also gives an algorithm for determining $\mathcal{C}\ell_K$. Let's briefly discuss it.

a) Find $S = \{I < \mathcal{O}_K \mid \mathcal{N}I \leq B_K\}$.
b) For $I, J \in S$, test whether $I \sim J$, i.e., whether IJ^{-1} is principal.
c) Find relations $[IJ] = [H]$ and $[I^{-1}] = [J]$.

Let us describe how to carry out step b). There exists $H < \mathcal{O}_K$ such that $JH = (\mathcal{N}J)$, and then

$$IJ^{-1} = \frac{IH}{JH} = \frac{IH}{(\mathcal{N}J)}.$$

It now suffices to check whether $IH = (\mathcal{N}J)(\alpha) =: (\beta)$ for some $\alpha \in \mathcal{O}_K$, as then IJ^{-1} is principal. We have

$$\mathcal{N}(IH) = \mathcal{N}(\beta) \overset{4.3}{=} |N\beta|,$$

which leads to a diophantine equation.

Example. Consider the case $K := \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and consider the ideal

$$(3) = (3, \sqrt{-5} - 1)(3, \sqrt{-5} + 1).$$

Does there exist α such that

$$N\alpha = \mathcal{N}(3, \sqrt{-5} - 1) = 3?$$

Rewriting $N\alpha$ as $a^2 + 5b^2$ yields the diophantine equation

$$a^2 + 5b^2 = 3,$$

which clearly has no solutions, hence the ideal $(3, \sqrt{-5} - 1)$ is not principal in $\mathcal{O}_K$.

4.3 Lattices

Definition. Let V be a real vector space of dimension $n < \infty$. A *lattice* Λ in V is a subgroup

$$\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_r,$$

where e_i are linearly independent over $\mathbb{R}$.
A lattice is *full* if $r = n$.

Example. $\mathbb{Z}[i] \subset \mathbb{C}$ is a lattice with basis $1, i$. This lattice can be identified with the lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$.
On the other hand, consider $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} \cdot 1 + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$. Since 1 and $\sqrt{2}$ are not linearly independent over $\mathbb{R}$, $\mathbb{Z}[\sqrt{2}]$ is not a lattice in $\mathbb{R}$.

Lemma 4.7. *Let V be a finite-dimensional real vector space and $\Lambda < V$ an additive subgroup. Then Λ is a lattice iff it is discrete, i.e., for every $\lambda \in \Lambda$ there exists an open set $U \subset V$ such that $U \cap \Lambda = \{\lambda\}$.*

Proof. The proof is left as an exercise. □

Definition. Let $\Lambda = \sum \mathbb{Z}e_i$ be a full lattice. We call the set

$$D := \left\{ \sum a_i e_i \;\middle|\; 0 \leq a_i < 1 \right\}$$

a *fundamental parallelepiped* for Λ.

Definition. By *volume* we shall mean the usual measure on $V \simeq \mathbb{R}^n$ and denote it by Vol.
Let Λ be a lattice with a fundamental parallelepiped D. The *covolume* of Λ is the volume $\operatorname{Vol} D$.

Lemma 4.8. *Let $\Lambda = \sum \mathbb{Z}e_i$ be a full lattice with fundamental parallelepiped D. Then:*
a)

$$V = \bigsqcup_{\lambda \in \Lambda} (\lambda + D)$$

(where $\bigsqcup$ denotes the disjoint union).
b) For every $v \in V$ there exists a unique $\lambda \in \Lambda$ such that $v - \lambda \in D$. In other words D is a fundamental domain for the action of shifting by Λ.
c)

$$\operatorname{Vol}(D) = |\det(e_1, \ldots, e_n)|.$$

d) The volume of D is preserved under a change of basis.

Based on part b) of the lemma, we shall use the terms "fundamental domain" and "fundamental parallelepiped" interchangeably.

Proof. a), b) are trivial, and we know c) from linear algebra.
d) Changing the basis results in multiplying $\operatorname{Vol}(D)$ by the determinant of the transition matrix, which is 1. □

Further, we want to relate the covolumes of a lattice and its sublattice. For that we shall use the following well-known result (also called *Structure theorem for subgroups of free abelian groups of finite rank*).

Theorem 4.9 (Invariant factor theorem)**.** *Consider full lattices $\Lambda' \subset \Lambda \subset V$. There exists a basis $e_1, \ldots, e_n$ for Λ and positive integers $m_1 \mid m_2 \mid \cdots \mid m_n$ such that $m_i e_i$ is a basis for Λ'.*

Proof. Let us start with arbitrary bases $e_1, \ldots, e_n$ for Λ and $f_1, \ldots, f_n$ for Λ'. As each f_i also lies in Λ, we can express them as $\mathbb{Z}$-linear combinations of $e_1, \ldots, e_n$ and consider the corresponding matrix (i.e., the transition matrix from $e_1, \ldots, e_n$ to $f_1, \ldots, f_n$).
With this matrix, we can do the following operations: We can do usual row and column operations (adding or subtracting a multiple of a given row/column from another row/column), and we can also permute the rows (or columns), as this corresponds to renumbering the basis elements. Note that these after any sequence of these operations, we still have two bases for V, and so the corresponding transition matrix is regular. In particular, it can't contain a row or column that would be identically 0.

We will do the following iterative algorithm:

(1) Choose the element a in the matrix with the smallest nonzero absolute value, and place it in the position $(1,1)$.
(2) By row and column operations, reduce all the elements in the 1st row and column modulo $|a|$.
(3) Repeat steps (1) and (2) until the 1st row and column contain only the element a_{11}, and all other elements are 0. (This process terminates, for the absolute values $|a|$ in step (1) form a decreasing sequence of positive integers.)
(4) Next we want to make sure that the element a_{11} divides all the elements of the matrix (which need not be the case after (3)). If not, then assume that $a_{11} \nmid a_{ij}$, add the ith row to the first row, and return to step (2). The element a_{ij} now appears at the position $(1,j)$, and so it can be reduced modulo a_{11}. Repeating steps (1)–(3), we obtain a new, smaller value of a_{11}.
(5) Repeat step (4) until $a_{11} \mid a_{ij}$ for all i,j. (This process terminates, for the absolute values $|a_{11}|$ in step (4) form a decreasing sequence of positive integers.)
(6) From now on, ignore the first row and column, and repeat steps (1)–(5) with the $(n-1)\times(n-1)$ submatrix $(a_{ij})_{2\le i,j\le n}$, until the entry $a_{22} \mid a_{ij}$ for all $2 \le i,j \le n$. Note that by (5), we have $a_{11} \mid a_{22}$
(7) Iteratively ignore the first k rows and repeat the steps above. Eventually, we obtain a diagonal matrix satisfying $a_{11} \mid a_{22} \mid a_{33} \mid \cdots \mid a_{nn}$. This matrix corresponds to the desired bases. □

Proposition 4.10. *Consider full lattices $\Lambda' \subset \Lambda \subset V$. Then*

$$\frac{\mathrm{Vol}(D')}{\mathrm{Vol}(D)} = (\Lambda : \Lambda'),$$

where $(\Lambda : \Lambda')$ is the index of a subgroup.

Proof. Using Theorem 4.9, we have that $(\Lambda : \Lambda') = \prod m_i$. We can then view the ratio of volumes on the LHS by cutting D' into $m_1, \ldots, m_n$ pieces in the directions given by e_i, which yields the desired equality. □

Proof of Proposition 4.3. By definition we have

$$\mathcal{N}(\beta\mathcal{O}_K) = \#\mathcal{O}_K/\beta\mathcal{O}_K.$$

Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$. Then $\beta\omega_1, \ldots, \beta\omega_n$ is a basis for $\beta\mathcal{O}_K$ and

$$\mathcal{O}_K = \sum \mathbb{Z}\omega_i, \qquad \beta\mathcal{O}_K = \sum \mathbb{Z}\beta\omega_i.$$

Thus we can view $\beta\mathcal{O}_K \subset \mathcal{O}_K \subset \mathbb{R}^n$ as lattices.
Apply Proposition 4.10 with $\Lambda = \mathcal{O}_K$ and $\Lambda' = \beta\mathcal{O}_K$. We get

$$\mathcal{N}(\beta\mathcal{O}_K) = \#\mathcal{O}_K/\beta\mathcal{O}_K = (\Lambda : \Lambda') \overset{4.10}{=} \frac{\mathrm{Vol}(D')}{\mathrm{Vol}(D)} \overset{4.8c}{=} \frac{|\det(\beta\omega_1, \ldots, \beta\omega_n)|}{|\det(\omega_1, \ldots, \omega_n)|} \overset{\mathrm{def}}{=} |\det M_e(\beta)| = |N(\beta)|. \ \square$$

4.4 Lattice points in convex bodies

Proposition 4.11. *Let $\Lambda \subset V$ be a full lattice with fundamental domain D and let $S \subset V$ be a measurable set. If $\mathrm{Vol}\, S > \mathrm{Vol}\, D$, then there exist $\alpha, \beta \in S$ such that*

$$\beta - \alpha \in \Lambda.$$

Proof. For $\lambda \in \Lambda$ we denote $S_\lambda := S \cap (\lambda + D)$. Now we can express the volume of S as

$$\operatorname{Vol} S = \sum_{\lambda \in \Lambda} \operatorname{Vol} S_\lambda.$$

The volume $\operatorname{Vol} S_\lambda$ remains unchanged under shifting the set S_λ, and so

$$\operatorname{Vol} D > \operatorname{Vol} S = \sum_{\lambda \in \Lambda} \operatorname{Vol}(-\lambda + S_\lambda).$$

As $(-\lambda + S_\lambda) \subset D$ for all λ, and the total volume of these sets is greater than the volume of D, two of these sets must intersect.
Thus there exist $\alpha, \beta \in S$ and $\lambda, \lambda' \in \Lambda$ such that $-\lambda + \alpha = -\lambda' + \beta$. This implies that $\alpha - \beta = \lambda - \lambda' \in \Lambda$, as we wanted. □

Theorem 4.12 (Minkowski)**.** *Let V be a real vector space of dimension n. Let $T \subset V$ be a subset which is*

- *compact,*
- *convex, and*
- *symmetric around the origin, i.e., $\alpha \in T$ iff $-\alpha \in T$.*

Let Λ be a full lattice in V with fundamental domain D.
If

$$\operatorname{Vol} T \geq 2^n \operatorname{Vol} D, \qquad \text{then} \qquad T \cap \Lambda \neq \{0\}.$$

Proof. Clearly $T \neq \emptyset$. Then $0 \in T$ by symmetry and convexity. However, we want to show that some nonzero element lies in T. We will show this when $\operatorname{Vol} T > 2^n \operatorname{Vol} D$; if the volumes are equal, then one slightly enlarges T without increasing its intersection with Λ (this uses compactness of T; exercise).
We set

$$S := \frac{1}{2}T = \left\{ \frac{t}{2} \;\middle|\; t \in T \right\}.$$

Now $\operatorname{Vol} S > \operatorname{Vol} D$. By Proposition 4.11 there exist $\alpha, \beta = \frac{\gamma}{2}, \frac{\delta}{2} \in S$ such that

$$\Lambda \ni \beta - \alpha = \frac{\delta + (-\gamma)}{2}.$$

We have $-\gamma \in T$ by symmetry, and so the whole RHS lies in T by convexity. □

Minkowski theorem has a fun application.

Corollary 4.13. *Every positive integer is a sum of four squares.*

Proof. We have Euler's four-square identity (from 1748)

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = \\ (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 + (ag - bh - ce + df)^2 + (ah + bg - cf - de)^2.\end{aligned}$$

Therefore it suffices to prove the statement only for primes.
For $p = 2$, we have $p = 1 + 1 + 0 + 0$.
From now on, let $p > 2$ be an odd prime.

Lemma 4.14. *There are $m, n \in \mathbb{Z}$ such that*

$$m^2 + n^2 + 1 \equiv 0 \mod p.$$

Proof. Rewriting the congruence as

$$m^2 \equiv -n^2 - 1 \mod p,$$

one can see that there are $\frac{p+1}{2}$ possible values for the RHS and $\frac{p+1}{2}$ possible values for the LHS. By pigeonhole principle, at least two must be equal and give a solution. □

Fix a pair (m, n) from Lemma 4.14 and consider

$$\Lambda := \{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv ma + nb \mod p, \quad d \equiv mb - na \mod p\}.$$

This is clearly a subgroup of $\mathbb{Z}^4$. Since $\mathbb{Z}^4$ is discrete, Λ is also discrete. Thus Λ is a lattice by Lemma 4.7.
For $(a, b, c, d) \in \Lambda$, we have

$$a^2 + b^2 + c^2 + d^2 \equiv a^2(1 + m^2 + n^2) + b^2(1 + m^2 + n^2) + 2mnab - 2mnab \equiv 0 \mod p.$$

Lemma 4.15. $(\mathbb{Z}^4 : \Lambda) = p^2$, *and so the volume of fundamental domain D for Λ is* $\operatorname{Vol} D = p^2$.

Proof. We have $\mathbb{Z}^4 \supset \Lambda \supset (p\mathbb{Z})^4$, and so Λ is a full lattice.
By second isomorphism theorem

$$\mathbb{Z}^4/\Lambda \simeq \left((\mathbb{Z}/p\mathbb{Z})^4\right)/\left(\Lambda/(p\mathbb{Z})^4\right).$$

From this we see that $(\mathbb{Z}^4 : \Lambda) = \left(\mathbb{F}_p^4 : \Lambda/(p\mathbb{Z})^4\right)$. The quotient $\Lambda/(p\mathbb{Z})^4$ is an $\mathbb{F}_p$-vector space of dimension 2 (because a, b can be chosen arbitrarily, and they then determine c, d), and so the index

$$\left(\mathbb{F}_p^4 : \Lambda/(p\mathbb{Z})^4\right) = \frac{\#\mathbb{F}_p^4}{\#\Lambda/(p\mathbb{Z})^4} = \frac{p^4}{p^2} = p^2.$$ □

Let T denote the closed ball of radius r at the origin in $\mathbb{R}^4$, where $r^2 = (2 - \varepsilon)p$ for some sufficiently small $\varepsilon > 0$. We have

$$\operatorname{Vol} T = \frac{\pi^2 r^4}{2} = \pi^2(2 - \varepsilon)^2 p^2 \frac{1}{2} > 2^4 \operatorname{Vol} D,$$

and so by Theorem 4.12 there exists nonzero $(a, b, c, d) \in T \cap \Lambda$, i.e.,

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \mod p$$
$$a^2 + b^2 + c^2 + d^2 < r^2 < 2p.$$

Thus $p = a^2 + b^2 + c^2 + d^2$. □

Exercise. *Show that all primes $p \equiv 1 \mod 4$ can be expressed as the sum of two squares.*

4.5 Minkowski space

Definition. Let K be a number field of degree n with r real embeddings $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ and $2s$ complex embeddings

$$\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s} : K \hookrightarrow \mathbb{C}.$$

We then define the *Minkowski embedding* as the map

$$\begin{aligned} \sigma : \quad & K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \\ & \alpha \mapsto (\sigma_1\alpha, \ldots, \sigma_{r+s}\alpha). \end{aligned}$$

We call the real vector space $V := \mathbb{R}^r \times \mathbb{C}^s$ of dimension $r + 2s = n$ the *Minkowski space*.

Proposition 4.16. *Let $I < \mathcal{O}_K$. Then $\sigma(I)$ is a full lattice in V of covolume*

$$\mathcal{N}I \cdot \frac{|\Delta_K|^{1/2}}{2^s}.$$

Proof. Take an integral basis for the ideal $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$; such a basis exists by Proposition 2.9. The image $\sigma(I)$ is generated by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. We need to check whether they are independent over $\mathbb{R}$ to see if they form a lattice.

Let A be a matrix, whose i-th row is of the form

$$(\sigma_1\alpha_i \ldots \sigma_r\alpha_i,\ \operatorname{Re}\sigma_{r+1}\alpha_i,\ \operatorname{Im}\sigma_{r+1}\alpha_i, \ldots).$$

Matrix A has a nonzero determinant, hence the generators of $\sigma(I)$ are indeed linearly independent over $\mathbb{R}$ and thus $\sigma(I)$ is a lattice.
Now consider a matrix B with i-th row of the form

$$(\sigma_1\alpha_i \ldots \sigma_r\alpha_i,\ \sigma_{r+1}\alpha_i,\ \bar{\sigma}_{r+1}\alpha_i, \ldots).$$

Matrices A and B are related by some column operations.

$$\det A = (-2\sqrt{-1})^{-s} \det B \neq 0.$$

The determinant of B is nonzero because B is the matrix M from Lemma 2.4 and $\Delta_K \overset{2.6}{\neq} 0$. Thus $\sigma(I)$ is a full lattice. Since A can be viewed as having $\sigma\alpha_i$'s as its rows, $\operatorname{Vol} D = |\det A|$. By Corollary 2.6b)

$$|\Delta(\alpha_1, \ldots, \alpha_n)| = (\mathcal{O}_K : I)^2 |\Delta_K|$$
$$|\det A| = 2^{-s}(\mathcal{O}_K : I)|\Delta_K|^{1/2} = 2^{-s}|\Delta_K|^{1/2}\mathcal{N}I.$$

□

Lemma 4.17. *Let $x := (x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) \in V$. We define a norm on V as*

$$\|x\| := \sum_{i=1}^{r} |x_i| + 2\sum_{i=r+1}^{r+s} |z_i|.$$

Furthermore we shall denote the measure associated with this norm by Meas *and define the closed ball in V as the set*

$$X(t) := \{x \in V \mid \|x\| \leq t\}.$$

Then

$$\operatorname{Meas} X(t) = \frac{2^r \pi^s t^n}{n! 2^s}.$$

Exercise. *Check that Lemma 4.17 holds for $(r, s) = (1, 0), (0, 1)$.*

Proposition 4.18. *Let $I < \mathcal{O}_K$. Then there exists a nonzero element $\alpha \in I$ such that*

$$|N\alpha| \leq B_K \cdot \mathcal{N}I.$$

Proof. Let D be fundamental domain for $\sigma(I)$. The set $X(t)$ is symmetric, convex and compact. Choose t so that $\operatorname{Vol} X(t) \geq 2^n \operatorname{Vol} D$; by Theorem 4.12, there exists a nonzero $\sigma(\alpha) \in \sigma(I) \cap X(t)$. Now

$$|N\alpha| = |\sigma_1\alpha| \ldots |\sigma_r\alpha| \cdot |\sigma_{r+1}\alpha|^2 \ldots |\sigma_{r+s}\alpha|^2 \overset{AG}{\leq}$$
$$\overset{AG}{\leq} \left(\sum_{i=1}^{r} |\sigma_i\alpha| + 2\sum_{j=r+1}^{r+s} |\sigma_j\alpha|\right)^n \cdot \frac{1}{n^n} \leq \frac{t^n}{n^n}.$$

By our assumption $\operatorname{Vol} X(t) \geq 2^n \operatorname{Vol} D$, together with 4.16 and 4.17, we have

$$\frac{2^r \pi^s t^n}{n! 2^s} \geq \mathcal{N}I \cdot \frac{|\Delta_K|^{1/2}}{2^s}.$$

Choosing t so that equality holds and isolating t^n gives

$$|N\alpha| \leq \frac{t^n}{n^n} = \frac{n!}{n^n} \cdot \frac{2^n}{2^r \pi^s} \cdot \mathcal{N}I \cdot |\Delta_K|^{1/2} = B_K \cdot \mathcal{N}I.$$

□

Now we can prove the Minkowski bound from Theorem 4.4

Proof of Theorem 4.4. Let $[A] \in \mathcal{C}l_K$. Consider the class $[A^{-1}]$, which contains some ideal $J < \mathcal{O}_K$. By Proposition 4.18 there exists a nonzero $\beta \in J$ such that

$$|N\beta| \leq B_K \cdot \mathcal{N}J.$$

Since $\beta\mathcal{O}_K \subset J$, we have $J \mid \beta\mathcal{O}_K$, so there exists an ideal $H < \mathcal{O}_K$ such that $HJ = \beta\mathcal{O}_K$. Now

$$[H] = [J^{-1}] = [A] \implies H \in [A].$$

Therefore

$$\begin{aligned} \mathcal{N}J \cdot \mathcal{N}H = \mathcal{N}(\beta\mathcal{O}_K) \overset{4.3}{=} |N\beta| &\leq B_K \cdot \mathcal{N}J \\ \mathcal{N}H &\leq B_K. \end{aligned}$$

□

4.6 Dirichlet's unit theorem

In this section we will state Dirichlet's unit theorem and prove it. The proof will be split into parts, which we will prove separately throughout this section.

Definition. We denote by $\mu(K)$ the *torsion subgroup* of $\mathcal{O}_K^\times$, i.e., the subgroup of all elements of finite order.

Note that each $\zeta \in \mu(K)$ is a root of unity and we will often refer to them as such.

Theorem 4.19 (Dirichlet's unit theorem)**.** *Let K be a number field with r real embeddings and $2s$ complex embeddings. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$.*

Definition. The free generators of $\mathcal{O}_K^\times$ are called *fundamental units*, i.e.,

$$\mathcal{O}_K^\times = \{\zeta \cdot u_1^{m_1} \dots u_{r+s-1}^{m_{r+s-1}} \mid \zeta \in \mu(K), m_i \in \mathbb{Z}\},$$

where $\zeta, u_1, \dots, u_{r+s-1}$ are pairwise distinct. The tuple $(u_1, \dots, u_{r+s-1})$ is called the *system of fundamental units*.

Lemma 4.20. *An element $\alpha \in K$ lies in $\mathcal{O}_K^\times$ iff $\alpha \in \mathcal{O}_K$ and $N\alpha = \pm 1$.*

Proof. Let $\alpha \in \mathcal{O}_K^\times$. Since α is invertible, there exists $\beta \in \mathcal{O}_K^\times$ such that $\alpha\beta = 1$. Then

$$N\alpha \cdot N\beta = 1.$$

Since both $N\alpha$ and $N\beta$ lie in $\mathbb{Z}$, we get $N\alpha = \pm 1$.

Let $\alpha \in \mathcal{O}_K$ with $N\alpha = \pm 1$.

$$\pm 1 = N\alpha \overset{2.2}{=} \prod_\sigma \sigma\alpha$$
$$\pm 1 = \alpha \cdot \prod_{\sigma \neq \mathrm{id}} \sigma\alpha =: \alpha \cdot \beta$$

Since K is a field and $\beta = \alpha^{-1}$, we have $\beta \in K$. The conjugates $\sigma\alpha$ are roots of m_α, hence $\sigma\alpha \in \mathcal{O}_{\bar{\mathbb{Q}}}$, and therefore $\beta \in \mathcal{O}_{\bar{\mathbb{Q}}} \cap K = \mathcal{O}_K$. □

Lemma 4.21. *$\mu(K)$ is finite and cyclic.*

Proof. Since every finite multiplicative subgroup of a field is cyclic, it suffices to show that $\mu(K)$ is finite.

Let $\zeta_m \in \mu(K)$ be an m-th root of unity. Since $\mathbb{Q}(\zeta_m) \subset K$, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ divides $[K : \mathbb{Q}]$. However there are only finitely many m with $\varphi(m) \leq C$ for each bound C, hence $\mu(K)$ is finite. □

We will now start building up towards the proof of Dirichlet's unit theorem. We will first show that $\mathcal{O}_K^\times$ is finitely generated by proving the following proposition.

Proposition 4.22. *Let $m, M \in \mathbb{Z}$. Then the set of all $\alpha \in \mathcal{O}_{\overline{\mathbb{Q}}}$ such that*

- $\deg_{m_\alpha} := \deg \alpha \leq m$
- *$|\alpha'| \leq M$ for all conjugates α' of α*

is finite.

Proof. α is a root of a monic polynomial $f = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with $\deg f \leq m$. By Vieta's formulas, the coefficients of f are also bounded. Since f is monic, we have

$$-a_{d-1} = \sum \alpha'.$$

Now

$$|a_{d-1}| \leq \sum |\alpha'| < dM \leq mM,$$

but then there are only finitely many possible α'. □

Corollary 4.23. *Let $\alpha \in \mathcal{O}_{\overline{\mathbb{Q}}}$ be such that each conjugate α' of α satisfies $|\alpha'| \leq 1$. Then α is a root of unity or zero.*

Proof. For any $k \geq 1$, $\alpha^k \in \mathbb{Q}(\alpha)$ and hence α^k has bounded degree. Since taking a conjugate is a homomorphism, we have $|\alpha^k| \leq 1$. By Proposition 4.22 the set $\{1, \alpha, \alpha^2 \dots\}$ is finite, which means $\alpha^k = \alpha^\ell$ for some $k \neq \ell$. Then $\alpha^{\ell-k} = 1$, hence α is either zero or a root of unity. □

Definition. We define a map

$$\begin{aligned} L: \quad K^\times(\cdot) &\to \mathbb{R}^{r+s}(+) \\ \alpha &\mapsto (\log|\sigma_1\alpha|, \dots, \log|\sigma_r\alpha|, 2\log|\sigma_{r+1}\alpha|, \dots), \end{aligned}$$

which is a group homomorphism called the *logarithmic Minkowski embedding*.

Now consider taking $u \in \mathcal{O}_K^\times$, so $|Nu| = 1$. We have

$$1 = |\sigma_1 u| \cdot \dots \cdot |\sigma_r u| \cdot |\sigma_{r+1} u|^2 \dots$$
$$0 = \log|\sigma_1 u| + \dots + \log|\sigma_r u| + 2\log|\sigma_{r+1} u| + \dots$$

The image $L(u)$ thus lies in a hyperplane consisting of solutions to

$$x_1 + \dots + x_{r+s} = 0.$$

We shall denote this hyperplane by H and remark that $H \simeq \mathbb{R}^{r+s-1}$ as real vector spaces (e.g., consider the map $x \mapsto (x_1, \dots, x_{r+s-1})$).

Proposition 4.24. *The image of $L : \mathcal{O}_K^\times \to H$ is a lattice in H and the kernel $\operatorname{Ker} L = \mu(K)$ is finite.*

Proof. Let $\alpha \in \operatorname{Ker} L$, thus $|\sigma_i \alpha| = 1$ for all i. By Corollary 4.23 α is a root of unity and hence lies in $\mu(K)$, which is finite by Lemma 4.21.

Consider a bounded subset $C \subset H$ containing the origin. C is contained in a box

$$\{(x_1, \dots, x_{r+s}) \in H \mid |x_i| \le M\}$$

for some bound M. If $L(u) \in C$, then $|\sigma_j u| \le e^M$ for all j. By Proposition 4.22 there are only finitely many $u \in \mathcal{O}_K^\times$ such that $L(u) \in C$, hence $L(\mathcal{O}_K^\times)$ is discrete and thus it is a lattice. □

We now have

$$\operatorname{Rank} \mathcal{O}_K^\times = \operatorname{Rank}(L(\mathcal{O}_K^\times)) \le \dim H = r + s - 1,$$

hence we have an upper bound for the rank of $\mathcal{O}_K^\times$. Now we complete the proof of Dirichlet's theorem by showing the precise rank of $\mathcal{O}_K^\times$ in the following theorem.

Theorem 4.25. *$L(\mathcal{O}_K^\times)$ is a full lattice. Therefore* $\operatorname{Rank} \mathcal{O}_K^\times = r + s - 1$.

Proof. For $x := (x_1, \dots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s$ we define

$$Nx := x_1 \cdots x_r \cdot x_{r+1}\bar{x}_{r+1} \cdots x_{r+s}\bar{x}_{r+s},$$

so that $N_{K/\mathbb{Q}}(\alpha) = N(\sigma\alpha)$ where σ is the Minkowski embedding. Note that

$$|Nx| = |x_1| \cdots |x_r| \cdot |x_{r+1}|^2 \cdots |x_{r+s}|^2.$$

Let $x \in \mathbb{R}^r \times \mathbb{C}^s$ with $|Nx| = 1$ and consider the set

$$x \cdot \sigma(\mathcal{O}_K) = \{x \cdot \sigma\alpha \mid \alpha \in \mathcal{O}_K\},$$

where "$\cdot$" denotes the coordinate-wise product. By Proposition 4.16, $\sigma(\mathcal{O}_K)$ is a full lattice with covolume $\operatorname{Vol} D = 2^{-s}|\Delta_K|^{1/2}$, and $x \cdot \sigma(\mathcal{O}_K)$ is also a full lattice with the same covolume (since $|Nx| = 1$).
Consider $T \subset \mathbb{R}^r \times \mathbb{C}^s$ as in Theorem 4.12. Then there exists a nonzero $\gamma \in \mathcal{O}_K$ such that $x \cdot \sigma\gamma \in T$. Since T is compact, there is a constant $M > 0$ (depending only on T) such that $|Ny| \le M$ for all $y \in T$. In particular,

$$|N_{K/\mathbb{Q}}(\gamma)| = |N(\sigma\gamma)| = |N(x \cdot \sigma\gamma)| \le M,$$

where the second equality uses $|Nx| = 1$. Therefore the principal ideal $\gamma\mathcal{O}_K$ has bounded norm. There are only finitely many such principal ideals; denote them $(\gamma_1), \dots, (\gamma_t)$. For our γ, we have $(\gamma) = (\gamma_i)$ for some i, so there exists $\varepsilon \in \mathcal{O}_K^\times$ with $\gamma = \gamma_i\varepsilon$. Then $x \cdot \sigma\varepsilon \in \sigma(\gamma_i^{-1}) \cdot T$. Let

$$T' := \sigma(\gamma_1^{-1}) \cdot T \cup \dots \cup \sigma(\gamma_t^{-1}) \cdot T,$$

which is compact. Therefore, for all x with $|Nx| = 1$ there exists $\varepsilon \in \mathcal{O}_K^\times$ such that $|x_j \cdot \sigma_j \varepsilon| \leq M'$ for all j, where M' is independent of x.
For $r+s-1 = 0$ the theorem holds trivially. Let $r+s-1 \geq 1$. For each $1 \leq i \leq r+s$, choose x with $|Nx| = 1$ and $|x_j| > M'$ for all $j \neq i$. The bound above gives a unit $\varepsilon_i \in \mathcal{O}_K^\times$ such that $|\sigma_j \varepsilon_i| < 1$ for all $j \neq i$, i.e., $\log |\sigma_j \varepsilon_i| < 0$.

Now we shall prove that

$$L(\varepsilon_1), \dots, L(\varepsilon_{r+s-1})$$

are linearly independent vectors in $L(\mathcal{O}_K^\times)$, i.e., the matrix with rows of the form

$$(\ell_1 \varepsilon_i, \dots, \ell_r \varepsilon_i, 2\ell_{r+1}\varepsilon_i, \dots, 2\ell_{r+s-1}\varepsilon_i)$$

is invertible, where

$$\ell_j \varepsilon_i := \log |\sigma_j \varepsilon_i|.$$

We know $\ell_j \varepsilon_i < 0$ for all $j \neq i$ and

$$\ell_1 \varepsilon_i + \dots + 2\ell_{r+s}\varepsilon_i = 0.$$

Then the sum of i-th row is $-2\ell_{r+s}\varepsilon_i > 0$. Proving the following lemma from linear algebra concludes the proof.

Lemma 4.26. *Let (a_{ij}) be a real matrix such that*
a) $a_{ij} < 0$ for all $j \neq i$
b) $\sum_j a_{ij} > 0$ for all i
Then it is invertible.

□

The proof of Theorem 4.19 is thus also concluded. Let us now provide some remarks about the system of fundamental units.

How to find fundamental units
a) Choose $m \in \mathbb{Z}^+$ and find many $\alpha_i \in \mathcal{O}_K$ such that $N(\alpha_i) = \pm m$. Since there are only finitely many such α_i's, we will have collisions of the form $(\alpha_i) = (\alpha_j)$, but then $\alpha_i \alpha_j^{-1} \in \mathcal{O}_K^\times$.
b) Repeat a) until you have found enough such units, they then generate a subgroup of finite index. But how do we know when we have enough units? We will introduce the notion of regulator, which will help us determine that

Regulator
Let $t := r + s - 1$ and $\varepsilon_1, \dots, \varepsilon_t$ be independent units.

Definition. The *regulator* denoted by $\operatorname{Reg}(\varepsilon_1, \dots, \varepsilon_t)$ is the determinant of a matrix with i-th row of the form

$$\ell\varepsilon_i = (\log |\sigma_1 \varepsilon_i|, \dots, 2\log |\sigma_{r+1}\varepsilon_i|, \dots).$$

Moreover we define

$$\operatorname{Reg} K := \operatorname{Reg} \mathcal{O}_K^\times = |\operatorname{Reg}(\varepsilon_1, \dots, \varepsilon_t)|,$$

where $(\varepsilon_1, \dots, \varepsilon_t)$ is the system of fundamental units.

Class number formula
Now how do we find $\operatorname{Reg} \mathcal{O}_K^\times$? We will use the class number formula

$$h_K = \frac{w_K |\Delta_K|^{1/2}}{2^r (2\pi)^s \operatorname{Reg} \mathcal{O}_K^\times} \cdot \operatorname{res}_{s=1} \zeta_K(s),$$

where $w_K = \#\mu(K)$ and ζ_K is the Dedekind zeta function. Note that $\mu(K)$ is finite by Lemma 4.21 and $w_K \geq 2$ because we always have $\pm 1 \in \mu(K)$.
The Dedekind zeta function is defined as

$$\zeta_K(s) = \sum_{I < \mathcal{O}_K} N(I)^{-s}.$$

It generalizes the Riemann zeta function: for $K = \mathbb{Q}$ we have $\mathcal{O}_K = \mathbb{Z}$, and since all ideals $I < \mathbb{Z}$ are principal of the form (n) with $\mathcal{N}(n) = n$,

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

which is the Riemann zeta function.
Now since we know how to find h_K from the previous chapter, the only thing that remains is $\operatorname{Reg} \mathcal{O}_K^\times$, which we can obtain from the class number formula.

S-units

Definition. Let K be a number field and S a finite set of prime ideals in $\mathcal{O}_K$. The set of *algebraic S-integers* is

$$\mathcal{O}_K(S) := \{\alpha \in K \mid \operatorname{ord}_P \alpha \geq 0 \text{ for all } P \notin S\}.$$

Furthermore, the set of *algebraic S-units* is

$$\mathcal{O}_K^\times(S) := \{\alpha \in K \mid \operatorname{ord}_P \alpha = 0 \text{ for all } P \notin S\}.$$

Exercise. *Show that $\mathcal{O}_K(\emptyset) = \mathcal{O}_K$.*

Example. Let $K = \mathbb{Q}$ and $S = \{(2), (3), (5)\}$. Then

$$\mathcal{O}_K^\times(S) = \{\pm 2^k 3^\ell 5^m \mid k, \ell, m \in \mathbb{Z}\}.$$

Theorem 4.27. *$\mathcal{O}_K^\times(S)$ is a finitely generated group of rank $r + s - 1 + \#S$ for any finite set of primes S and any number field K.*

5. Cyclotomic fields & FLT

5.1 Cyclotomic fields

From now on let ζ be a primitive n-th root of 1 and consider the number field $K := \mathbb{Q}(\zeta)$. In this section we will aim to understand the ring of integers $\mathcal{O}_K$ of such number fields. Some proofs will not be provided and together with more details can be found in the text (in Czech only) linked below.
https://www.karlin.mff.cuni.cz/~kala/files/TC25.pdf

Exercise. *Show that if ζ is a primitive n-th root of 1, then ζ^a is a primitive n-th root of 1 iff $(a, n) = 1$.*

Now $K = \mathbb{Q}(\zeta)$ is a splitting field for $m_{\zeta,\mathbb{Q}}$ and also it is the splitting field for $x^n - 1 = \prod_{a=1}^{n}(x - \zeta^a)$. Moreover $K/\mathbb{Q}$ is a Galois extension.

Definition. For $n \in \mathbb{Z}^+$ we define the n-th *cyclotomic polynomial*

$$\Phi_n(x) = \prod_{a=1,(a,n)=1}^{n} (x - \zeta^a) = \prod_{\zeta'}(x - \zeta'),$$

where ζ' is a primitive n-th root of 1.

Remark. *a)* $\deg \Phi_n(x) = \phi(n)$*, where ϕ is Euler's totient function.*
b) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

From now on let $G := \mathrm{Gal}\left(K/\mathbb{Q}\right)$. Elements of G permute the roots of $x^n - 1$. For $\sigma \in G$ we have $\sigma\zeta = \zeta^a$ for some a. Since σ is invertible, a is also an invertible element mod n, hence $(a, n) = 1$ and thus elements of G map primitive n-th roots to primitive n-th roots. The coefficients of Φ_n are therefore also preserved by elements of G and thus

$$\Phi_n \in \mathbb{Q}[x] \cap \mathcal{O}_{\overline{\mathbb{Q}}}[x] \implies \Phi_n \in \mathbb{Z}[x].$$

For $(a, n) = 1$ we define a map σ_a such that $\sigma_a\zeta = \zeta^a$. For each $\sigma \in G$ there exists a such that $\sigma = \sigma_a$.
However σ_a is not necessarily well-defined. Consider $f, g \in \mathbb{Q}[x]$, then

$$\sigma_a(f(\zeta)) \overset{\text{def}}{=} f(\zeta^a).$$

If we suppose that $f(\zeta) = g(\zeta)$, then for σ_a to be well-defined it is necessary that $f(\zeta^a) = g(\zeta^a)$. Let us examine a simpler case. WLOG let $f(\zeta) = 0$, then we need that ζ^a is also a root of f. Since $f(\zeta) = 0 \iff m_{\zeta,\mathbb{Q}} \mid f$, it would suffice that $m_{\zeta,\mathbb{Q}}(\zeta^a) = 0$. This is equivalent to Φ_n being the minimal polynomial, hence irreducible.
Consider now the following injective group homomorphism

$$\begin{aligned} \psi :\ G &\to \left(\mathbb{Z}/n\right)^\times \\ \sigma_a &\mapsto a \end{aligned}$$

This map is surjective (and thus an isomorphism) if and only if Φ_n is irreducible.
We can summarize our findings so far into the following proposition.

Proposition 5.1. *TFAE*
a) $\psi : G \to \left(\mathbb{Z}/n\right)^{\times}$ *is an isomorphism.*
b) $[K : \mathbb{Q}] = \phi(n)$
c) G *acts transitively on primitive* n*-th roots of* 1.
d) Φ_n *is irreducible in* $\mathbb{Z}[x]$.

Proof. Left as an exercise. Try proving equivalences involving a). □

Theorem 5.2. *Let* ζ *be a primitive* n*-th root of* 1 *and* $K = \mathbb{Q}(\zeta)$. *Then*
a) $[K : \mathbb{Q}] = \phi(n)$
b) $\mathcal{O}_K = \mathbb{Z}[\zeta]$, *i.e.,* $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ *is an integral basis.*
c) if a prime number p *ramifies in* K, *then* $p \mid n$. *More precisely if* $n = p^r m$ *with* $p \nmid m$ *then*

$$p\mathcal{O}_K = (\underbrace{P_1 \cdots P_s}_{\text{pairwise distinct}})^{\varphi(p^r)}.$$

Proof. For proof see Milne's Algebraic Number Theory available at:
http://www.jmilne.org/math/CourseNotes/ant.html □

Proposition 5.3. *Let* $n = p^r$ *for* p *a prime number and let* ζ *be a primitive* n*-th root of unity. If we denote* $K = \mathbb{Q}(\zeta)$, *then*
a) $[K : \mathbb{Q}] = \phi(p^r) = p^{r-1}(p-1)$.
b) $\mathcal{O}_K = \mathbb{Z}[\zeta]$
c) $\pi = 1 - \zeta$ *is a prime element in* $\mathcal{O}_K$, *i.e.,* $(p) = (\pi)^e$, *where* $e = \phi(p^r)$. *By the efg theorem (3.1) this means*

$$\mathcal{O}_K/(\pi) \simeq \mathbb{Z}/(p).$$

d) $\Delta_K = \pm p^c$, *where* $c = p^{r-1}(pr - r - 1)$.

Proof. Since ζ is a root of $x^n - 1$, we have $\zeta \in \mathcal{O}_K$ and $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$. It remains to prove the other direction. For that purpose, we first make the following easy observation.

Lemma 5.4. *Let* ζ' *be some other primitive* n*-th root of unity. Then* $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$ *and* $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta') = K$.

Further, we have $\zeta^s = \zeta'$ for some $(s, n) = 1$.

$$\frac{1-\zeta'}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$$
$$\frac{1-\zeta}{1-\zeta'} \in \mathbb{Z}[\zeta'] = \mathbb{Z}[\zeta],$$

therefore

$$\frac{1-\zeta'}{1-\zeta} \in \mathbb{Z}[\zeta]^{\times} \subset \mathcal{O}_K^{\times}.$$

Let us now prove part a). We have

$$\deg m_{\zeta} = [K : \mathbb{Q}] \leq \deg \Phi_n = \phi(n).$$

Recall that we can write

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x),$$

hence

$$x^{p^r} - 1 = \Phi_{p^r}(x) \cdot (x^{p^{r-1}} - 1) \tag{5.1}$$

If we denote $t := x^{p^{r-1}}$, we can rewrite

$$\Phi_n(x) = \Phi_{p^r}(x) = 1 + t + \cdots + t^{p-1}$$
$$\Phi_{p^r}(1) = p = \prod_{\zeta'}(1-\zeta') = \prod \frac{1-\zeta'}{1-\zeta}(1-\zeta).$$

Since $\frac{1-\zeta'}{1-\zeta}$ lies in $\mathcal{O}_K^\times$, we obtain

$$p = \Phi_{p^r}(1) = u \cdot (1-\zeta)^e$$

for some $u \in \mathcal{O}_K^\times$. Denoting $\pi := 1 - \zeta$ yields the equality $(\pi)^e = (p)$. By the efg theorem (3.1) we have

$$e \leq [K : \mathbb{Q}] \leq \phi(n) = e,$$

which proves part a). Since (π) is a prime ideal in $\mathcal{O}_K$, π is a prime element (exercise), which also proves part c).

Thanks to the efg theorem we now also have the following isomorphism

$$\mathcal{O}_K/(\pi) \simeq \mathbb{Z}/(p).$$

Consider the map

$$\mathbb{Z}/(p) \to \mathcal{O}_K/(\pi)$$
$$a + (p) \mapsto a + (\pi)$$

which is an injection between fields. Since the inertia degree is equal to 1, this map is also an isomorphism, which yields

$$\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K \tag{5.2}$$

If we now show that

$$\Delta\left(\mathbb{Z}[\zeta]/\mathbb{Z}\right) = \Delta(1, \zeta, \ldots, \zeta^{n-1}) = \Delta\left(\mathcal{O}_K/\mathbb{Z}\right) \cdot (\mathcal{O}_K : \mathbb{Z}[\zeta])^2 = p^k$$

for some k, then we will have $\Delta_K = p^k$ and $(\mathcal{O}_K : \mathbb{Z}[\zeta]) = p^M$, i.e., $p^M\mathcal{O}_K \subset \mathbb{Z}[\zeta]$.

We have

$$\Delta(1, \zeta, \ldots, \zeta^{n-1}) = N_{K/\mathbb{Q}}(\Phi_n'(\zeta)).$$

Using (5.1) we obtain

$$\Phi_n'(\zeta) = \frac{n\zeta^{n-1}}{\zeta^{p^{r-1}} - 1}.$$

Furthermore we have

$$N(p^r) = N(p)^r = p^{re}$$
$$N(\zeta) = 1.$$

To determine $N(\zeta^{p^{r-1}} - 1)$, we use the following lemma.

Lemma 5.5. *For all $0 \leq s < r$, we have $N(1 - \zeta^{p^s}) = \pm p^{p^s}$.*

Proof. If $s = 0$, then $N(1-\zeta)$ is plus or minus the constant term of $\Phi_n(1-x)$, which is $\Phi_n(1) = p$. The rest of the proof of this lemma as well as the rest of part d) is left as an exercise. □

What remains to be proven is part b), so we aim to prove $\mathcal{O}_K = \mathbb{Z}[\zeta]$. From (5.2) we have

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z}[\zeta] + \pi\mathcal{O}_K \\ \pi\mathcal{O}_K &= \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K \\ \mathcal{O}_K &= \mathbb{Z}[\zeta] + \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K \\ \mathcal{O}_K &= \mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K\end{aligned}$$

and hence

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^j\mathcal{O}_K$$

for all j. Thus we can rewrite it as

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + p^m\mathcal{O}_K$$

for all m. However for $m = M$ we have $p^M\mathcal{O}_K \subset \mathbb{Z}[\zeta]$ and therefore $\mathcal{O}_K = \mathbb{Z}[\zeta]$, which concludes the proof. □

5.2 Regular primes and units

Definition. Let p be an odd prime number and let h_p denote the class number of $\mathbb{Q}(\zeta_p)$. We say that p is *regular* if $p \nmid h_p$.

Remark. *It is not known whether there are infinitely many regular primes. However it is known that there are infinitely many irregular primes.*

Theorem 5.6. *TFAE:*
a) p is a regular prime.
b) p does not divide the denominator of B_k for all $k = 2, 4, \ldots, p-3$, where B_k is the k-th Bernoulli number. Those are numbers that satisfy the following:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \cdot \frac{t^n}{n!}.$$

Definition. Let ζ be a primitive n-th root of unity. We define

$$\mathbb{Q}(\zeta)^+ := \mathbb{Q}(\zeta + \zeta^{-1}),$$

which is the largest *totally real* subfield in $\mathbb{Q}(\zeta)$, i.e., all conjugates of the generator are real or equivalently all embeddings of $\mathbb{Q}(\zeta)^+$ are real.

Lemma 5.7. *Let $K = \mathbb{Q}(\zeta)$ and $n = p^r$. Then for all $u \in \mathcal{O}_K^\times$ there exists $\mu \in \mu(\mathbb{Q}(\zeta))$ and $v \in \mathcal{O}_{\mathbb{Q}(\zeta)^+}^\times$ such that*

$$u = \mu \cdot v.$$

Proof. The proof is left as an exercise. □

5.3 FLT

Theorem 5.8. *Let p be an odd regular prime number. Then there are no $x, y, z \in \mathbb{Z}$ satisfying*

$$x^p + y^p = z^p \quad \text{and } p \nmid xyz.$$

Proof. Assume towards contradiction that there is a solution and that $(x, y, z) = 1$ (they are coprime). For $p = 3$ we have

$$a^3 \equiv 0, \pm 1 \mod 9$$

for all a, which leads to a contradiction. Similarly for $p = 5$. We assume then that $p \geq 7$ and WLOG assume $p \nmid x - y$ (exercise).

Consider a polynomial in variable T

$$T^p + 1 = \prod_{i=0}^{p-1} (T + \zeta^i).$$

Now for $T = \frac{x}{y}$ we obtain

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y) = z^p.$$

Let us now view the terms $(x + \zeta^i y)$ in $\mathbb{Z}[\zeta] = \mathcal{O}_{\mathbb{Q}(\zeta)}$.

Lemma 5.9. *$x + \zeta^i y \in \mathbb{Z}[\zeta]$ generate pairwise coprime ideals.*

Proof of Lemma 5.9. Assume for contradiction that there exists a prime ideal P such that

$$P \mid (x + \zeta^i y), \quad P \mid (x + \zeta^j y)$$

for some $i \neq j$. Then we have

$$P \mid ((\zeta^i - \zeta^j) y).$$

Observe now that $(\zeta^i - \zeta^j) = (\pi) = (1 - \zeta)$ and hence

$$P \mid (\pi y) \text{ and } P \mid (\pi x).$$

Since x and y are coprime in $\mathbb{Z}$, they are also coprime in $\mathbb{Z}[\zeta]$, so $P \mid (\pi)$. But (π) is a prime ideal, hence $P = (\pi)$. Now we have

$$\begin{aligned}
&\pi = 1 - \zeta \implies 1 \equiv \zeta^i && \mod \pi \\
\implies &x + y \equiv x + \zeta^i y \equiv 0 && \mod \pi \\
\implies &x + y \in \mathbb{Z} \cap (\pi) = (p) \\
\implies &z^p = x^p + y^p \equiv x + y \equiv 0 && \mod \pi
\end{aligned}$$

Hence $z \in \mathbb{Z} \cap (\pi) = (p)$, i.e., $p \mid z$, which contradicts the assumption $p \nmid xyz$. □

We will also need the following lemma.

Lemma 5.10. *a) For every $\alpha \in \mathbb{Z}[\zeta]$, we have $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta]$.*
b) Let $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ with $a_i \in \mathbb{Z}$ and at least one $a_i = 0$. If $n \in \mathbb{Z}$ is such that $n \mid \alpha$, then $n \mid a_i$ for all i.

Proof of Lemma 5.10 is left as an exercise.

Consider the following as an equality of ideals in $\mathbb{Z}[\zeta]$:

$$(z)^p = \prod_{i=0}^{p-1} (x + \zeta^i y).$$

The ideals $(x + \zeta^i y)$ are pairwise coprime (Lemma 5.9), so their prime factorizations must be disjoint. Moreover each factor must be a p-th power, so we write $(x + \zeta^i y) =: A_i^p$. Since A_i^p is principal, the

order of A_i in the class group divides p, so it is either 1 or p. By Lagrange's theorem, the order of A_i also divides h_p, and since p is a regular prime, the order must be 1, meaning that A_i is principal. Let $A_i =: (\alpha_i)$ for all i and consider for example α_1:

$$x + \zeta y = u\alpha_1^p$$

for some $u \in \mathcal{O}^\times_{\mathbb{Q}(\zeta)}$. By Lemma 5.7 we have

$$u = \mu \cdot v$$

where $\mu = \zeta^r$ for some r. Therefore

$$x + \zeta y = v\zeta^r \cdot \alpha_1^p,$$

with $v = \bar{v}$, because $v \in \mathbb{Q}(\zeta)^+$ (by Lemma 5.7). Now by Lemma 5.10a) we have

$$\alpha_1^p \equiv b \mod p\mathbb{Z}[\zeta]$$

for some $b \in \mathbb{Z}$. From this we have

$$\begin{aligned} x + \zeta y &\equiv v\zeta^r \cdot b \mod p\mathbb{Z}[\zeta] \\ x + \bar{\zeta} y &\equiv v\zeta^{-r} \cdot b \\ \implies vb &\equiv \zeta^{-r}(x + \zeta y) \\ &\equiv \zeta^r(x + \zeta^{-1} y) \end{aligned}$$

Hence $p \mid \zeta^{-r}(x+\zeta y) - \zeta^r(x+\zeta^{-1}y)$. Written in the basis $1, \zeta, \ldots, \zeta^{p-2}$, this element has at least one zero coefficient (using $p \nmid x - y$). By Lemma 5.10b), p divides all its coefficients, which forces $p \mid x$ and $p \mid y$, contradicting $p \nmid xyz$. □