Algebraic Number Theory
Vorlesung 2022

Prof. Dr. G. Nebe, Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen

Contents

Literatur:
Neukirch, Algebraische Zahlentheorie

All rings are associative and have a unit.

1 The ring of integers

1.1 The integral closure

Definition 1.1. *An* **algebraic number field** *K is a finite extension of $\mathbb{Q}$.*

Example. $K = \mathbb{Q}[\sqrt{5}] \cong \mathbb{Q}[x]/(x^2-5)$.

Remark 1.2. *Let L/K be a finite extension of fields and let $a \in L$. Then $\epsilon_a : K[x] \to L, p(x) \mapsto p(a)$ defines a K-algebra homomorphism with image $K[a]$ (the minimal K-subalgebra of L that contains a). Since $K[x]$ is a principal ideal domain, the kernel of ϵ_a is generated by a monic polynomial $\mathrm{Kern}(\epsilon_a) = (\mu_a(x))$. The image of ϵ_a is an integral domain, so $\mu_a(x) \in K[x]$ irreducible. This uniquely determined monic irreducible polynomial μ_a is called the* **minimal polynomial** *of a over K.*

Example. $a = \frac{1+\sqrt{5}}{2} \in \mathbb{Q}[\sqrt{5}] \Rightarrow \mu_a = x^2 - x - 1$ is the minimal polynomial of a over $\mathbb{Q}$.

Definition 1.3. *If B is a ring and A a subring of the* **center** *$Z(B) := \{b \in B \mid bx = xb \text{ for all } x \in B\}$, then B is called an* **A-algebra**.
If B is an A-algebra then $b \in B$ is called **integral** *over A, if there is $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in A$ such that*

$$(\star) \quad b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a_n = 0.$$

B is called **integral** *over A, if any element of B is integral over A.*

Theorem 1.4. *Let B be an A-algebra and $b \in B$. The following are equivalent*

(a) b is integral over A.

(b) The smallest A-subalgebra a $A[b]$ of B, that contains b is a finitely generated A-module.

(c) b is contained in some A-subalgebra of B, that is a finitely generated A-module.

Proof. (a) $\Rightarrow$ (b): If b is integral, then $(\star)$ implies that $A[b] = \langle 1, b, \ldots, b^{n-1}\rangle_A$.
(b) $\Rightarrow$ (c): Clear.
(c) $\Rightarrow$ (a): Let $R = \langle b_1, \ldots, b_n\rangle_A \leq B$ be some A-subalgebra of B that contains b. Assume wlog that $1 \in R$. Then there are (not necessarily unique) $a_{ij} \in A$ such that

$$bb_i = \sum_{j=1}^{n} a_{ij} b_j \text{ for all } 1 \leq i, j \leq n.$$

Let $f = \det(xI_n - (a_{ij})) \in A[x]$ be the characteristic polynomial of $(a_{ij}) \in A^{n \times n}$. Then $f \in A[X]$ is monic and $f((a_{ij})) = 0 \in A^{n \times n}$. Therefore $f(b)b_i = 0$ for all $1 \leq i \leq n$, so

$f(b)1 = f(b) = 0$, and hence b is integral over A. □

Example.
(a) $\alpha := \frac{1+\sqrt{5}}{2} \in \mathbb{Q}[\sqrt{5}]$ is integral over $\mathbb{Z}$.
(b) $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$.

Theorem 1.5. *Let B be a commutative A-algebra and*

$$\mathrm{Int}_A(B) := \{b \in B \mid b \textit{ integral over } A\}.$$

Then $\mathrm{Int}_A(B)$ is a subring of B called the **integral closure** *of A in B.*

Proof. We need to show that $\mathrm{Int}_A(B)$ is a ring, so closed under multiplication and addition. Let $b_1, b_2 \in \mathrm{Int}_A(B)$ and

$$A[b_1] = \langle c_1, \ldots, c_n \rangle_A, \ A[b_2] = \langle d_1, \ldots, d_m \rangle_A.$$

Since $c_i d_j = d_j c_i$ for all i, j and $1 \in A[b_1] \cap A[b_2]$ we get

$$A[b_1, b_2] \subset \langle c_i d_j \mid 1 \leq i \leq n, 1 \leq j \leq m \rangle_A.$$

This is a subring of B that is a finitely generated A-module and contains $b_1+b_2, b_1-b_2, b_1 b_2$. □

Theorem 1.6. *Let C be a commutative ring, $A \leq B \leq C$. If C is integral over B and B is integral over A, then C is integral over A.*

Proof. Let $c \in C$. Since C is integral over B there are $n \in \mathbb{N}$ and $b_1, \ldots, b_n \in B$ such that

$$c^n + b_1 c^{n-1} + \ldots + b_{n-1} c + b_n = 0.$$

Put $R := A[b_1, \ldots, b_n]$. Since B is integral over A this ring R is a finitely generated A-module. Moreover $c \in R[c]$ and $R[c]$ is a finitely generated R-module. So also $R[c]$ is a finitely generated A-module. and hence c is integral over A. □

Definition 1.7. *Let A be an integral domain with field of fraction $K := Quot(A)$.*

$$\mathrm{Int}_A(K) := \{x \in K \mid x \textit{ is integral over } A\}$$

is called the **integral closure** *of A in K.*
If $A = \mathrm{Int}_A(K)$, then A is called **integrally closed**.

Example. $\mathbb{Z}$ is integrally closed.
$\mathbb{Z}[\sqrt{2}]$ is integrally closed.
$\mathbb{Z}[\sqrt{5}]$ is not integrally closed.

Theorem 1.8. *Let $L \supseteq K$ be a finite field extension and $A \subset K$ integrally closed with $K = Quot(A)$. The for any $b \in L$:*
b is integral over A, if and only if $\mu_{b,K} \in A[x]$.

Proof. $\Leftarrow$ clear.
$\Rightarrow$: Let $b \in L$ be integral over A. Then there are $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in A$ such that

$$b^n + a_1 b^{n-1} + \ldots + a_{n-1} b + a_n = 0.$$

Put $p(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in A[x]$ and $\tilde{L} := Zerf_K(p)$ be the spitting field of p, Then all zeros $\tilde{b} \in \tilde{L}$ of p are integral over A. The minimal polynomial $\mu_{b,K}$ of b over K divides p, so also the zeros of $\mu_{b,K}$ are integral over A. The coefficients of $\mu_{b,K}$ are polynomials in the zeros, so also integral over A. Since these lie in K, they indeed lie in $\mathrm{Int}_A(K) = A$. So $\mu_{b,K} \in A[x]$. □

Corollary 1.9. *Let K be an algebraic number field. Then the ring of* **integers**

$$\mathbb{Z}_K = \mathrm{Int}_K(\mathbb{Z}) = \{a \in K \mid \mu_{a,\mathbb{Q}} \in \mathbb{Z}[x]\}.$$

Any $\mathbb{Z}$-basis of $\mathbb{Z}_K$ is called an **integral basis** *of K.*

Example. For $K = \mathbb{Q}[\sqrt{2}]$ we obtain $\mathbb{Z}_K = \mathbb{Z}[\sqrt{2}]$ and $(1, \sqrt{2})$ is a $\mathbb{Z}$-basis of K.
If $K = \mathbb{Q}[\sqrt{5}]$, then $\mathbb{Z}_K = \mathbb{Z}[(1+\sqrt{5})/2]$ and $(1, (1+\sqrt{5})/2)$ is a $\mathbb{Z}$-basis of K.
In the exercise you prove the more general statement: Let $1 \neq d \in \mathbb{Z}$ be square free and $K := \mathbb{Q}[\sqrt{d}]$, then $\alpha := \frac{1+\sqrt{d}}{2}$ is integral over $\mathbb{Z}$ if and only if $d \equiv_4 1$. In this case $(1, \alpha)$ is an integral basis of K, in all other cases $(1, \sqrt{d})$ is an integral basis.

1.2 Norm, Trace and Discriminant.

Remark 1.10. *Let L/K be a extension of fields of finite degree $[L : K] := \dim_K(L) = n < \infty$.*

(a) *Any $\alpha \in L$ induces a K-linear map*

$$mult_\alpha \in \mathrm{End}_K(L); x \mapsto \alpha x.$$

In particular this endomorphism has a trace, determinant, characteristic polynomial $\chi_{\alpha,K} := \chi_{mult_\alpha}$ and minimal polynomial $\mu_{\alpha,K} := \mu_{mult_\alpha}$.

(b) *The map mult: $L \to \mathrm{End}_K(L)$ is an injective homomorphism of K-algebras.*

(c) *The map $S_{L/K} : L \to K, \alpha \mapsto$ trace $(mult_\alpha)$ is a K-linear map, called the* **trace** *of L over K.*

(d) *The map $N_{L/K} : L \to K, \alpha \mapsto \det(mult_\alpha)$ is multiplicative, i.e. $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$ for all $\alpha, \beta \in L$. In particular it defines a group homomorphism $N_{L/K} : L^* \to K^*$ between the multiplicative groups L^* and $K^* = (K \setminus \{0\}, \cdot)$ of the fields.*

(e) *Let $\alpha \in L$. Then $\mu_{\alpha,K} \in K[X]$ is an irreducible polynomial of degree $d := [K(\alpha) : K] := \dim_K(K(\alpha))$ dividing n and $\chi_{\alpha,K} = \mu_{\alpha,K}^{n/d}$.*

(f) *If $\chi_{\alpha,K} = X^n - a_1 X^{n-1} + \ldots + (-1)^{n-1} a_{n-1} X + (-1)^n a_n \in K[X]$, then $N_{L/K}(\alpha) = a_n$ and $S_{L/K}(\alpha) = a_1$.*

Proof. Exercise. □

Theorem 1.11. *Assume that L/K is a finite separable extension and let $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ be the distinct K-algebra homomorphisms of L into the algebraic closure $\overline{K}$ of K (so $n = [L : K]$). Then for all $\alpha \in L$*

(a) $\chi_{\alpha,K} = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$.

(b) $\mu_{\alpha,K} = \prod_{i=1}^{d}(X - \alpha_i)$ *where* $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\} = \{\alpha_1, \dots, \alpha_d\}$ *has order* $d = [K(\alpha) : K]$.

(c) $S_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.

(d) $N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$.

Proof. (c) and (d) follow from (a) using Remark 1.10 (f) above.
To see (b) let $d := [K(\alpha) : K]$. Since L/K is separable, also the subfield $K(\alpha)$ is separable over K, so $\mu_{\alpha,K} = \prod_{i=1}^{d}(X - \alpha_i)$ for d distinct $\alpha_i \in \overline{K}$. The d distinct K-algebra homomorphisms $\varphi_1, \dots, \varphi_d$ from $K(\alpha)$ into $\overline{K}$ correspond to the d possible images $\varphi_i(\alpha) = \alpha_i \in \overline{K}$ of α.
In particular this proves (a) and (b) if $L = K(\alpha)$.
For the more general statement we use the following:
Fact.[1] Any K-algebra homomorphism $\tau : E \to \overline{K}$ of some algebraic extension E of K into the algebraic closure $\overline{K}$ extends to an automorphism $\tilde{\tau} \in \mathrm{Aut}_K(\overline{K})$.
Let $\tilde{\varphi}_j$ be such an extension of φ_j for all $j = 1, \dots, d$ and let $\{\tau_1, \dots, \tau_{n/d}\} = \mathrm{Hom}_{K(\alpha)}(L, \overline{K})$. Then

$$\{\sigma_1, \dots, \sigma_n\} = \{\tilde{\varphi}_j \circ \tau_i \mid 1 \le j \le d, 1 \le i \le n/d\}$$

In particular each φ_j can be extended in exactly n/d ways to a K-homomorphism $\tilde{\varphi}_j \circ \tau_i : L \to \overline{K}$, $1 \le i \le n/d$.
This implies that $\chi_{\alpha,K} = \mu_{\alpha,K}^{n/d}$ and also (a) and (b) follow. □

Corollary 1.12. *Let $K \subseteq L \subseteq M$ be a tower of separable field extensions of finite degree. Then*

$$S_{M/K} = S_{L/K} \circ S_{M/L} \text{ and } N_{M/K} = N_{L/K} \circ N_{M/L}$$

Proof. Let $m := [M : K]$, $\ell := [L : K]$ and $n := [M : L]$. Then $m = \ell n$. Define an equivalence relation on $\{\sigma_1, \dots, \sigma_m\} = \mathrm{Hom}_K(M, \overline{K})$ by

$$\sigma_j \sim \sigma_i \Leftrightarrow (\sigma_j)_L = (\sigma_i)_L.$$

As we have seen in the last proof each equivalence class A_j contains exactly n elements. Therefore for any $\alpha \in M$

$$S_{M/K}(\alpha) = \sum_{i=1}^{m} \sigma_i(\alpha) = \sum_{j=1}^{\ell} \sum_{\sigma \in A_j} \sigma(\alpha).$$

[1] (1.33) of the script of the Algebra lecture

Wlog we assume that $A_j = [\sigma_j]$. Then

$$\sum_{\sigma \in A_j} \sigma(\alpha) = S_{\sigma_j(M)/\sigma_j(L)}(\sigma_j(\alpha)) = \sigma_j(S_{M/L}(\alpha)).$$

Therefore $S_{M/K}(\alpha) = \sum_{j=1}^{\ell} \sigma_j(S_{M/L}(\alpha)) = (S_{L/K} \circ S_{M/L})(\alpha)$. Similarly for the norm. □

Definition 1.13. *Let L/K be a separable extension and let $B := (\alpha_1, \ldots, \alpha_n)$ be a K-basis of L.*

(a) The **Trace-Bilinear-Form** *$S : L \times L \to K$, $S(\alpha, \beta) := S_{L/K}(\alpha\beta)$ is a symmetric K-bilinear form.*

(b) The **discriminant** *of B is the determinant of the Gram matrix of B, $d(B) := \det(S(\alpha_i, \alpha_j)_{i,j})$.*

Remark 1.14. *If $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \overline{K})$ then $d(B) = \det((\sigma_i(\alpha_j))_{i,j})^2$.*

Proof. $S_{L/K}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = [(\sigma_k(\alpha_i)_{i,k})^{tr}(\sigma_k(\alpha_i)_{i,k})]_{i,j}$ so $(S_{L/K}(\alpha_i\alpha_j)) = A^{tr}A$ with $A = (\sigma_k(\alpha_i)_{i,k})$. □

Example. If $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{d}]$ then $B := (1, \sqrt{d})$ is a K-basis of L and $d(B) = 2 \cdot (2d) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2$

Theorem 1.15. *Let L/K be a separable extension an let $B := (\alpha_1, \ldots, \alpha_n)$ be a K-basis of L. Then the trace bilinear form is a non-degenerate symmetric K-bilinear form. In particular $d(B) \neq 0$.*

Proof. Choose a primitive element $\alpha \in L$, so $L = K(\alpha)$ and $B_1 := (1, \alpha, \ldots, \alpha^{n-1})$ is another K-basis of L. By the transformation rule for Gram matrices, $d(B) = d(B_1)a^2$ where $a \in K^*$ is the determinant of the base change matrix between B and B_1. So it is enough to show that $d(B_1) \neq 0$. By the remark above $d(B_1) = d(A)^2$ where

$$A = ((\sigma_i(\alpha^j))_{j=0,..,n-1, i=1,..,n} = \begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \ldots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \ldots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & \ldots & \ldots & \vdots \\ 1 & \sigma_n(\alpha) & \sigma_n(\alpha)^2 & \ldots & \sigma_n(\alpha)^{n-1} \end{pmatrix}$$

and $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_K(L, \overline{K})$. By Vandermonde $det(A) = \prod_{i<j}(\sigma_j(\alpha) - \sigma_i(\alpha))$, so $d(B_1) = (\prod_{i<j}(\sigma_j(\alpha) - \sigma_i(\alpha)))^2 \neq 0$, since the different embeddings of L into $\overline{K}$ have different values on the primitive element α. □

Definition 1.16. *Let K be an algebraic number field and $B := (\alpha_1, \ldots, \alpha_n)$ be an integral basis of K (i.e. a $\mathbb{Z}$-basis of the ring of integers $\mathbb{Z}_K$). Then the* **discriminant** *of K is $d_K := d(B)$.*

More general let $\mathcal{A} = \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}}$ be a free $\mathbb{Z}$-module of full rank in K. Then

$$d_{\mathcal{A}} := d((\beta_1, \ldots, \beta_n))$$

is called the **discriminant** *of $\mathcal{A}$.*

Remark 1.17. *d_K and $d_{\mathcal{A}}$ are well defined, which means that they do not dependent on the choice of the integral basis B.*
If $\mathcal{A}' \subseteq \mathcal{A} \subseteq K$ are two finitely generated $\mathbb{Z}$-modules of full rank in K, then by the main theorem on finitely generated $\mathbb{Z}$-modules (elementary divisor theorem) the index

$$a := [\mathcal{A} : \mathcal{A}'] := |\mathcal{A}/\mathcal{A}'| < \infty$$

and $d_{\mathcal{A}'} = a^2 d_{\mathcal{A}}$.

Example. $K = \mathbb{Q}[\sqrt{d}]$, $0, 1 \neq d \in \mathbb{Z}$ square-free. Integral basis, Gram matrix, discriminant.

1.2.1 An algorithm to determine an integral basis of a number field.

Definition 1.18. *Let $V \cong \mathbb{R}^n$ be an n-dimensional real vector space and $\Phi : V \times V \to \mathbb{R}$ a non-degenerate symmetric bilinear form.*

(a) A **lattice** *in V is the set of all integral linear combinations of an $\mathbb{R}$-basis of V.*

$$L = \langle B \rangle_{\mathbb{Z}} = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z}\}$$

for some basis $B = (b_1, \ldots, b_n)$ of V. Any such $\mathbb{Z}$-basis B of L is called a **basis** *of L and the determinant of the Gram matrix of B with respect to Φ is called the* **determinant** *of L.*

(b) For a lattice $L := \langle B \rangle_{\mathbb{Z}}$ the set $L^{\#} := \{x \in V \mid \Phi(x, L) \subseteq \mathbb{Z}\}$ is called the **dual lattice** *of L (wrt Φ).*

(c) L is called **integral** *(wrt Φ), if $L \subseteq L^{\#}$.*

Remark. $L^{\#}$ is a lattice in V, the dual basis B^* of any lattice basis B of L is a lattice basis of $L^{\#}$. The base change matrix between B and B^* is the Gram matrix $M_B(\Phi) = (\Phi(b_i, b_j))$ of B. In particular $\det(M_B(\Phi)) = [L^{\#} : L] = |L^{\#}/L|$ for any integral lattice L.

Theorem 1.19. *Let K be an algebraic number field, $\mathcal{O} \subseteq \mathbb{Z}_K$ a full $\mathbb{Z}$-lattice in K. Then $(\mathcal{O}, S_{K/\mathbb{Q}})$ is an integral lattice and*

$$\mathcal{O} \underbrace{\subseteq}_{f} \mathbb{Z}_K \underbrace{\subseteq}_{d_K} \mathbb{Z}_K^{\#} \underbrace{\subseteq}_{f} \mathcal{O}^{\#}$$

which yields an algorithm to compute $\mathbb{Z}_K$.

Corollary. The ring of integers $\mathbb{Z}_K$ in an algebraic number field is finitely generated, so any algebraic number field has an integral basis.

1.3 Dedekind domains.

Example. Let $K = \mathbb{Q}[\sqrt{-5}]$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$ and

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

has no unique factorization.
Note that the factors above are irreducible but not prime.
Reason: The ideals $3\mathbb{Z}_K = \wp_3\wp_3'$, $7\mathbb{Z}_K = \wp_7\wp_7'$, $(1+2\sqrt{-5})\mathbb{Z}_K = \wp_3\wp_7$, and $(1-2\sqrt{-5})\mathbb{Z}_K = \wp_3'\wp_7'$ are not prime ideals, where

$$\wp_3 = (3, 1 + 2\sqrt{-5}),\ \wp_3' = (3, 1 - 2\sqrt{-5}),\ \wp_7 = (7, 1 + 2\sqrt{-5}),\ \wp_7' = (7, 1 - 2\sqrt{-5})$$

and so $21\mathbb{Z}_K = \wp_3\wp_3'\wp_7\wp_7'$ is a unique product of prime ideals.
A ring with a unique prime ideal factorisation is called a Dedekind ring:

Definition 1.20. *A Noetherian, integrally closed, integral domain in which all non-zero prime ideals are maximal ideals is called a* **Dedekind domain***.*

Example. $\mathbb{Z}[x]$ is not a Dedekind domain, because (x) is a prime ideal (the quotient is isomorphic to $\mathbb{Z}$) but not maximal, since $\mathbb{Z}$ is not a field.

Theorem 1.21. *Let K be a number field. Then $\mathbb{Z}_K$ is a Dedekind domain.*

Proof. Clearly $\mathbb{Z}_K$ is integrally closed and an integral domain.
We first show that $\mathbb{Z}_K$ is Noetherian, i.e. any ideal of $\mathbb{Z}_K$ is finitely generated. Let $0 \neq \mathcal{A} \trianglelefteq \mathbb{Z}_K$ be an ideal and choose $0 \neq a \in \mathcal{A}$. If $B := (b_1, \ldots, b_n)$ is an integral basis of K, then $aB := (ab_1, \ldots, ab_n) \in \mathcal{A}^n$ is also a $\mathbb{Q}$-basis of K. The lattice $\langle aB \rangle_{\mathbb{Z}} \subseteq \mathcal{A} \subseteq \langle B \rangle_{\mathbb{Z}} = \mathbb{Z}_K$ has finite index in $\mathbb{Z}_K$. Therefore also $\mathcal{A}$ has finite index in $\mathbb{Z}_K$ and, by the main theorem on finitely generated $\mathbb{Z}$-modules, $\mathcal{A}$ is finitely generated as a $\mathbb{Z}$-module and hence also as a $\mathbb{Z}_K$-module.
The above consideration also applies to non-zero prime ideals $0 \neq \wp \trianglelefteq \mathbb{Z}_K$ of $\mathbb{Z}_K$, in particular any such prime ideal has finite index in $\mathbb{Z}_K$. Therefore $\mathbb{Z}_K/\wp$ is a finite integral domain, so a field, which means that $\wp$ is a maximal ideal. □

Lemma 1.22. *Any finite integral domain R is a field.*

Proof. Let $0 \neq a \in R$, then $\mathrm{mult}_a : R \to R$ is injective (the kernel is 0, since R is an integral domain) and hence surjective (since R is finite). In particular there is some $x \in R$ such that $\mathrm{mult}_a(x) = 1$. □

Definition 1.23. *Let R be a commutative ring and $A, B \trianglelefteq R$. Then*

$$A + B := \{a + b \mid a \in A, b \in B\} \trianglelefteq R,\ AB := \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in A, b_i \in B\} \trianglelefteq R.$$

If $A \subseteq B$ we say that B **divides** *A. The* **greatest common divisor**

$$\mathrm{ggT}(A, B) := (A, B) = A + B$$

is the ideal generated by A and B.

From now on let R be a Dedekind domain and $K = Quot(R)$.

Main theorem 1.24. *Any ideal $0 \neq I \trianglelefteq R$ in R has a unique factorization into prime ideals,*

$$I = \wp_1 \dots \wp_s, s \in \mathbb{N}_0, \wp_i \trianglelefteq R \textit{ prime ideals} .$$

For the proof we need two lemmata:

Lemma 1.25. *If $0 \neq I \trianglelefteq R$ then there are non-zero prime ideals $\wp_1, \dots, \wp_s \trianglelefteq R$ such that $\wp_1 \dots \wp_s \subseteq I$.*

Proof. Let $\mathcal{M} := \{ \begin{array}{l} I \trianglelefteq R \mid I \neq 0, \text{ and for all prime ideals } \wp_1, \dots, \wp_s \text{ the product} \\ \wp_1 \dots \wp_s \text{ is not contained in } I \end{array} \}$. We need to show that $\mathcal{M} = \emptyset$. Assume that $\mathcal{M} \neq \emptyset$. Since any ascending chain of ideals in R is finite, the set $\mathcal{M}$ contains some maximal element $\mathcal{A} \in \mathcal{M}$. Then $\mathcal{A}$ is not a prime ideal, hence there are $b_1, b_2 \in R$ such that

$$b_1 b_2 \in \mathcal{A}, b_1 \notin \mathcal{A}, b_2 \notin \mathcal{A}.$$

Let $\mathcal{A}_i := (b_i) + \mathcal{A}$. Then $\mathcal{A}_i \supsetneq \mathcal{A}$ but $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}$. Since $\mathcal{A}$ is maximal in $\mathcal{M}$, both $\mathcal{A}_i$ contain a product of prime ideals, hence also $\mathcal{A}_1\mathcal{A}_2$ and therefore $\mathcal{A}$, a contradiction. □

Lemma 1.26. *Let $0 \neq \wp \trianglelefteq R$ be a prime ideal and put*

$$\wp^{-1} := \{x \in K \mid x\wp \subseteq R\}.$$

Then for any non zero ideal $0 \neq \mathcal{A} \trianglelefteq R$ the ideal $\mathcal{A}\wp^{-1}$ properly contains $\mathcal{A}$.

Proof. We first show that $\wp^{-1} \neq R$: Choose some $0 \neq a \in \wp$ and let $s \in \mathbb{N}$ be minimal with the property that there are non-zero prime ideals $\wp_1, \dots, \wp_s$ in R such that $\wp_1 \dots \wp_s \subseteq (a) \subseteq \wp$. (These exist since R is Noetherian.)
Claim. There is some i such that $\wp_i \subseteq \wp$.
Otherwise there are $a_i \in \wp_i \setminus \wp$ for all $i = 1, \dots, s$, but $a_1 \dots a_s \in \wp_1 \dots \wp_s \subseteq \wp$ which contradicts the fact that $\wp$ is a prime ideal.
Assume wlog that $\wp_1 \subseteq \wp$. Since R is a Dedekind domain, the non-zero prime ideal $\wp_1$ is maximal. Therefore $\wp = \wp_1$.
By the minimality of s we have that $\wp_2 \dots \wp_s \not\subseteq (a)$ so there is some $b \in \wp_2 \dots \wp_s$ such that $a^{-1}b \notin R$. On the other hand

$$a^{-1}b\wp = a^{-1}b\wp_1 \subseteq a^{-1}\wp_1 \dots \wp_s \subseteq a^{-1}(a) = R$$

so $a^{-1}b \in \wp^{-1} \setminus R$.
Now choose some nonzero ideal $\mathcal{A} \trianglelefteq R$ and assume that $\mathcal{A}\wp^{-1} = \mathcal{A}$. Let $\mathcal{A} = \langle \alpha_1, \dots, \alpha_n \rangle_R$ (observe that $\mathcal{A}$ is finitely generated, since R is Noetherian). Then for any $x \in \wp^{-1}$ and any i we have $x\alpha_i = \sum_{j=1}^n x_{ij}\alpha_j$ for some matrix $(x_{ij}) =: X \in R^{n \times n}$. Therefore the vector $(\alpha_1, \dots, \alpha_n)^{tr}$ is in the kernel of $(xI_n - X) \in K^{n \times n}$, so the determinant of this matrix is 0. But then x is a zero of some monic polynomial with coefficients in R, so $x \in \mathrm{Int}_K(R) = R$, since R is integrally closed. This holds for any $x \in \wp^{-1}$ contradicting the fact that $\wp^{-1} \not\subseteq R$. □

Corollary 1.27. *For any non-zero prime ideal $0 \neq \wp \trianglelefteq R$ the product $\wp\wp^{-1} = R$.*

Proof. $\wp \subsetneq \wp\wp^{-1} \subseteq R$. Since R is a Dedekind domain, $\wp$ is a maximal ideal, so $\wp\wp^{-1} = R$. □

Proof of the main Theorem 1.24

Existence. Let $\mathcal{M} := \{\mathcal{A} \trianglelefteq R \mid 0 \neq \mathcal{A} \neq R, \mathcal{A} \neq \wp_1 \dots \wp_s$ for all prime ideals $\wp_1, \dots, \wp_s$ and all $s \in \mathbb{N}\}$. We need to show that $\mathcal{M} = \emptyset$. If $\mathcal{M} \neq \emptyset$, then $\mathcal{M}$ contains some maximal element, say $\mathcal{A}$. Since maximal ideals are prime ideals, the ideal $\mathcal{A}$ is not a maximal ideal. There is some maximal ideal $\wp \trianglelefteq R$ that contains $\mathcal{A}$, so $\mathcal{A} \subseteq \wp \subseteq R$ and hence $\mathcal{A} \subsetneq \mathcal{A}\wp^{-1} \subseteq \wp\wp^{-1} = R$. Now $\mathcal{A} \neq \wp$ was maximal in $\mathcal{M}$, so there are prime-ideals $\wp_1, \dots, \wp_s$ such that

$$\mathcal{A}\wp^{-1} = \wp_1 \dots \wp_s \Rightarrow \mathcal{A} = \wp_1 \dots \wp_s \wp$$

a contradiction.

Uniqueness. (this is analogues to the proof of uniqueness of prime factorization in $\mathbb{Z}$) We have seen in the proof of Lemma 1.26 that if a prime ideal $\wp$ divides the product of two ideals, then it divides one of the factors

$$I_1 I_2 \subseteq \wp \Rightarrow I_1 \subseteq \wp \text{ or } I_2 \subseteq \wp.$$

So assume that

$$\mathcal{A} = \wp_1 \dots \wp_s = \mathcal{Q}_1 \dots \mathcal{Q}_t$$

then $\wp_1$ divides $\mathcal{Q}_1 \dots \mathcal{Q}_t$ so it divides one of the factors, say $\mathcal{Q}_1$. Since $\mathcal{Q}_1$ is maximal, this implies $\mathcal{Q}_1 = \wp_1$, so

$$\wp^{-1}\mathcal{A} = \wp_2 \dots \wp_s = \mathcal{Q}_2 \dots \mathcal{Q}_t$$

Definition 1.28. *A* **fractional ideal** *of R is a finitely generated R-submodule $\neq 0$ of K.*

Remark 1.29. *Let J be a fractional ideal of R. Then there is $c \in K$, $\mathcal{A} \trianglelefteq R$, such that $c\mathcal{A} = J$.*

Proof. Let $J = \langle \alpha_1, \dots, \alpha_n \rangle_R$, $\alpha_i = \frac{\beta_i}{\gamma_i} \in K$ wit $\beta_i, \gamma_i \in R$. Let $\gamma := \gamma_1 \dots \gamma_n$. Then $\mathcal{A} := \gamma J \trianglelefteq R$ and $J = \gamma^{-1}\mathcal{A}$. □

Theorem 1.30. *The set of fractional ideal of R is an abelian group, the* **ideal group** *of R.*

Proof. The group law is of course ideal multiplication, this is associative, commutative, the unit is $(1) = R$ and the inverse is $\mathcal{A}^{-1} = \{x \in K \mid xI \subseteq R\}$. □

Corollary 1.31. *Any fractional ideal $\mathcal{A}$ of R has a unique factorization*

$$\mathcal{A} = \wp_1^{n_1} \dots \wp_s^{n_s}$$

with non-zero prime ideals $\wp_1, \dots, \wp_s$ and $n_i \in \mathbb{Z}$.

Definition 1.32. *The* **ideal group** *of R is denoted by J_R. It contains the subgroup $\{(c) \mid c \in K^*\} = P_R$ of* **principal fractional ideals***. The quotient $Cl_K := J_R/P_R$ is called the* **class group** *of K.*

There is an exact sequence

$$1 \to R^* \overset{\varphi_1}{\to} K^* \overset{\varphi_2}{\to} J_R \overset{\varphi_3}{\to} Cl_K \to 1$$

where φ_1 is just the inclusion, $\varphi_2(c) = (c)$, and φ_3 is the natural epimorphism. This means that φ_1 is injective, $im(\varphi_1) = ker(\varphi_2)$, $im(\varphi_2) = P_R = ker(\varphi_3)$, and φ_3 is surjective.

If $R = \mathbb{Z}_K$ is the ring of integers in an algebraic number field K, then

- $\mathbb{Z}_K^*$ is a finitely generated abelian group
- Cl_K is a finite group, $h_K := |Cl_K|$ is called the **class number** of K

2 Geometry of numbers.

Definition 2.1. *Let $(\mathbb{R}^n, (,))$ be a Euclidean space. Any $\mathbb{Z}$-module generated by a basis of $\mathbb{R}^n$ is called a* **full lattice** *in $(\mathbb{R}^n, (,))$. Let $\Gamma := \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}}$ be a full lattice. Then $B = (b_1, \ldots, b_n)$ is called a* **basis** *of Γ and*

$$E(B) := \{\sum_{i=1}^{n} \lambda_i b_i \mid 0 \le \lambda_i \le 1\}$$

the **fundamental parallelotope** *of B. The* **determinant** *of Γ is $\det(\Gamma) := \det((b_i, b_j))$ and the* **covolume** *of Γ is*

$$\mathrm{covol}(\Gamma) := \mathrm{vol}(\mathbb{R}^n/\Gamma) := \mathrm{vol}(E(B)) = \sqrt{\det(\Gamma)}.$$

Example. $\mathbb{Z}^2$: Different bases yield different $E(B)$ but these have the same covolume.

Remark 2.2. *$E(B)$ is a* **fundamental domain** *for the action of Γ on $\mathbb{R}^n$ by translation. this means that*

$$\mathbb{R}^n = \bigcup_{\gamma \in \Gamma} \gamma + E(B)$$

and this union is almost disjoint, Γ-translates of $E(B)$ are either equal or intersect only in the boundary.

Definition 2.3. *Let $\emptyset \neq X \subset \mathbb{R}^n$.*
(a) X is called **centrally symmetric***, if for any $x \in X$ also its negative $-x \in X$.*
(b) X is called **convex***, if for any two $x, y \in X$ and any $t \in [0,1]$ also $x + t(y - x) \in X$.*

Clear: $\emptyset \neq X$ convex and centrally symmetric, then $0 \in X$.

Theorem 2.4. *(Minkowski) Let $\Gamma \subset (\mathbb{R}^n, (,))$ be a full lattice in Euclidean space and let $X \subseteq \mathbb{R}^n$ be convex and centrally symmetric. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\mathbb{R}^n/\Gamma)$ then $\Gamma \cap X \neq \{0\}$.*

Proof. We show that there are $\gamma_1 \neq \gamma_2 \in \Gamma$ such that

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$$

Then there are $x_1, x_2 \in X$ such that $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ and hence

$$\frac{1}{2}(x_1 - x_2) = \gamma_2 - \gamma_1 \in \Gamma \cap X$$

is a nonzero vector. Note that $\frac{1}{2}(x_1 - x_2)$ is the midpoint of the line between x_1 and $-x_2$ and therefore in X.
So assume that the Γ -translates of the set $\frac{1}{2}X = \{\frac{1}{2}x \mid x \in X\}$ are disjoint,

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) = \emptyset \text{ for all } \gamma_1 \neq \gamma_2 \in \Gamma$$

But then also the intersection with the fundamental parallelotope

$$(E(B) \cap (\frac{1}{2}X + \gamma_1)) \cap (E(B) \cap (\frac{1}{2}X + \gamma_2)) = \emptyset \text{ for all } \gamma_1 \neq \gamma_2 \in \Gamma \text{ so}$$

$$\begin{array}{l} \mathrm{vol}(\mathbb{R}^n/\Gamma) = \mathrm{vol}(E(B)) \geq \sum_{\gamma\in\Gamma} \mathrm{vol}(E(B) \cap (\frac{1}{2}X + \gamma)) = \\ \sum_{\gamma\in\Gamma} \mathrm{vol}((E(B) - \gamma) \cap \frac{1}{2}X) = \mathrm{vol}(\frac{1}{2}X) = \frac{1}{2^n}\mathrm{vol}(X) \end{array}$$

which contradicts the assumption. □

Example. The bound is tight: Take $\Gamma = \mathbb{Z}^2$ and

$$X := \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \mid |x_1| < 1 \text{ and } |x_2| < 1\}.$$

Then $\mathrm{vol}(X) = \mathrm{vol}(\overline{X}) = 2^2$, $\mathrm{covol}(\Gamma) = 1$ and $X \cap \Gamma = \{0\}$.

We now apply this to number fields K. For this aim we need to embed K into some euclidean space.

Remark 2.5. *Let K be an algebraic number field of degree $[K : \mathbb{Q}] =: n$. Let*

$$\sigma_1, \dots, \sigma_n : K \to \overline{\mathbb{Q}} \subset \mathbb{C}$$

be the n distinct embeddings of K into the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ which we embed into the field of complex numbers. This yields an embedding

$$j : K \hookrightarrow K_{\mathbb{C}} := \prod_{k=1}^{n} \mathbb{C} = \mathbb{C}^{\{\sigma_1,\dots,\sigma_n\}}, x \mapsto (\sigma_1(x), \dots, \sigma_n(x)) = (x_{\sigma_1}, \dots, x_{\sigma_n}).$$

The Galois group of $\mathbb{C}$ over $\mathbb{R}$ $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \overline{\ } \rangle \cong C_2$ acts on $K_{\mathbb{C}}$ via

$$\overline{(x_{\sigma_1}, \dots, x_{\sigma_n})} = (y_{\sigma_1}, \dots, y_{\sigma_n}) \textit{ with } y_{\sigma_j} = \overline{x_{\overline{\sigma_j}}}.$$

Here $\overline{\sigma_j} : K \to \mathbb{C}, \overline{\sigma_j}(x) := \overline{\sigma_j(x)}$. We call $\sigma : K \to \mathbb{C}$ **real**, *if $\sigma = \overline{\sigma}$ and* **complex** *if $\sigma \neq \overline{\sigma}$. Let*

$$K_{\mathbb{R}} := \mathrm{Fix}_{\langle \overline{\ } \rangle}(K_{\mathbb{C}}) := \{(x_\sigma) \in K_{\mathbb{C}} \mid x_{\overline{\sigma}} = \overline{x_\sigma}\}.$$

Then $j(K) \subset K_{\mathbb{R}}$.

Example. $K \cong \mathbb{Q}[X]/(X^3-2) = \mathbb{Q}[\sqrt[3]{2}]$. Let $\alpha \in K$ with $\alpha^3 = 2$. Then α is a primitive element of K and the embeddings of K into $\mathbb{C}$ are given by

$$\sigma_1 : \alpha \mapsto \sqrt[3]{2} (\in \mathbb{R}),\ \sigma_2 : \alpha \mapsto \zeta_3 \sqrt[3]{2},\ \sigma_3 = \overline{\sigma_2} : \alpha \mapsto \zeta_3^2 \sqrt[3]{2}.$$

Then σ_1 is real, σ_2 and σ_3 are complex and the action of the complex conjugation on $K_{\mathbb{C}}$ is

$$\overline{(x,y,z)} = (\overline{x}, \overline{z}, \overline{y}).$$

Therefore we obtain $K_{\mathbb{R}} = \{(a, b+ic, b-ic) \mid a,b,c \in \mathbb{R}\}$.

Remark 2.6. *The mappings*

$$\begin{array}{ll} N : K_{\mathbb{C}} \to \mathbb{C}, & N(x_1,\ldots,x_n) = \prod_{i=1}^n x_i \\ S : K_{\mathbb{C}} \to \mathbb{C}, & S(x_1,\ldots,x_n) = \sum_{i=1}^n x_i \end{array}$$

extend norm and trace, in the sense that for any $\alpha \in K$

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) = N(j(\alpha)),\ S_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) = S(j(\alpha)).$$

Remark 2.7. *Let* $\rho_1,\ldots,\rho_r : K \to \mathbb{R} \subset \mathbb{C}$ *be the real places of* K *and* $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$ *the complex places of* K*, so* $n = [K : \mathbb{Q}] = r + 2s$*. Then*

$$m : K_{\mathbb{R}} \to \mathbb{R}^{r+2s}, (x_{\rho_1},\ldots,x_{\rho_r}, x_{\sigma_1}, x_{\overline{\sigma_1}}, \ldots, x_{\sigma_s}, x_{\overline{\sigma_s}}) \mapsto (x_{\rho_1},\ldots,x_{\rho_r}, \Re(x_{\sigma_1}), \Im(x_{\sigma_1}), \ldots, \Re(x_{\sigma_s}), \Im(x_{\sigma_s}))$$

is a $\mathbb{R}$*-linear isomorphism that maps the restriction of the standard inner product* $\langle x,y\rangle := \sum_{i=1}^n x_i \overline{y_i}$ *on* $K_{\mathbb{C}}$ *to the canonical metric (***Minkowski metric***)*

$$(x,y) := \sum_{i=1}^r x_i y_i + 2 \sum_{j=r+1}^{r+2s} x_j y_j.$$

Proof. Wlog $r = 0, s = 1$, so $K_{\mathbb{R}} = \{(x, \overline{x}) \mid x \in \mathbb{C}\}$. Then

$$\langle (x,\overline{x}), (y, \overline{y})\rangle = x\overline{y} + \overline{x}y = 2(\Re(x)\Re(y) + \Im(x)\Im(y)).$$

□

In the following we will treat all lattices in $K_{\mathbb{R}}$ as lattices in $(\mathbb{R}^{r+2s}, (,))$ with respect to the positive definite Minkowski metric.

Theorem 2.8. *If* $0 \neq \mathcal{A} \trianglelefteq \mathbb{Z}_K$ *is an ideal in* $\mathbb{Z}_K$ *then* $\Gamma := j(\mathcal{A})$ *is a full lattice in* $K_{\mathbb{R}}$ *with covolume*

$$\mathrm{covol}(\Gamma) = \sqrt{|d_K|}|\mathbb{Z}_K/\mathcal{A}|.$$

In particular $\det(j(\mathbb{Z}_K)) = |d_K|$ *is the absolute value of the discriminant of* K.

Proof. Let $B = (\alpha_1, \ldots, \alpha_n)$ be an integral basis of $\mathcal{A}$. and let $A := (\sigma_i(\alpha_j))_{i,j=1}^n \in \mathbb{C}^{n\times n}$. Then the Gram matrix of B with respect to the trace bilinear form S is

$$M_B(S) = A^{tr} A.$$

So $d_{\mathcal{A}} = \det(M_B(S)) = \det(A)^2 = [\mathbb{Z}_K : \mathcal{A}]^2 d_K$. On the other hand

$$(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k=1}^n = (\sum_{\ell=1}^n \sigma_\ell(\alpha_i)\overline{\sigma_\ell}(\alpha_k))_{i,k=1}^n = \overline{A}^{tr} A$$

and therefore $\mathrm{vol}(K_{\mathbb{R}}/\Gamma) = \sqrt{\det(\overline{A}^{tr} A)} = |\det(A)| = \sqrt{|d_K|}[\mathbb{Z}_K : \mathcal{A}]$. □

Definition 2.9. *For any nonzero integral ideal $0 \neq \mathcal{A} \trianglelefteq \mathbb{Z}_K$ we define the* **norm** *of $\mathcal{A}$ to be $N(\mathcal{A}) := [\mathbb{Z}_K : \mathcal{A}]$.*

Clearly for $a \in \mathbb{Z}_K$ this is the usual norm $N_{K/\mathbb{Q}}(a) = N((a))$.

Remark 2.10. *For any two nonzero integral ideals $\mathcal{A}, \mathcal{B}$ we have*

$$N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$$

so N defines a group homomorphism

$$N : J_K \to \mathbb{R}_{>0}, N(\wp_1^{n_1} \cdots \wp_s^{n_s}) := N(\wp_1)^{n_1} \cdots N(\wp_s)^{n_s}.$$

Proof. Since $\mathcal{A}, \mathcal{B}$ have a factorisation into prime ideals it is enough to show the multiplicativity in the following two cases
(a) $\gcd(\mathcal{A}, \mathcal{B}) = 1$: But then $\mathcal{AB} = \mathcal{A} \cap \mathcal{B}$ and by Chinese Remainder Theorem $\mathbb{Z}_K/\mathcal{AB} \cong \mathbb{Z}_K/\mathcal{A} \times \mathbb{Z}_K/\mathcal{B}$ has order

$$N(\mathcal{AB}) = |\mathbb{Z}_K/\mathcal{AB}| = |\mathbb{Z}_K/\mathcal{A}||\mathbb{Z}_K/\mathcal{B}| = N(\mathcal{A})N(\mathcal{B}).$$

(b) powers of prime ideals $N(\wp^n) = N(\wp)^n$. For any prime ideal $0 \neq \wp \trianglelefteq \mathbb{Z}_K$, the ideals of $\mathbb{Z}_K/\wp^n$ are precisely $\wp^i/\wp^n$ with $0 \leq i \leq n$. This yields a composition series

$$\mathbb{Z}_K \supseteq \wp \supseteq \wp^2 \supseteq \ldots \supseteq \wp^{n-1} \supseteq \wp^n$$

where all composition factors $\wp^i/\wp^{i+1}$ are isomorphic to $\mathbb{Z}_K/\wp$. More precisely for any $p \in \wp \setminus \wp^2$ multiplication by p yields an isomorphism between $\mathbb{Z}_K/\wp$ and $\wp/\wp^2$, etc. So $|\mathbb{Z}_K/\wp| = |\wp/\wp^2| = \ldots = |\wp^{n-1}/\wp^n| = N(\wp)$ and $|\mathbb{Z}_K/\wp^n| = \prod_{i=1}^n |\wp^{i-1}/\wp^i| = N(\wp)^n$. □

3 Finiteness of the ideal class group.

Remark 3.1. *For any $n \in \mathbb{N}$ there are only finitely many integral $\mathbb{Z}_K$-ideals $I \trianglelefteq \mathbb{Z}_K$ with norm $N(I) \leq n$. Here a fractional $\mathbb{Z}_K$-ideal is called* **integral***, if it is contained in $\mathbb{Z}_K$, hence if it is an ideal in the usual sense.*

Proof. Let $I \trianglelefteq \mathbb{Z}_K$ be an ideal with norm $N(I) = |\mathbb{Z}_K/I| = n$. Then $n\mathbb{Z}_K \subseteq I \subseteq \mathbb{Z}_K$ and $I/n\mathbb{Z}_K$ is one of the finitely many subgroups of the finite abelian group $\mathbb{Z}_K/n\mathbb{Z}_K \cong \mathbb{Z}/n\mathbb{Z}^{[K:\mathbb{Q}]}$. □

General assumption:
K is a number field of degree $[K : \mathbb{Q}] = r + 2s = n$,

$$\sigma_1, \dots, \sigma_r : K \to \mathbb{R} \subset \mathbb{C}, \sigma_{r+1}, \dots \sigma_{r+s}, \sigma_{r+s+1} = \overline{\sigma_{r+1}}, \dots, \sigma_{r+2s} = \overline{\sigma_{r+s}} : K \to \mathbb{C}$$

the real resp. complex embeddings of K into $\mathbb{C}$. These are also called the **places** of K.

Theorem 3.2. *Let $0 \neq \mathcal{A} \trianglelefteq \mathbb{Z}_K$ be an ideal. For any $i \in \{1, \dots, r+s\}$ let $c_i = c_{\sigma_i} \in \mathbb{R}_{>0}$ such that $c_{r+i} = c_{r+s+i}$ for all $1 \leq i \leq s$ ($c_{\sigma_i} = c_{\overline{\sigma_i}}$) and*

$$\prod_{i=1}^{r+2s} c_i > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathcal{A}).$$

Then there is some $0 \neq a \in \mathcal{A}$ such that $|\sigma_i(a)| < c_{\sigma_i}$ for all $1 \leq i \leq n$. In particular any integral ideal contains an element $0 \neq a \in \mathcal{A}$, such that $|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathcal{A})$.

Proof. Let $X := \{(x_1, \dots, x_n) \in K_{\mathbb{R}} \mid |x_i| \leq c_i \text{ for all } 1 \leq i \leq n\}$. Then X and its image $m(X)$ is convex and centrally symmetric, where $m : K_{\mathbb{R}} \to \mathbb{R}^{r+2s}$,

$$(x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}, \underbrace{x_{r+s+1}, \dots, x_{r+2s}}_{=\overline{x_{r+1}}, \dots, \overline{x_{r+s}}}) \mapsto (x_1, \dots, x_r, \Re(x_{r+1}), \Im(x_{r+1}), \dots, \Re(x_{r+s}), \Im(x_{r+s}))$$

and $\mathbb{R}^{r+2s}$ is endowed with the positive definite bilinear form $(x, y) := \sum_{i=1}^r x_i y_i + 2 \sum_{j=1}^{2s} x_{r+j} y_{r+j}$. With respect to this metric, the volume of $m(X)$ is

$\mathrm{vol}(m(X)) = \mathrm{vol}\{(x_1, \dots, x_n) \in \mathbb{R}^{r+2s} \mid |x_i| \leq c_i, x_{r+2j-1}^2 + x_{r+2j}^2 \leq c_{r+j}^2 \text{ for all } 1 \leq i \leq r, 1 \leq j \leq s\} =$

$(\prod_{i=1}^r 2c_i) \prod_{j=1}^s 2\pi c_{r+j}^2 = 2^{r+s} \pi^s \prod_{i=1}^n c_i > 2^{r+s} \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathcal{A}) = 2^{r+2s} \mathrm{vol}(\mathbb{R}^n/\Gamma)$ where $\Gamma = j(\mathcal{A})$. By Minkowski's lattice point theorem there is some non-zero element in $m(X) \cap m(j(\mathcal{A})) = m(X \cap j(\mathcal{A}))$. □

Theorem 3.3. *Recall that the class group of K is $\mathrm{Cl}_K := J_K/P_K$ is the group of equivalence classes of fractional $\mathbb{Z}_K$-ideals in K, where two ideals $\mathcal{A}$ and $\mathcal{B}$ are called equivalent, if they differ by a principal ideal, so if there is $0 \neq x \in K$ such that $(x)\mathcal{A} = \mathcal{B}$.*

(a) Any ideal class $[\mathcal{A}] \in \mathrm{Cl}_K$ contains an integral ideal $\mathcal{A}_1 \in [\mathcal{A}]$, $\mathcal{A}_1 \trianglelefteq \mathbb{Z}_K$ such that

$$N(\mathcal{A}_1) \leq M_K := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

(b) The **class number of** *K, $h_K := |\mathrm{Cl}_K|$ is finite.*

Proof. (a) implies (b) since there are only finitely many integral ideals of norm $\leq M_K$.
To see (a), let $\mathcal{A} \trianglelefteq \mathbb{Z}_K$ an integral representative of the ideal class. By Theorem 3.2 there is some $0 \neq a \in \mathcal{A}$, such that $|N(a)| \leq M_K N(\mathcal{A})$. Let $\mathcal{A}_1 := (a)\mathcal{A}^{-1}$. Then $\mathcal{A}_1$ is integral, in the class of $\mathcal{A}^{-1}$ and $N(\mathcal{A}_1) = |N(a)| N(\mathcal{A})^{-1} \leq M_K$. □

Example: $K = \mathbb{Q}[\sqrt{5}]$, $d_K = 5$, $r = 2, s = 0$, so $M_K = \sqrt{5} < 3$ and any ideal class contains some integral ideal of norm 1 or 2.

Norm 1 Then the ideal is $(1) = \mathbb{Z}_K$ and therefore principal.

Norm 2 If $N(I) = 2$, $I \trianglelefteq \mathbb{Z}_K$, then $2\mathbb{Z}_K \subseteq I \subseteq \mathbb{Z}_K$. The ring $\mathbb{Z}_K/2\mathbb{Z}_K \cong \mathbb{F}_2[x]/(x^2+x-1) \cong \mathbb{F}_4$ has no nontrivial ideals, so there are no ideals of norm 2 (note that $N(2\mathbb{Z}_K) = 4$).

So we have seen that $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is a principal ideal domain.

Example: $K = \mathbb{Q}[\sqrt{15}]$, $d_K = 60$, $r = 2, s = 0$, so $M_K = 2\sqrt{15} < 8$ and we have to consider all integral ideals of norm 2,3,4,5,7.

Norm 2 $\wp_2 = (2, 1 + \sqrt{15})$ is the unique ideal of norm 2. ($\mathbb{Z}_K/2\mathbb{Z}_K \cong \mathbb{F}_2[X]/(X^2 - 15) \cong \mathbb{F}_2[X]/(X+1)^2$ has a unique non-trivial ideal). $\wp_2$ is not a principal ideal since otherwise $\mathbb{Z}[\sqrt{15}]$ contains an element $a = x + y\sqrt{5}$ of norm $N(a) = x^2 - 15y^2 = \pm 2$. Then $x^2 \equiv_5 \pm 2$ which is a contradiction.

Norm 3 $\wp_3 = (3, \sqrt{15})$ but $\wp_2\wp_3 = (3 + \sqrt{15})$ is a principal ideal.

Norm 4 $2\mathbb{Z}_K = \wp_2^2$.

Norm 5 $\wp_5 = (5, \sqrt{15})$ but $\wp_3\wp_5 = (\sqrt{15})$ is a principal ideal.

Norm 7 $\wp_7 = (7, 1 + \sqrt{15})$, $\wp_7' = (7, 1 - \sqrt{15})$. These ideals satisfy $\wp_7\wp_2 = (1 + \sqrt{15})$ and $\wp_7'\wp_2 = (1 - \sqrt{15})$.

So in total $\mathrm{Cl}_K = \langle [\wp_2] \rangle \cong C_2$.

Example: $K = \mathbb{Q}[\sqrt{5}]$, $O = \mathbb{Z}[\sqrt{5}]$, $d_O = 20$, $r = 2, s = 0$, so $M_O = 2\sqrt{5} < 5$

Norm 2 $\wp_2 = (2, 1 + \sqrt{5}) = 2\mathbb{Z}_K$ is the unique ideal of norm 2 in O. Note that $\wp_2^2 = 2\wp_2$ so $\wp_2$ is not invertible as an O-ideal.

Norm 3 no ideal of norm 3 as $X^2 - 5$ is irreducible in $\mathbb{F}_3[X]$.

Norm 4 Let $X \trianglelefteq O$ be of index 4. Then $\mathbb{Z}_K X \trianglelefteq \mathbb{Z}_K$ is of index 4 or 8 and hence $\mathbb{Z}_K X = 2\mathbb{Z}_K = \wp_2$. So we have $2\wp_2 \subset X \subset \wp_2$ and need to enumerate all such O-modules. Now $\wp_2 \cong \mathbb{Z}^2$ with basis $B = (2, 1 + \sqrt{5})$ and we compute

$$ {}^{B}\sqrt{5}^{B} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}. $$

So all submodules of $\wp_2/2\wp_2$ are O-ideals; these are

$$ 2O, (1 + \sqrt{5})O, (1 - \sqrt{5})O $$

and hence all isomorphic to O.

Remark 3.4. *Since any ideal is a product of prime ideals, the class group is generated by the classes of prime ideals $\wp_i \trianglelefteq \mathbb{Z}_K$ such that $N(\wp_i) \leq M_K$. Note that the norm of the prime ideal $\wp$ is a power of the prime p with $p\mathbb{Z} = \wp \cap \mathbb{Z}$.*

Remark 3.5. *What is known about class numbers? Not much.*
If $K = \mathbb{Q}[\sqrt{d}]$ ($d < 0$, $d \in \mathbb{Z}$ square free) is an imaginary quadratic number field then $h_K = 1$ if and only if $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.
One conjectures that there are infinitely many real quadratic number fields K (so $r = 2, s = 0$) for which $h_K = 1$, but one cannot even prove that there are infinitely many number fields (without restricting the degree) with class number 1.

4 Dirichlet's theorem

We start with some preliminary technical remarks on lattices. Let $V = (\mathbb{R}^n, (,))$ always denote the Euclidean space of dimension n.

Lemma 4.1. *A subgroup $\Gamma \leq V$ is a lattice (i.e. there are $\mathbb{R}$-linear independent elements $(v_1, \ldots, v_m) \in V^m$ such that $\Gamma = \langle v_1, \ldots, v_m \rangle_{\mathbb{Z}}$) if and only if Γ is discrete, which means that for all $\gamma \in \Gamma$ there is some $\epsilon > 0$ such that $B_\epsilon(\gamma) \cap \Gamma = \{\gamma\}$.*

Proof. Let $V_0 := \langle \Gamma \rangle_{\mathbb{R}}$ and $B := (\gamma_1, \ldots, \gamma_m) \in \Gamma^m$ a basis of V_0. Put $\Gamma_0 := \langle \gamma_1, \ldots, \gamma_m \rangle_{\mathbb{Z}}$. Then Γ_0 is a lattice. We prove that Γ/Γ_0 is finite, because then Γ is finitely generated and by the main theorem on f.g. abelian groups it is free of the same rank as Γ_0.
Let $E(B)$ be the fundamental parallelotope defined by B, then $\mathrm{vol}(E(B))$ is finite and $V_0 = \cup_{\gamma \in \Gamma_0} E(B) + \gamma$. Since $E(B)$ is compact and Γ is discrete, there are only finitely many points in $E(B) \cap \Gamma = \{x_1, \ldots, x_a\}$. But then $\Gamma = \cup_{i=1}^a x_i + \Gamma_0$ and hence $|\Gamma/\Gamma_0| \leq a$. □

Lemma 4.2. *Let $\Gamma \leq V$ be a lattice. Then Γ is a full lattice (i.e. contains a basis of V), if and only if Γ has finite covolume in V, if and only if there is some bounded set $M \subset V$ such that $V = \cup_{\gamma \in \Gamma} M + \gamma$.*

Proof. If Γ is a full lattice, and B a lattice basis of Γ, then $M := E(B)$ is such a bounded set.
On the other hand assume that Γ has not full rank in V and choose some $v \in V \setminus \langle \Gamma \rangle_{\mathbb{R}}$. If $V = \cup_{\gamma \in \Gamma} M + \gamma$ for some bounded set M, then for any $n \in \mathbb{N}$ there is some $a_n \in M$ such that $nv = a_n + \gamma_n$ for some $\gamma_n \in \Gamma$. Since M is bounded, $\lim_{n \to \infty} \frac{1}{n} a_n = 0$, so

$$v = \frac{1}{n}(a_n + \gamma_n) = \lim_{n \to \infty} \frac{1}{n} a_n + \lim_{n \to \infty} \frac{1}{n} \gamma_n = \lim_{n \to \infty} \frac{1}{n} \gamma_n \in \langle \Gamma \rangle_{\mathbb{R}}$$

because subspaces are closed. □

We now want to apply these basic facts on lattices to study the unit group $\mathbb{Z}_K^*$ of the ring of integers in some algebraic number field.

Recall that the places $\sigma_1, \ldots, \sigma_{r+2s}$ of K define an embedding

$$j : K \hookrightarrow K_{\mathbb{R}} = \{(x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y_1}, \ldots, \overline{y_s}) \mid x_i \in \mathbb{R}, y_i \in \mathbb{C}\}$$

and that we identified $K_{\mathbb{R}}$ via the mapping m with $\mathbb{R}^{r+2s}$ where

$$m : K_{\mathbb{R}} \to \mathbb{R}^{r+2s}, (x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y_1}, \ldots, \overline{y_s}) \mapsto (x_1, \ldots, x_r, \Re(y_1), \Im(y_1), \ldots, \Re(y_s), \Im(y_s)).$$

Note that j is a ring homomorphism so it defines a group homomorphism $j : K^* \to K_{\mathbb{R}}^*$. Define the logarithm

$$\ell : K_{\mathbb{R}}^* \to \mathbb{R}^{r+s}, \ell(x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y_1}, \ldots, \overline{y_s}) := (\log(|x_1|), \ldots, \log(|x_r|), \log(|y_1|^2), \ldots, \log(|y_s|^2)).$$

Then ℓ is again a group homomorphism from the multiplicative group $K_{\mathbb{R}}^*$ to the additive group of the vector space $\mathbb{R}^{r+s}$.

Theorem 4.3. *Let $\lambda := \ell \circ j : \mathbb{Z}_K^* \to \mathbb{R}^{r+s}$. Then λ is a group homomorphism with*

$$\ker(\lambda) = \mu_K = \{z \in K \mid z^a = 1 \textit{ for some } a \in \mathbb{N}\}$$

the group of roots of unity in K. Let $\Gamma := \lambda(\mathbb{Z}_K^*) \leq \mathbb{R}^{r+s}$.

Proof. It is clear that λ is a group homomorphism. The image of λ is a subgroup of the additive group of a vector space, hence torsion free, so all elements of $\mathbb{Z}_K^*$ that have finite order lie in the kernel of λ and therefore $\mu_K \subseteq \ker(\lambda)$. To see equality let $x \in \mathbb{Z}_K^*$ be such that $\lambda(x) = 0$. Then

$$j(x) \in X := \{(x_1, \ldots, x_r, y_1, \ldots, y_s) \in K_{\mathbb{R}} \mid |x_i| = 1, |y_i|^2 = 1\}.$$

So $j(\ker(\lambda))$ is contained in a bounded subset of $K_{\mathbb{R}}$. On the other hand $j(x) \in j(\mathbb{Z}_K) =: \Lambda$ is contained in the lattice $j(\mathbb{Z}_K) = \langle j(b_1), \ldots, j(b_n)\rangle_{\mathbb{Z}}$ for any integral basis $(b_1, \ldots, b_n)$ of K. But $\Lambda \cap X$ is always finite, so $\ker(\lambda)$ is finite and hence a torsion group, so contained in μ_K. □

Remark 4.4. *Since the norm is multiplicative $\mathbb{Z}_K^* = \{x \in \mathbb{Z}_K \mid N_{K/\mathbb{Q}}(x) = \pm 1\}$. Note that if $x \in \mathbb{Z}_K$ satisfies $N_{K/\mathbb{Q}}(x) = 1$ then $x^{-1} \in \mathbb{Z}[x]$ can be obtained from the minimal polynomial of x.*
Let $U_K := \{x \in K \mid N(x) = \pm 1\}$.
Then $\lambda(\mathbb{Z}_K^*) \subseteq \lambda(U_K) = H := \{(a_1, \ldots, a_{r+s}) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r+s} a_i = 0\} \cong \mathbb{R}^{r+s-1}$.

Theorem 4.5. *Let $\Gamma := \lambda(\mathbb{Z}_K^*) \leq \mathbb{R}^{r+s}$. Then $\Gamma \leq H := \{(a_1, \ldots, a_{r+s}) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r+s} a_i = 0\} \cong \mathbb{R}^{r+s-1}$ is a full lattice in H.*

Proof. We have to show that Γ is a full lattice in H. It is clear that $\Gamma \leq H$ is a subgroup. We first show that Γ is discrete. To this aim we show that for any $c > 0$ the set

$$X_c := \{(a_m) \in \mathbb{R}^{r+s} \mid |a_m| < c \text{ for all } m\}$$

meets Γ in only finitely many points. But

$$\ell^{-1}(X_c) = \{(x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y}_1, \ldots, \overline{y}_s) \in K_{\mathbb{R}} \mid e^{-c} \leq |x_i| \leq e^c, e^{-c} \leq |y_i|^2 \leq e^c\}$$

is bounded and therefore contains only finitely many points of the lattice $\Lambda = j(\mathbb{Z}_K) \subset j(\mathbb{Z}_K^*)$. Therefore also $|\Gamma \cap X_c| < \infty$.
We now show that Γ has finite covolume in H: Choose $c_1, \ldots, c_r, d_1, \ldots, d_s \in \mathbb{R}_{>0}$ such that

$$\prod_{i=1}^{r} c_i \prod_{j=1}^{s} d_j^2 =: C > M_K.$$

Let $X := \{(x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y}_1, \ldots, \overline{y}_s) \in K_\mathbb{R} \mid |x_i| < c_i, |y_j|^2 < d_j^2\}$. Then $X \subset K_\mathbb{R}$ is a bounded set.

Since there are only finitely many ideals of a given norm in $\mathbb{Z}_K$ there are $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}_K \setminus \{0\}$ such that for any element $\alpha \in \mathbb{Z}_K$ with $|N(\alpha)| \leq C$ there is some unit $u \in \mathbb{Z}_K^*$ and some $1 \leq i \leq N$ such that $\alpha = u\alpha_i$.

Let $U := \{y \in K_\mathbb{R}^* \mid N(y) = \pm 1\} \leq K_\mathbb{R}^*$. Then $\ell(U) = H$ and U is the full preimage of H under ℓ. Put

$$T := U \cap \bigcup_{i=1}^{N} X j(\alpha_i^{-1}).$$

We then claim that $U = \cup_{\epsilon \in \mathbb{Z}_K^*} T j(\epsilon)$.
Let $y \in U$. Then $Xy^{-1} = \{x \in K_\mathbb{R} \mid |x_i| \leq c_i'\}$ where $c_i' = c_i |y_i|^{-1}$. Since $\prod_i |y_i| = N(y) = 1$ also $\prod_i c_i' = \prod_i c_i = C$. By Minkowski's theorem there is some $0 \neq a \in \mathbb{Z}_K$ such that $j(a) \in Xy^{-1}$, so $j(a) = xy^{-1}$ for some $x \in X$. This means that $|N_{K/Q}(a)| < C$ so there is some $u \in \mathbb{Z}_K^*$ and some $i \in \{1, \ldots, N\}$ such that $a = u\alpha_i$. Then

$$y = xj(a)^{-1} = xj(\alpha_i)^{-1} j(u)^{-1} \in Tj(u^{-1}).$$

□

Corollary 4.6. *Let $t := r + s - 1$. Then there are $\epsilon_1, \ldots, \epsilon_t \in \mathbb{Z}_K^*$ and $\mu \in \mu_K$ such that*

$$\mathbb{Z}_K^* = \langle \mu \rangle \times \langle \epsilon_1, \ldots, \epsilon_t \rangle \cong C_{|\mu_K|} \times \mathbb{Z}^{r+s-1}.$$

The ϵ_i are called **fundamental units** *of K.*

Example. $K = \mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ then $\mathbb{Z}_K^* = \langle -1 \rangle \times \langle \frac{1+\sqrt{5}}{2} \rangle$.

Definition 4.7. *A subset $\Gamma \subset K$ is called an* **lattice** *in K, if there is some $\mathbb{Q}$-basis B of K such that $\Gamma = \langle B \rangle_\mathbb{Z}$.*
A subset $O \subset K$ is called an **order** *in K, if O is a subring of K that is a lattice.*

Example. If $\Gamma \subset K$ is a lattice then

$$O(\Gamma) := \{x \in K \mid x\Gamma \subseteq \Gamma\}$$

is an order in K.

Clearly any order O is consists of integral elements and hence is contained in the unique maximal order $\mathbb{Z}_K$ of K. Since O also contains a basis of K, the index $|\mathbb{Z}_K/O|$ is finite. Moreover $O^* = \{x \in O \mid N(x) = \pm 1\}$.

Theorem 4.8. *If O is an order in K, then $O^* \leq \mathbb{Z}_K^*$ is a subgroup of finite index.*

Proof. The same proof as above proves that also O^* has $t = r + s - 1$ fundamental units. □

The Regulator

Definition 4.9. *Let K be a number field and σ_i $(1 \leq i \leq r+s)$ a complete set of pairwise non- conjugate embeddings of K in $\mathbb{C}$. Then the* **regulator** *of a set $\{\epsilon_1, \epsilon_2, ..., \epsilon_{r+s-1}\}$ of $r+s-1$ elements in K^* of norm ± 1 is defined as*

$$Reg(\epsilon_1, \epsilon_2, ..., \epsilon_{r+s-1}) = \det(n_i \log|\sigma_i(\epsilon_j)|)_{i,j=1}^{r+s-1}.$$

Here the integer $n_i \in \{1, 2\}$ equals 1 if σ_i is a real embedding and 2 otherwise. The regulator Reg(R) of an order R in K is the regulator of a system of fundamental units for R^*. We put Reg(R) = 1 if R^* is finite, i.e., if R is either $\mathbb{Z}$ or an imaginary quadratic order. The regulator of K is $R(K)$ =Reg($\mathbb{Z}_K$).

By the Dirichlet unit theorem, regulators of orders do not vanish. Unlike the discriminant of the order, which is an integer, the regulator of an order is a positive real number that is usually transcendental as it is an expression in terms of logarithms of algebraic numbers.

A few formulas relating regulator $R(K)$, class number $h(K)$, number of roots of unity $|\mu_K| =: \omega(K)$ and discriminant $|d(K)|$. We keep the notation $[K : \mathbb{Q}] = n = r + 2s$.

Theorem 4.10. *Let $\zeta_K(z) := \sum_A \frac{1}{N(A)^z}$ denote the Dedekind zeta function of K, where the sum is over all non-zero integral ideals of $\mathbb{Z}_K$. Then ζ_K has an analytic continuation to $\mathbb{C}$ with a simple pole at $z = 1$.*

(a) $\lim_{z\to 0} z^{-(r+s-1)}\zeta_K(z) == h(K)R(K)\omega(K)^{-1}$.

(b) $\lim_{z\to 1}(z-1)\zeta_K(z) = 2^r(2\pi)^s \frac{h(K)R(K)}{\omega(K)\sqrt{|d(K)|}}$.

(c) $\lim_{x\to\infty} \frac{N_K(x)}{x} = 2^r(2\pi)^s \frac{h(K)R(K)}{\omega(K)\sqrt{|d(K)|}}$ *where $N_K(x)$ denotes the number of integral ideals of $\mathbb{Z}_K$ of norm $\leq x$.*

5 Quadratic number fields

Let $K = \mathbb{Q}[\sqrt{d}]$, $d \in \mathbb{Z}$, $d \neq 1, 0$ square-free be a quadratic number-field (i.e. an extension of $\mathbb{Q}$ of degree 2). Then $\mathbb{Z}_K = \mathbb{Z}[\omega]$ with $\omega := \begin{cases} \sqrt{d} & d \equiv_4 2, 3 \\ \frac{1+\sqrt{d}}{2} & d \equiv_4 1 \end{cases}$. Note that $d_K = d$ if $d \equiv_4 1$ and $d_K = 4d$ otherwise, in particular d_K is either 0 or 1 modulo 4.

Theorem 5.1. *Let Γ be a full lattice in K.*
(a) There is some $m \in \mathbb{Q}$ and $\gamma \in K$ such that $\Gamma = \langle m, m\gamma\rangle_{\mathbb{Z}}$.
(b) Let $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$, $a > 0$, such that $a\gamma^2 + b\gamma + c = 0$. Then $a\gamma = h + k\omega \in \mathbb{Z}_K$ and

$$O(\Gamma) := \{x \in K \mid x\Gamma \subseteq \Gamma\} = \langle 1, a\gamma\rangle_{\mathbb{Z}} = \langle 1, k\omega\rangle_{\mathbb{Z}}.$$

Proof. (a) Is just the Hermite normal form for integral matrices: If $\Gamma = \langle \alpha, \beta \rangle_{\mathbb{Z}}$, then there are $x, y \in \mathbb{Q}$ such that $1 = x\alpha + y\beta$. Choose $m \in \mathbb{Q}$ such that $u := mx$ and $v := my$ both lie in $\mathbb{Z}$ and $\gcd(u, v) = 1$. Then there are $r, s \in \mathbb{Z}$ such that $1 = us - rv$. Put

$$\gamma := \frac{r\alpha + s\beta}{m}, \text{ then } \Gamma = \langle m, m\gamma \rangle_{\mathbb{Z}}.$$

(b) Clearly $O(\langle m, m\gamma \rangle_{\mathbb{Z}}) = O(\langle 1, 1\gamma \rangle_{\mathbb{Z}})$, so wlog assume that $m = 1$. Then $O(\Gamma)$ contains $a\gamma$, since both, $a\gamma$ and $a\gamma^2 = -b\gamma - c$ lie in Γ. On the other hand let $x + y\gamma =: \delta \in O(\Gamma)$. Then $x + y\gamma \in \Gamma$, so $x, y \in \mathbb{Z}$ and $y\gamma \in O(\Gamma)$, so $y\gamma^2 \in \Gamma$ implying that y is divisible by a. □

Corollary 5.2. *Let O be an order in K. Then $O = O_f := \langle 1, f\omega \rangle$ for some $f \in \mathbb{N}$. This number f is called the* **conductor** *(***Führer***) of O.*
We have $f\mathbb{Z}_K \subset O_f \subset \mathbb{Z}_K$ and $d(O_f) = f^2 d_K$.

Remark 5.3. *Let $\langle \sigma \rangle = \mathrm{Gal}(K/\mathbb{Q})$ (so $\sigma(\sqrt{d}) = -\sqrt{d}$). Then for all $a \in K$ we have $\sigma(a) = S_{K/\mathbb{Q}}(a) - a$ and in particular any order O in K satisfies $\sigma(O) = O$.*

Definition 5.4. *Let $O \subset K$ be an order. Then*

$$\mathcal{M}(O) := \{\Gamma \subseteq K \mid \Gamma \textit{ is a lattice }, O(\Gamma) = O\}$$

Theorem 5.5. *$\mathcal{M}(O)$ is a group with respect to the usual multiplication of ideals. If $\Gamma = \langle m, m\gamma \rangle_{\mathbb{Z}} \in \mathcal{M}(O)$ where $\gamma \in K, m \in \mathbb{Q}, a, b, c \in \mathbb{Z}$ are as in Theorem 5.1 (b), then we define $N(\Gamma) := \frac{m^2}{a}$ and the inverse of Γ is $\Gamma^{-1} = N(\Gamma)^{-1}\sigma(\Gamma)$.*

Proof. Clearly ideal multiplication is associative, commutative, etc.
The unit element in $\mathcal{M}(O)$ is O.
We first show that the elements in $\mathcal{M}(O)$ have an inverse:
Let $\Gamma = \langle m, m\gamma \rangle \in \mathcal{M}(O)$. Since $O(\sigma(\Gamma)) = \sigma(O(\Gamma)) = O$, also the conjugate $\sigma(\Gamma)$ is in $\mathcal{M}(O)$. Moreover

$$\Gamma\sigma(\Gamma) = m^2\langle 1, \gamma, \sigma(\gamma), \gamma\sigma(\gamma) \rangle = N(\Gamma)\langle a, a\gamma, a\sigma(\gamma), a\gamma\sigma(\gamma) \rangle$$

where a, b, c are as in Theorem 5.1 (b). Then $a\gamma^2 + b\gamma + c = 0$ so $b = a\gamma + a\sigma(\gamma)$ and $c = a\gamma\sigma(\gamma)$. In particular

$$\Gamma\sigma(\Gamma) = N(\Gamma)\langle a, b, c, a\gamma \rangle = N(\Gamma)O.$$

We now show that the product of two elements of $\mathcal{M}(O)$ is again in $\mathcal{M}(O)$:
Let $\Gamma_1, \Gamma_2 \in \mathcal{M}(O)$. Then $O \subseteq O(\Gamma_1\Gamma_2)$ by the associativity of ideal multiplication. Moreover

$$O = (\Gamma_1\Gamma_2)(\Gamma_1^{-1}\Gamma_2^{-1}) = N(\Gamma_1)^{-1}N(\Gamma_2)^{-1}(\Gamma_1\Gamma_2)\sigma(\Gamma_1)\sigma(\Gamma_2)$$

so $O(\Gamma_1\Gamma_2) \subseteq O(O) = O$. □

Definition 5.6. *Let O be an order in $K = \mathbb{Q}[\sqrt{d}]$.*
(a) $e(O) := [\mathbb{Z}_K^* : O^*]$.
(b) $K_+ := \{a \in K^* \mid N(a) > 0\}$, $n(O) := [K^* : (K_+O^*)]$.
(c) $\mathrm{Cl}(O) := \mathcal{M}(O)/\{aO \mid a \in K^*\}$ is called the **class group of O**.
(d) $\mathrm{Cl}_0(O) := \mathcal{M}(O)/\{aO \mid a \in K_+\}$ is called the **ray class group of O**.

Remark 5.7. *(a) If $d < 0$ then $K_+ = K^*$, $n(O) = 1$.*
(b) If $d > 0$ then $O^* = \langle -1 \rangle \times \langle \epsilon \rangle$ and $n(O) = 1$ if and only if $N_{K/\mathbb{Q}}(\epsilon) = -1$. Otherwise $n(O) = 2$.
(c) The kernel of the map $\mathrm{Cl}_0(O) \to \mathrm{Cl}(O)$ has order $n(O)$.
(d) Every class $[\Gamma]_0 \in \mathrm{Cl}_0(O)$ has a representative of the form $\Gamma = \langle 1, \gamma \rangle$ with $\gamma = x + y\omega$, $x, y \in \mathbb{Q}$, $y > 0$. Such a $\gamma \in K$ is called **admissible**.

Theorem 5.8. *Let $\gamma_1, \gamma_2 \in K$ be admissible and put $\Gamma_i := \langle 1, \gamma_i \rangle$. Assume that $O(\Gamma_1) = O(\Gamma_2)$. Then*

$$[\Gamma_1]_0 = [\Gamma_2]_0 \in \mathrm{Cl}_0(O) \Leftrightarrow \exists A = \begin{pmatrix} k & \ell \\ m & n \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \text{ such that } \gamma_2 = \frac{k\gamma_1 + \ell}{m\gamma_1 + n}.$$

<u>Proof.</u> $\Rightarrow$: Let $[\Gamma_1]_0 = [\Gamma_2]_0$. Then there is some $\alpha \in K$, $N(\alpha) > 0$ and $A = \begin{pmatrix} k & \ell \\ m & n \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \gamma_2 \\ 1 \end{pmatrix} = A \begin{pmatrix} \alpha\gamma_1 \\ \alpha \end{pmatrix}, \text{ so } \begin{pmatrix} \gamma_2 & \sigma(\gamma_2) \\ 1 & 1 \end{pmatrix} = A \begin{pmatrix} \alpha\gamma_1 & \sigma(\alpha)\sigma(\gamma_1) \\ \alpha & \sigma(\alpha) \end{pmatrix}.$$

Taking the determinant we obtain

$$(\star) \quad \gamma_2 - \sigma(\gamma_2) = \det(A) N(\alpha)(\gamma_1 - \sigma(\gamma_1)).$$

Since γ_1 and γ_2 are admissible, the coefficient of $\sqrt{d}$ is positive on both sides and hence $\det(A) > 0$ (note that $N(\alpha) > 0$ by assumption), so $A \in \mathrm{SL}_2(\mathbb{Z})$. Moreover

$$\gamma_2 = \frac{\gamma_2}{1} = \frac{k\alpha\gamma_1 + \alpha\ell}{m\alpha\gamma_1 + \alpha n} = \frac{k\gamma_1 + \ell}{m\gamma_1 + n}.$$

$\Leftarrow$: Put $\alpha := \frac{1}{m\gamma_1 + n}$. Then

$$\alpha\Gamma_1 = \langle \alpha, \alpha\gamma_1 \rangle = \langle A \begin{pmatrix} \alpha\gamma_1 \\ \alpha \end{pmatrix} \rangle = \langle \gamma_2, 1 \rangle = \Gamma_2.$$

Because of $(\star)$ and $\det(A) = 1$ we obtain $N(\alpha) > 0$. □

Definition 5.9. *Let $\Gamma := \langle 1, \gamma \rangle \in \mathcal{M}(O)$, $\gamma \in K$ admissible and let $a, b, c \in \mathbb{Z}$, $a > 0$, $\gcd(a, b, c) = 1$ such that $a\gamma^2 + b\gamma + c = 0$. Then*

$$F_\gamma := F_\gamma(X, Y) := \frac{1}{N(\Gamma)}(X - \gamma Y)(X - \sigma(\gamma)Y) = aX^2 + bXY + cY^2$$

is called the **binary quadratic form defined by** *γ.*

Then Theorem 5.8 immediately implies

Theorem 5.10. *Let $\Gamma_i = \langle 1, \gamma_i\rangle \in \mathcal{M}(O)$, γ_i admissible $i = 1, 2$. Then*

$$[\Gamma_1]_0 = [\Gamma_2]_0 \in \mathrm{Cl}_0(O) \Leftrightarrow \exists A = \begin{pmatrix} k & \ell \\ m & n \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } F_{\gamma_1}(nX-\ell Y, -mX+kY) = F_{\gamma_2}(X,Y).$$

Proof. Put $N_i := N(\Gamma_i)$. Then

$$N_1 F_{\gamma_1}(nX-\ell Y, -mX+kY) = ((nX-\ell Y)-\gamma_1(-mX+kY))((nX-\ell Y)-\sigma(\gamma_1)(-mX+kY)) =$$

$$(n+m\gamma_1)(n+m\sigma(\gamma_1))(X - \frac{k\gamma_1+\ell}{m\gamma_1+n}Y)(X - \frac{k\sigma(\gamma_1)+\ell}{m\sigma(\gamma_1)+n}Y) = N_1 F_{\gamma_2}(X,Y).$$

□

Definition 5.11. *Let $F = F_{a,b,c} = aX^2 + bXY + cY^2$ be a binary quadratic form.*
(a) $disc(F) := -4ac + b^2 = -\det \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ is called the **discriminant** *of F.*
(b) Two forms $F_{a,b,c}$ and $F_{a'b'c'}$ are called **properly equivalent**, *if there is some $A \in \mathrm{SL}_2(\mathbb{Z})$, such*

$$A \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} A^{tr} = \begin{pmatrix} 2a' & b' \\ b' & 2c' \end{pmatrix}.$$

(c) For any $D \in \mathbb{Z}$ we define

$$Q(D) := \{F_{a,b,c} \mid a,b,c \in \mathbb{Z}, \gcd(a,b,c) = 1, a > 0, -4ac + b^2 = D\}/\,\mathrm{SL}_2(\mathbb{Z})$$

to be the set of proper equivalence classes of binary quadratic forms of discriminant D.

Theorem 5.12. *$\mathrm{Cl}_0(O_f)$ is in bijection with $Q(f^2 d_K)$ by mapping $[\langle 1, \gamma\rangle]_0$ to $[F_\gamma]$ (where γ is admissible).*

Proof. We first show that the map is well defined: If $\Gamma = \langle 1, \gamma\rangle$ and $a\gamma^2 + b\gamma + c = 0$ with $a, b, c \in \mathbb{Z}$, $a > 0$, $\gcd(a, b, c) = 1$ then $O(\Gamma) = \langle 1, a\gamma\rangle$ has discrimimant

$$d(O(\Gamma)) = \det \begin{pmatrix} 2 & -b \\ -b & b^2 - 2ac \end{pmatrix} = -4ac + b^2.$$

Now the inverse bijection is given by assigning to $F := F_{a,b,c}$ the admissible root γ of $F(X, 1)$. Then $F(X,Y) = a(X - \gamma Y)(X - \sigma(\gamma)Y)$ with $\gamma \in \mathbb{Q}[\sqrt{disc(F)}] = \mathbb{Q}[\sqrt{f^2 d_K}] = K$. □

5.1 Imaginary quadratic number fields.

Theorem 5.13. *Let $D = f^2 d_K < 0$. Then*

$$R(D) := \{F_{a,b,c} \mid a > 0, -4ac+b^2 = D, a,b,c \in \mathbb{Z}, \gcd(a,b,c) = 1, |b| \leq a \leq c, \text{ and } b > 0 \text{ if } a = c \text{ or } |b| = a\}$$

is a system of representatives for $Q(D)$.

Proof. Let $F_{a,b,c} \in [F_{a,b,c}] \in Q(D)$ such that a is minimal. Then $a \leq c$ since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2c & -b \\ -b & 2a \end{pmatrix}$$

Let $k := \lfloor \frac{a-b}{2a} \rfloor$. Then

$$\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2a & b+2ak \\ b+2ak & 2(ak^2+bk+c) \end{pmatrix}$$

with $b' = b + 2ak \in [-a, a]$, $c' = ak^2 + bk + c$ and $F_{a,b',c'} \in R(D)$.
On the other hand any two forms in $Q(D)$ are inequivalent under the action of $SL_2(\mathbb{Z})$ (exercise). □

Remark 5.14. *If $F_{a,b,c} \in R(D)$ then $a \leq \sqrt{|D|/3}$ because $|D| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$.*

Example. $D = -47$, then $a \leq \sqrt{47/3} < 4$, so $a = 1, 2, 3$. Moreover $-47 = -4ac + b^2$, so b is odd.
$a = 1$: $\begin{pmatrix} 2 & 1 \\ 1 & 24 \end{pmatrix}$.
$a = 2$: $\begin{pmatrix} 4 & 1 \\ 1 & 12 \end{pmatrix}$, $\begin{pmatrix} 4 & -1 \\ -1 & 12 \end{pmatrix}$.
$a = 3$: $\begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix}$, $\begin{pmatrix} 6 & -1 \\ -1 & 8 \end{pmatrix}$.
Let $\omega := \frac{1+\sqrt{-47}}{2}$. Then $\omega^2 - \omega + 12 = 0$ and the corresponding ideals are

$$\mathbb{Z}_K = \langle 1, \omega \rangle, \wp_2 = \langle 2, -\sigma(\omega) \rangle, \wp_2' = \langle 2, \omega \rangle, \wp_3 = \langle 3, -\sigma(\omega) \rangle, \wp_3' = \langle 3, \omega \rangle.$$

The class group has order 5, so $\mathrm{Cl}_K = \langle \wp_2 \rangle \cong C_5$.

Remark 5.15. *The integral ideal $\langle a, a\gamma \rangle \in [\langle 1, \gamma \rangle]_0$ has norm N with $a \mid N \mid a^2$.*

The 2-rank of the class group.

This works similarly also for real quadratic number-fields, but we restrict to imaginary quadratic fields. So let $d \in \mathbb{Z}$ be squarefree, $d > 0$, $K = \mathbb{Q}[\sqrt{-d}]$ with ring of integers $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-d}]$ and discriminant $d_K = 4d$ if $-d \equiv 2, 3 \pmod 4$ resp. $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ and discriminant $d_K = d$ if $-d \equiv 1 \pmod 4$.
Let $\alpha := \sqrt{-d}$ resp. $\alpha := \frac{1+\sqrt{-d}}{2}$ denote a generator of $\mathbb{Z}_K$ and f its minimal polynomial.
Let σ denote the non-trivial Galois automorphism of K, so $\sigma(\sqrt{-d}) = -\sqrt{-d}$.

Lemma 5.16. *A prime p is a divisor of d_K, if and only if there is a prime ideal $\wp \trianglelefteq \mathbb{Z}_K$ such that $\wp^2 = p\mathbb{Z}_K$. (We say that p is* **ramified** *in K.)*

Proof. Let p be a prime. Then the prime ideals dividing p correspond to the maximal ideals of $\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{F}_p[x]/(f)$. This is a uniserial ring, iff f has a double zero mod p which is equivalent to p dividing d_K. (Treat 2 separately, for odd primes, one may replace f by $X^2 + d$ where this is obvious). □

Theorem 5.17. $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2 \cong \Omega_2(\mathrm{Cl}(K)) = \{[I] \mid [I]^2 = 1\} \cong C_2^{g-1}$ *where g is the number of distinct prime divisors of d_K. More precisely for each prime divisor p_j of d_K let $\wp_j$ be the prime ideal dividing $p_j\mathbb{Z}_K$. Then*

$$\Omega_2(\mathrm{Cl}(K)) = \langle [\wp_j] \mid i = 1, \ldots, g \rangle \text{ and } \begin{cases} \wp_1 \cdots \wp_g = \sqrt{-d} & \text{if } -d \equiv 1, 2 \pmod 4 \\ \wp_2 \cdots \wp_g = \sqrt{-d} & \text{if } -d \equiv 3 \pmod 4 \end{cases}$$

where we assumed in the last case that $\wp_1^2 = 2\mathbb{Z}_K$.

It is clear that all ramified prime ideals $\wp$ have order at most 2 in the class group since $\wp^2 = p\mathbb{Z}_K$ is principal. We need to show that
(a) Any class of order 2 contains an ideal $\mathcal{A}$ such that $\mathcal{A} = \sigma(\mathcal{A})$.
(b) Any such σ-invariant ideal is equivalent (in the class group) to a product of ramified prime ideals.
(c) There is no other relation between the classes of the ramified prime ideals.

Lemma 5.18. *(Hilbert 90) Let $a \in K$ such that $N(a) = a\sigma(a) = 1$. Then there is some $b \in K$ such that $a = \frac{\sigma(b)}{b}$.*

Proof. If $a = -1$ then put $b = \sqrt{-d}$. Otherwise let $b := (1 + a)^{-1}$. Then

$$\frac{\sigma(b)}{b} = \frac{1 + a}{1 + \sigma(a)} = \frac{(1 + a)a}{(1 + \sigma(a))a} = \frac{(1 + a)a}{a + 1} = a.$$

□

Lemma 5.19. *Let $\mathcal{A}$ be a fractional ideal such that $\sigma(\mathcal{A}) = \mathcal{A}$. Then $\mathcal{A} = r\mathcal{Q}$ where $r \in \mathbb{Q}_{>0}$ and $\mathcal{Q}$ is a (possibly empty) product of distinct ramified prime ideals.*

Proof. By the uniqueness of the prime ideal decomposition it is enough to show this for prime ideals $\wp$. The non-trivial Galois automorphism σ acts on the zeros of f mod p. If f has a double zero mod p then σ fixes the prime ideal $\wp$ dividing p (these are the ramified primes).
If f is irreducible mod p, then $p\mathbb{Z}_K$ is a prime ideal.
If f is a product of two distinct linear polynomials then σ interchanges the two zeros of f modulo p and $p = \wp\sigma(\wp)$ is a product of two distinct prime ideals. □

Lemma 5.20. *Let $\mathcal{A} \trianglelefteq \mathbb{Z}_K$. Then $\mathcal{A}\sigma(\mathcal{A}) = N(\mathcal{A})\mathbb{Z}_K$.*

Proof. Again it is enough to show this for prime ideals where we did this in the last proof. □

The above lemma shows that for any ideal $\mathcal{A}$ the inverse $[\mathcal{A}]^{-1} = [\sigma(\mathcal{A})]$ in the class group of K. In particular $[\mathcal{A}] = [\sigma(\mathcal{A})]$ if and only if $[\mathcal{A}]$ has order 1 or 2 in the class group.

Lemma 5.21. *If $[\mathcal{A}] = [\sigma(\mathcal{A})]$ then this class contains a σ-invariant ideal.*

Proof. In this case there is some $r \in K^*$ such that $\sigma(\mathcal{A}) = \mathcal{A}r$. Then $N((r)) = N(\mathcal{A})^{-1}N(\sigma(\mathcal{A})) = 1$ and therefore $|N(r)| = 1$. But the norm form is positive definite, so $N(r) = 1$ and there is some $b \in K^*$ with $r = \frac{b}{\sigma(b)}$. Put

$$\mathcal{B} := \mathcal{A}b.$$

Then $\mathcal{B} \in [\mathcal{A}]$ satisfies

$$\sigma(\mathcal{B}) = \sigma(\mathcal{A})\sigma(b) = \mathcal{A}r\sigma(b) = \mathcal{A}b = \mathcal{B}$$

□

To see the last point (c), we need to show that no other product of distinct ramified prime ideals is principal. For simplicity we only deal with the case $-d \equiv 1, 2$ modulo 4 and show that in this case for any proper divisor $1 < m < d$ of d the ring $\mathbb{Z}_K$ does not contain an element of norm m. If $x, y \in \mathbb{Z}$ then the norm of $x + y\sqrt{-d}$ is $x^2 + y^2 d = m$ then (since $0 < m < d$) y^2 needs to be 0, so $m = x^2$ is a square which is a contradiction. In the case $-d \equiv 1$ modulo 4 we also have integral elements $(x + y\sqrt{d})/2$ where x and y are both odd. The norm of this element is $\frac{1}{4}(x^2 + y^2 d)$ so $(x^2 + y^2 d) = 4m$, which is only possible if $y = \pm 1$, then $x^2 = 4m - d = m(4 - \frac{d}{m})$ and $\frac{d}{m} = 3$. But this contradicts the fact that d and hence also m is squarefree, in particular m is not a square.

6 Ramification.

Let $\mathbb{Q} \subset K \subset L$ be a tower of algebraic number fields and $\mathbb{Z} \subset \mathbb{Z}_K \subset \mathbb{Z}_L$ the corresponding ring of integers.

Definition 6.1. *Let $0 \neq \wp \trianglelefteq \mathbb{Z}_K$ be a prime ideal. Then*

$$\wp\mathbb{Z}_L = \wp_1^{e_1} \cdots \wp_r^{e_r}$$

for prime ideals $\wp_i \trianglelefteq \mathbb{Z}_K$ and $e_1, \ldots, e_r \in \mathbb{N}$. Each $\wp_i$ defines a field extension

$$\mathbb{F}_q \cong \mathbb{Z}_K/\wp \hookrightarrow \mathbb{Z}_L/\wp_i \cong \mathbb{F}_{q^{f_i}}$$

of degree f_i, since $\wp = \wp_i \cap \mathbb{Z}_K$ for all i. Then e_i is called the **ramification index** *of $\wp_i$ and f_i is the* **inertia degree** *of $\wp_i$.*

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{-7}]$, $\alpha := \frac{1+\sqrt{-7}}{2}$.
ramified prime: $(\sqrt{-7})^2 = 7\mathbb{Z}_L$, $e = 2$, $f = 1$.
inert prime: $(3) = 3\mathbb{Z}_L$, $e = 1$, $f = 2$.
decomposed prime: $2\mathbb{Z}_L = (\alpha)(1 - \alpha)$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$.

Theorem 6.2. *Let $\mathbb{Q} \subset K \subset L$ and $0 \neq \wp \trianglelefteq \mathbb{Z}_K$ be a prime ideal with $\wp\mathbb{Z}_L = \wp_1^{e_1} \cdots \wp_r^{e_r}$ for prime ideals $\wp_i \trianglelefteq \mathbb{Z}_L$ and inertia degrees $f_i = [(\mathbb{Z}_L/\wp_i) : (\mathbb{Z}_K/\wp)]$. Then $\sum_{i=1}^r e_i f_i = n = [L : K]$.*

Proof. By the Chinese remainder theorem

$$\mathbb{Z}_L/\wp\mathbb{Z}_L = \bigoplus_{i=1}^{r} \mathbb{Z}_L/\wp_i^{e_i}.$$

Put $k := \mathbb{Z}_K/\wp$. Then $\mathbb{Z}_L/\wp\mathbb{Z}_L$ is a vector space over k and

$$\dim_k(\mathbb{Z}_L/\wp\mathbb{Z}_L) = \sum_{i=1}^{r} \dim_k(\mathbb{Z}_L/\wp_i^{e_i}) = \sum_{i=1}^{r} e_i f_i.$$

So we need to show that $\dim_k(\mathbb{Z}_L/\wp\mathbb{Z}_L) = n = [L : K]$.
To this aim let $\omega_1, \ldots, \omega_m \in \mathbb{Z}_L$ such that $(\overline{\omega}_1, \ldots, \overline{\omega}_m)$ is a k-basis of $\mathbb{Z}_L/\wp\mathbb{Z}_L$.
Claim: $(\omega_1, \ldots, \omega_m)$ is a K-basis of L.
linearly independent: Assume that $a_i \in K$ not all $= 0$ are such that $\sum_{i=1}^{m} a_i\omega_i = 0$. Wlog we may assume that all $a_i \in \mathbb{Z}_K$. Let $\mathcal{A} := (a_1, \ldots, a_m) \trianglelefteq \mathbb{Z}_K$ and choose some $a \in \mathcal{A}^{-1} \backslash \mathcal{A}^{-1}\wp$. Let $b_i := aa_i$. Then $\sum_{i=1}^{m} b_i\omega_i = 0$ with $b_i \in \mathbb{Z}_K$ not all $b_i \in \wp$. Reducing this modulo $\wp$ we obtain a linear dependence of the $\overline{\omega}_i$ which is a contradiction.
generating system: This follows essentially from Nakayama's Lemma: Let

$$M := \langle \omega_1, \ldots, \omega_m \rangle_{\mathbb{Z}_K} \leq \mathbb{Z}_L \text{ and } N := \mathbb{Z}_L/M.$$

Then $\mathbb{Z}_L = M + \wp\mathbb{Z}_L$ so $\wp N \cong (\wp\mathbb{Z}_L + M)/M = \mathbb{Z}_L/M = N$. We claim that N is a torsion module. Let $N = \langle \alpha_1, \ldots, \alpha_s \rangle_{\mathbb{Z}_K}$ with $\alpha_i = \sum_{j=1}^{s} a_{ij}\alpha_j$ and $a_{ij} \in \wp$. Let $d := \det(A)$ where $A = (a_{ij})_{i,j=1}^{s} - I_s \in \mathbb{Z}_K^{s\times s}$. Then $d \equiv (-1)^s \pmod{\wp}$ and $A^*A = dI_s$ for $A^* \in \mathbb{Z}_K^{s\times s}$ the adjoint of A. So

$$0 = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = A^*A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{pmatrix} = \begin{pmatrix} d\alpha_1 \\ \vdots \\ d\alpha_s \end{pmatrix}$$

and therefore $dN = 0$, so $|N|$ is finite. Since M is of finite index in $\mathbb{Z}_L$ it has the same rank as $\mathbb{Z}_L$ and generates L as a vector space over K. □

6.1 How to compute inertia degree and ramification index ?

Let $L = K(\alpha)$ with $\alpha \in \mathbb{Z}_L$, $f := \mu_\alpha$ the minimal polynomial of α. Then $\mathcal{O} := \mathbb{Z}_K[\alpha] \cong \mathbb{Z}_K[X]/(f(X))$ is an order in L.

Definition 6.3. *Let $\mathcal{F}_\alpha := \{a \in \mathbb{Z}_L \mid a\mathbb{Z}_L \subseteq \mathbb{Z}_K[\alpha]\}$ be the largest $\mathbb{Z}_L$-ideal contained in $\mathbb{Z}_K[\alpha]$. Then $\mathcal{F}_\alpha$ is called the* **conductor** *(Führer) of α.*

Theorem 6.4. *Let $\wp \trianglelefteq \mathbb{Z}_K$ be a prime ideal such that $\gcd(\wp\mathbb{Z}_L, \mathcal{F}_\alpha) = 1$. Assume that $\overline{\mu_\alpha}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r} \in \mathbb{Z}_K/\wp[X]$. Then $\wp_i := (\wp, p_i(\alpha))) \trianglelefteq \mathbb{Z}_L$ $(1 \leq i \leq r)$ are the prime ideals dividing $\wp\mathbb{Z}_L$ and*

$$\wp\mathbb{Z}_L = \wp_1^{e_1} \cdots \wp_r^{e_r},\ f_i := [\mathbb{Z}_L/\wp_i : \mathbb{Z}_K/\wp] = \deg(p_i).$$

<u>Proof.</u> Let $\mathcal{O} := \mathbb{Z}_K[\alpha]$. Then

$$\mathbb{Z}_L = \mathcal{F}_\alpha + \wp\mathbb{Z}_L \subseteq \mathcal{O} + \wp\mathbb{Z}_L \subseteq \mathbb{Z}_L$$

and hence $\mathcal{O}/\wp\mathcal{O} \cong \mathbb{Z}_L/\wp\mathbb{Z}_L \cong k[X]/(\overline{\mu}_\alpha(X))$ with $k = \mathbb{Z}_K/\wp$. The ideals in this ring can be read off from the factorization of $\overline{\mu}_\alpha(X) \in k[X]$. □

Corollary 6.5. *There are only finitely many prime ideals $\wp \trianglelefteq \mathbb{Z}_K$ for which there is a prime ideal $\wp_i \trianglelefteq \mathbb{Z}_L$ such that $\wp_i^2 \mid \wp\mathbb{Z}_L$. (For short: $\mathbb{Z}_L$ contains only finitely many ramified primes.)*

Proof. Since $\mathcal{F}_\alpha$ has only finitely many divisors, we may assume that $\wp$ is prime to $\mathcal{F}_\alpha$. Then the polynomial $\overline{\mu}_\alpha(X) \in k[X]$ has multiple factors, iff

$$\gcd(\overline{\mu}_\alpha(X), \overline{\mu}'_\alpha(X) \neq 1 \Leftrightarrow \wp \text{ divides } disc(\mu_\alpha) = \prod_{i<j}(\alpha_i - \alpha_j) \in \mathbb{Z}_K.$$

where α_i are the roots of μ_α in the algebraic closure of K. But this ideal has only finitely many prime divisors. □

Example: Let $f := X^4 + 2X^3 - 5X^2 - 6X - 1 \in \mathbb{Q}[X]$, $L = \mathbb{Q}[X]/(f(X))$, $\alpha = \overline{X} \in L$, so $\mu_\alpha = f$. Then $\mathbb{Z}[\alpha]$ is of index 3 in $\mathbb{Z}_L$. $d_L = 1600$, $\operatorname{disc}(f) = 14400 = 9d_L$.

f	$\pmod 2$	$(X^2+X+1)^2$	$(2) = \wp_2^2$	$e = f = 2$
f	$\pmod 3$	$(X+2)^2(X^2+X+2)$		
f	$\pmod 5$	$(X^2+X+2)^2$	$(5) = \wp_5^2$	$e = f = 2$
f	$\pmod 7$	$(X^2+4)(X^2+2X+5)$	$(7) = \wp_7\wp_7'$	$e_1 = e_2 = 1, f_1 = f_2 = 2$

6.2 Hilbert's theory of ramification for Galois extensions.

Let $L \supseteq K$ be algebraic number fields and assume that L/K is Galois. Let $G := \operatorname{Gal}(L/K)$ denote the Galois group.

Remark 6.6. *For any $\sigma \in G$ we have $\sigma(\mathbb{Z}_L) = \mathbb{Z}_L$. If $\wp \trianglelefteq \mathbb{Z}_L$ is a prime ideal, then also $\sigma(\wp) \trianglelefteq \mathbb{Z}_L$ is a prime ideal and $\wp \cap \mathbb{Z}_K = \sigma(\wp) \cap \mathbb{Z}_K$.*

Theorem 6.7. *The Galois group acts transitively on the set of prime ideals of $\mathbb{Z}_L$ that contain a given prime ideal $\wp$ of $\mathbb{Z}_K$:*

$$\wp\mathbb{Z}_L = \wp_1^{e_1} \dots \wp_r^{e_r} \Rightarrow \textit{ for all } 1 \leq i \leq r \textit{ there is } \sigma_i \in G, \sigma_i(\wp_1) = \wp_i.$$

Proof. Assume that $\wp_2 \neq \sigma(\wp_1)$ for all $\sigma \in G$. By the Chinese remainder theorem there is some $x \in \mathbb{Z}_L$ such that

$$x \equiv 0 \pmod{\wp_2},\ x \equiv 1 \pmod{\sigma(\wp_1)} \text{ for all } \sigma \in G.$$

Then $N_{L/K}(x) = \prod_{\sigma\in G} \sigma(x) \in \wp_2 \cap \mathbb{Z}_K = \wp$.
On the other had $\sigma(x) \notin \wp_1$ for all $\sigma \in G$, so $N_{L/K}(x) \notin \wp_1 \cap \mathbb{Z}_K = \wp$ which is a contradiction.
□

Corollary 6.8. *$e_1 = \ldots = e_r =: e$, $f_1 = \ldots = f_r =: f$ and $[L : K] = n = ref$.*
e is called the **ramification index** *of $\wp$, $e = e_{L/K}(\wp) = e_{L/K}(\wp_i)$* for all *$i$.*
f is called the **inertia degree** *of $\wp$, $f = f_{L/K}(\wp) = f_{L/K}(\wp_i)$* for all *$i$.*

Definition 6.9. *Let $\wp \trianglelefteq \mathbb{Z}_L$ be a prime ideal in $\mathbb{Z}_L$. Then*

$$G_\wp := \{\sigma \in G \mid \sigma(\wp) = \wp\}$$

is called the **decomposition group** *of $\wp$ and $Z_\wp := \mathrm{Fix}_{G_\wp}(L) := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G_\wp\}$ is called the* **decomposition field** *of $\wp$.*

Theorem 6.10. *Let $\wp \trianglelefteq \mathbb{Z}_L$ be a prime ideal in $\mathbb{Z}_L$ and let $\wp_Z := \wp \cap Z_\wp$, $Z := Z_\wp$.*
(1) $\wp_Z \mathbb{Z}_L = \wp^e$.
(2) $f_{L/Z}(\wp) = f_{L/K}(\wp)$, $e_{L/Z}(\wp) = e_{L/K}(\wp) = e$.
(3) $e_{Z/K}(\wp_Z) = f_{Z/K}(\wp_Z) = 1$.

Proof. (1) $G_\wp = \mathrm{Gal}(L/Z)$, so the set of all prime ideals of $\mathbb{Z}_L$ that contain $\wp_Z$ is $\{\sigma(\wp) \mid \sigma \in G_\wp\} = \{\wp\}$.
(2) Let $r := [G : G_\wp]$ and let $\{\wp = \wp_1, \ldots, \wp_r\}$ be the set of prime ideals of $\mathbb{Z}_L$ that contain $P := \wp \cap \mathbb{Z}_K$. Then $ref = |G| = [L : K]$ where $e = e_{L/K}(\wp)$, $f = f_{L/K}(\wp)$. So $ef = |G_\wp| = e_{L/Z}(\wp) f_{L/Z}(\wp)$. Clearly $e_{L/Z}(\wp) \leq e_{L/K}(\wp)$ and $f_{L/Z}(\wp) \leq f_{L/K}(\wp)$ from which one obtains (2).
(3) $e_{L/K}(\wp) = e_{L/Z}(\wp) e_{Z/K}(\wp_Z)$ and $f_{L/K}(\wp) = f_{L/Z}(\wp) f_{Z/K}(\wp_Z)$. □

Theorem 6.11. *Let $k(\wp) := \mathbb{Z}_L/\wp$ and $k := \mathbb{Z}_K/P$ with $P = \wp \cap \mathbb{Z}_K$. Then $k(\wp)/k(P)$ is a normal extension and $G_\wp \to \mathrm{Gal}(k(\wp)/k(P))$ is surjective.*

Proof. We first note that $k \cong k(\wp_Z) = \mathbb{Z}_Z/\wp_Z$ so we may assume that $Z_\wp = K$ and $G_\wp = G$. Choose $\alpha \in \mathbb{Z}_L$ such that $\overline{\alpha} := \alpha + \wp \in k(\wp)$ is a primitive element, let $f := \mu_{\alpha,K} \in \mathbb{Z}_K[X]$ and $\overline{g} := \mu_{\overline{\alpha},k} \in k[X]$. Then $\overline{g}$ divides $\overline{f} \in k[X]$. Since L/K is normal, all roots of f lie in $\mathbb{Z}_L$, so $f \in \mathbb{Z}_L[X]$ is a product of linear factors, and hence also $\overline{f}$ and therefore $\overline{g} \in k(\wp)[X]$ is a product of linear factors, so $k(\wp)/k$ is normal.
Now let $\overline{\alpha}_1 \in k(\wp)$ be a zero of $\overline{g}$. Then there is $\alpha_1 \in \mathbb{Z}_L$ with $f(\alpha_1) = 0$ such that $\overline{\alpha}_1 = \alpha_1 + \wp$. This yields the existence of some $\sigma \in G = G_\wp$ such that $\sigma(\alpha) = \alpha_1$. This element σ maps onto the Galois automorphism of $k(\wp)$ that maps $\overline{\alpha}$ to $\overline{\alpha}_1$. □

Definition 6.12.

$$1 \to I_\wp \to G_\wp \to \mathrm{Gal}(k(\wp)/k) \to 1$$

is a short exact sequence. In particular the **inertia group** *of $\wp$ is*

$$I_\wp := \{\sigma \in G_\wp \mid \sigma(x) \equiv x \pmod{\wp} \text{ for all } x \in \mathbb{Z}_L\} \trianglelefteq G_\wp.$$

The fixed field $T_\wp := \mathrm{Fix}(I_\wp)$ is called the **inertia field** *of $\wp$.*

Corollary 6.13. *$T_\wp/Z_\wp$ is a Galois extension with Galois group*

$$\mathrm{Gal}(T_\wp/Z_\wp) \cong \mathrm{Gal}(k(\wp)/k) \cong G_\wp/I_\wp \cong C_f.$$

$$\begin{array}{ccccccc} L & \overbrace{\supseteq}^{e} & T_\wp & \overbrace{\supseteq}^{f} & Z_\wp & \overbrace{\supseteq}^{r} & K \\ & \mathrm{Gal}(L/T_\wp) = I_\wp & C_f & \cong G_\wp/I_\wp = & \mathrm{Gal}(T_\wp/Z_\wp) & G_\wp & = \mathrm{Gal}(L/Z_\wp) \end{array}$$

Example. $L = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$, $K = \mathbb{Q}$, $\mathrm{Gal}(L/\mathbb{Q}) = S_3$.
Prime ideal decompositions:
$5\mathbb{Z}_L = \wp_5\wp_5'\wp_5''$ with $f_i = 2$. Put $Z := \mathbb{Q}[\sqrt[3]{2}]$. Then $5\mathbb{Z}_Z = p_5p_5'$ with $f = 1, f' = 2$, wlog $\wp_5 = p_5\mathbb{Z}_L$ then $Z = Z_{\wp_5}$, $G_{\wp_5} = \mathrm{Gal}(L/Z) \cong C_2$ and $T_{\wp_5} = L$.
For the prime 2 we obtain $2\mathbb{Z}_L = \wp_2^3 = (\sqrt[3]{2})^3$, $T_{\wp_2} = \mathbb{Q}[\zeta_3]$, $Z_{\wp_2} = \mathbb{Q}$, $G_{\wp_2} = G$, $e = 3, f = 2$.

7 Cyclotomic fields.

Definition 7.1. *The* **cyclotomic polynomials** *are defined recursively by*

$$\Phi_1(X) := (X-1), \Phi_n(X) := (X^n - 1)/\prod_{d|n, 1\le d<n} \Phi_d(X)$$

The roots of Φ_n are the primitive n-th root of unity.

Remark 7.2. *In the Algebra class we have seen the following facts:*

(a) $\Phi_n(X) \in \mathbb{Q}[X]$ *is an irreducible polynomial with integral coefficients.*

(b) $\Phi_n(X) = \prod_{d\in(\mathbb{Z}/n\mathbb{Z})^*}(X - \zeta_n^d)$ *where ζ_n is any primitive nth root of unity.*

(c) $\deg(\Phi_n(X)) = \varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$.

(d) $\mathbb{Q}[\zeta_n] := K_n$ *is a Galois extension of $\mathbb{Q}$ with* $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ *with explicit isomorphism mapping $a \in (\mathbb{Z}/n\mathbb{Z})^*$ to $\sigma_a : (\zeta_n \mapsto \zeta_n^a)$. K_n is called the n-th cyclotomic field.*

(e) If $n = p_1^{a_1}\cdots p_s^{a_s}$ is a product of powers of distinct primes then

$$K_n = K_{p_1^{a_1}} \cdots K_{p_s^{a_s}},\ \zeta_n = \prod_{i=1}^{s} \zeta_{p_i^{a_i}}$$

Remark 7.3. *(cyclotomic units)*
(a) Assume that $n = p^a$ is a prime power and let $i, j \in \mathbb{N}$ such that $p\not| ij$. Then $(1-\zeta_n^j)/(1-\zeta_n^i) \in \mathbb{Z}[\zeta_n]^*$.
(b) Assume that n is divisible by at least two distinct primes. Then $(1-\zeta_n) \in \mathbb{Z}[\zeta_n]^*$ and $\prod_{j\in\mathbb{Z}/n\mathbb{Z}^*}(1-\zeta_n^j) = 1$.

Proof. Exercise. □

Theorem 7.4. *If $n = p^a$ is a prime power then $\mathbb{Z}_{K_n} = \mathbb{Z}[\zeta_n]$ and $d(K_n) = \pm p^{p^{a-1}(ap-a-1)}$.*

Proof. Let

$$\mathcal{O} := \mathbb{Z}[\zeta_n] = \langle 1, \zeta_n, \ldots, \zeta_n^{p^{a-1}(p-1)-1} \rangle_{\mathbb{Z}} \cong \mathbb{Z}[X]/(\Phi_n(X)).$$

Then $\wp := (1-\zeta_n) \trianglelefteq \mathcal{O}$ is a Galois invariant ideal of norm

$$N_{K_n/\mathbb{Q}}(1-\zeta_n) = \prod_{p \nmid j} (1-\zeta_n^j) = \Phi_n(1) = p.$$

Note that $\Phi_n(X) = (X^{p^a}-1)/(X^{p^{a-1}}-1) = (Y^p-1)/(Y-1) = Y^{p-1}+Y^{p-2}+\ldots+Y+1$ with $Y = X^{p^{a-1}}$. By comparing norms we obtain $\wp^d = p\mathcal{O}$ with $d = [K_n : \mathbb{Q}] = \varphi(n) = p^{a-1}(p-1)$. So the unique maximal ideal dividing $p\mathcal{O}$ is a principal ideal, hence $\mathcal{O} = \mathcal{O}(J_p(\mathcal{O}))$ is p-maximal. But the determinant of $\mathcal{O}$ is the discriminant of Φ_n which is not divisible by any prime $\ell \neq p$, since the n-th roots of unity are pairwise distinct modulo ℓ. Therefore $\mathcal{O}$ is also ℓ-maximal for all primes $\ell \neq p$ and hence a maximal order (Exercise 4, Sheet 2).

In particular we know that $\mathcal{O} = \mathbb{Z}_{K_n}$ and that the discriminant of K_n is a power of p. Put $\zeta := \zeta_n$. Then

$$d(\mathcal{O}) = d(\Phi_n) = \prod_{i \neq j \in \mathbb{Z}/p^a\mathbb{Z}^*} (\zeta^i - \zeta^j) = \prod_{i \in \mathbb{Z}/p^a\mathbb{Z}^*} \Phi_n'(\zeta^i) = N_{K_n/\mathbb{Q}} \Phi_n'(\zeta).$$

Note that $\Phi_n'(X) = \frac{d}{dX} \prod_{i \in \mathbb{Z}/p^a\mathbb{Z}^*} (X-\zeta^i) = \sum_{i \in \mathbb{Z}/p^a\mathbb{Z}^*} \prod_{j \neq i} (X-\zeta^j)$. To compute $\Phi_n'(\zeta)$ we differentiate the equation $(X^{p^{a-1}}-1)\Phi_n(X) = (X^{p^a}-1)$ to obtain

$$p^{a-1}X^{p^{a-1}-1}\Phi_n(X) + (X^{p^{a-1}}-1)\Phi_n'(X) = p^a X^{p^a-1}.$$

Evaluating at ζ we obtain $(\zeta^{p^{a-1}}-1)\Phi_n'(\zeta) = p^a\zeta^{p^a-1}$ since $\Phi_n(\zeta) = 0$. Now $\alpha := \zeta^{p^{a-1}}$ is a primitive pth root of unity and hence $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha - 1) = \pm p$, so

$$\begin{array}{l} N_{K_n/\mathbb{Q}}(\alpha-1) = \pm p^{p^{a-1}} \\ N_{K_n/\mathbb{Q}}(\zeta) = \pm 1 \\ N_{K_n/\mathbb{Q}}(p^a) = \pm (p^a)^{p^{a-1}(p-1)} \quad \Rightarrow \\ N_{K_n/\mathbb{Q}}(\Phi_n'(\zeta)) = \pm p^s \end{array}$$

where $s = p^{a-1}(ap-a-1)$. □

Theorem 7.5. *Let $n = p_1^{a_1} \cdots p_s^{a_s} \in \mathbb{N}$. Then $\mathbb{Z}_{K_n} = \mathbb{Z}[\zeta_n]$ and $d(K_n) = \prod_{i=1}^s d(K_{p_i^{a_i}})^{\varphi(\frac{n}{p_i^{a_i}})}$.*

This follows from the next more general Lemma.

Lemma 7.6. *Let K, K' be number fields of degree $n = [K : \mathbb{Q}]$, $n' := [K' : \mathbb{Q}]$ and discriminants $d := d(K)$ and $d' := d(K')$. Assume that $\gcd(d, d') = 1$ and $L := KK'$ has degree nn' over $\mathbb{Q}$. If $B := (w_1, \ldots, w_n)$ and $B' = (v_1, \ldots, v_{n'})$ are integral bases of K resp. K', then $BB := (w_i v_j \mid 1 \leq i \leq n, 1 \leq j \leq n')$ is an integral basis of $\mathbb{Z}_L$ and $d(L) = d^{n'}(d')^n$.*

Proof. (a) BB is a $\mathbb{Q}$-basis of L: It is a generating set by definition of L and these elements are linearly independent since we assumed that $[L : \mathbb{Q}] = nn'$.

(b) To compute $d(BB)$ let $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ resp. $\varphi_1, \ldots, \varphi_{n'} : K' \to \mathbb{C}$ be the distinct embeddings. Then $\sigma_i \varphi_j : L \to \mathbb{C}$ are the embeddings of L and

$$d(BB) = \det(M)^2, \text{ where } M = (\sigma_i \varphi_j(w_k v_l))_{(i,j),(k,l)} = (\sigma_i(w_k)\varphi_j(v_l))_{(i,j),(k,l)}.$$

This matrix M is easily seen to be the Kronecker product $M = A \otimes A'$ with $A = (\sigma_i(w_k))_{i,k}$ and $A' = (\varphi_j(v_l))_{j,l}$. Hence $d(BB) = d^{n'}(d')^n$ as claimed.
(c) BB is an integral basis. Basis is clear, also that the elements of BB are integral. So it remains to show that $\langle BB \rangle_{\mathbb{Z}} = \mathbb{Z}_L$. Let $\alpha = \sum_{i,j} a_{ij} w_i v_j \in \mathbb{Z}_L$ with $a_{ij} \in \mathbb{Q}$. We need to show that all $a_{ij} \in \mathbb{Z}$. Let A' be as above and put

$$a := (\varphi_1(\alpha), \ldots, \varphi_{n'}(\alpha))^{tr}, b := (\beta_1, \ldots, \beta_{n'})^{tr}, \text{ where } \beta_j = \sum_{i=1}^{n} a_{ij} w_i.$$

Then $a = A'b$ and $d'b = \det(A')b = (A')^* a$. Since all entries are integers, the vector $d'b$ only has integral entries, so $d' \sum_{i=1}^{n} a_{ij} w_i \in \mathbb{Z}_K$ which implies that $d' a_{ij} \in \mathbb{Z}$ for all i, j. Similarly we obtain $d a_{ij} \in \mathbb{Z}$ for all i, j and hence $a_{ij} \in \mathbb{Z}$ since d and d' are co-prime. □

We now investigate the ramification indices and inertia degrees of primes in K_n.

Theorem 7.7. *Let p be a prime, $m \in \mathbb{N}$ not divisible by p and put $n = p^a m \in \mathbb{N}$. Let $f \in \mathbb{N}$ be minimal such that $p^f \equiv 1 \pmod{m}$. Then the ramification index of p in K_n is $e = \varphi(p^a) = p^{(a-1)}(p-1)$ and the inertia degree of p in K_n is f. Moreover f divides $\varphi(m)$ and*

$$p\mathbb{Z}[\zeta_n] = (\wp_1 \cdots \wp_r)^e, f_{K_n/\mathbb{Q}}(\wp_i) = f.$$

where $r = \varphi(m)/f$.

Proof. We need to factorise $\overline{\Phi}_n(X) \in \mathbb{F}_p[X]$. If $\{\alpha_i \mid 1 \le i \le \varphi(p^a)\}$ is the set of primitive p^a-th roots of unity and $\{\beta_i \mid 1 \le i \le \varphi(m)\}$ is the set of primitive m-th roots of unity then

$$\{\alpha_i \beta_j \mid 1 \le i \le \varphi(p^a), 1 \le j \le \varphi(m)\}$$

is the set of primitive n-th root of unity and

$$\Phi_n(X) = \prod_{i,j}(X - \alpha_i\beta_j) \equiv_p \prod_j (X - \beta_j)^{\varphi(p^a)} \equiv_p \Phi_m(X)^e.$$

The m-th roots of unity are distinct mod p and $\mathbb{F}_{p^f}$ contains a primitive m-th root of unity, iff $m \mid p^f - 1$. So all irreducible factors of $\overline{\Phi}_m(X) \in \mathbb{F}_p[X]$ have degree f. □

Example. Let $n := 45 = 3^2 5$. Then $\mathrm{Gal}(K_n/\mathbb{Q}) \cong C_6 \times C_4$, $K_n = K_9 K_5$ and $3\mathbb{Z}[\zeta_n] = \wp_3^6$ is totally ramified in K_9 and inert in K_5. So $e_3 = 6$, $f_3 = 4$. So the decomposition field is $Z_3 = \mathbb{Q}$, the inertia field is $T_3 = \mathbb{Q}[\zeta_5]$.
Since $3 \not| 5 - 1$ the prime $5\mathbb{Z}[\zeta_n] = \wp_5^4$ with $e_5 = 4$, $f_5 = 6$. So the decomposition field is $Z_5 = \mathbb{Q}$, the inertia field is $T_5 = \mathbb{Q}[\zeta_3]$.
To compute the inertia degree of 2, we need to find the minimal $f = f_2$ for which $2^f - 1$ is a multiple of 45. $2^4 - 1 = 15$, so $f = 3 \cdot 4 = 12$ and $2\mathbb{Z}[\zeta_n] = \wp_2 \wp_2'$. The decomposition field of

2 is $\mathbb{Q}[\sqrt{-15}]$.
For the prime 11 one finds that $45 \mid 11^6 - 1$ and hence $f_{11} = 6$ and $11\mathbb{Z}[\zeta_n] = \wp_{11}\wp'_{11}\wp''_{11}\wp'''_{11}$. Since $3^5 \equiv_{11} 1$, the prime ideals over 11 are

$$\wp_{11} = (3-\zeta_5, 11),\ \wp'_{11} = (3-\zeta_5^2, 11),\ \wp''_{11} = (3-\zeta_5^3, 11),\ \wp'''_{11} = (3-\zeta_5^4, 11).$$

The decomposition field of 11 is $Z_{11} = \mathbb{Q}[\zeta_5]$.

Corollary 7.8. *Let n be either odd or a multiple of 4. Then p is ramified in $\mathbb{Z}[\zeta_n]$ if and only if $p \mid n$.*

7.1 Quadratic Reciprocity.

Theorem 7.9. *Let ℓ and p be odd primes and put $\ell^* := (-1)^{(\ell-1)/2}\ell$. Then p is (totally) decomposed in $\mathbb{Q}[\sqrt{\ell^*}]$, if and only if $p\mathbb{Z}[\zeta_\ell]$ is a product of an even number of prime ideals.*

Proof. Since K_ℓ has a subfield L of degree 2 over $\mathbb{Q}$ and ℓ is the only prime that ramifies in K_ℓ, this is also the only prime that ramifies in this unique quadratic subfield, so $L = \mathbb{Q}[\sqrt{\ell^*}]$. Now assume that $p\mathbb{Z}_L = \wp_1\wp_2$ is a product of two prime ideals in L and let $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q}) =: G$ be such that $\sigma(\wp_1) = \wp_2$. Then σ yields a bijection between the set of prime ideals of $\mathbb{Z}[\zeta_\ell]$ that contain $\wp_1$ and the ones that contain $\wp_2$, in particular the number of prime ideals of $\mathbb{Z}[\zeta_\ell]$ that contain p is even.
To see the opposite direction let $\wp$ be a prime ideal of $\mathbb{Z}[\zeta_\ell]$ such that $\wp \cap \mathbb{Z} = p\mathbb{Z}$ and let $G_\wp := \mathrm{Stab}_G(\wp)$ be its decomposition group. Since by assumption $|\wp^G|$ is even, the index $[G : G_\wp]$ is even. Now G is cyclic, so the unique quadratic subfield L of K_ℓ is contained in the decomposition field $L \subset Z_\wp = \mathrm{Fix}(G_\wp)$. Putting $P_Z := \wp \cap Z_\wp$ then $f_{Z_\wp/\mathbb{Q}}(P_Z) = 1$ so also $f_{L/\mathbb{Q}}(P_Z \cap L) = 1$. But p does not divide the discriminant of L, so it is not ramified, and therefore totally decomposed in L. □

Definition 7.10. *Let $2 \neq p$ be a prime, $a \in \mathbb{Z}$ such that $p \not| a$.*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \equiv_p x^2 \text{ for some } x \in \mathbb{Z} \\ -1 & \text{otherwise.} \end{cases}$$

is called the **Legendre symbol** *of a at p.*

Remark 7.11. *(a)* $\left(\frac{a}{p}\right) = 1 \Leftrightarrow (a + p\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z}^*)^2 \Leftrightarrow a^{(p-1)/2} \equiv_p 1$.
(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
(c) Let $a \in \mathbb{Z}\setminus\{0,1\}$ be squarefree and $K := \mathbb{Q}[\sqrt{a}]$. Then $\left(\frac{a}{p}\right) = 1 \Leftrightarrow p\mathbb{Z}_K = \wp_1\wp_2$ is totally decomposed.

Theorem 7.12. *(Gauss reciprocity)*
(a) Let ℓ and p be distinct odd primes. Then

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

(b) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
(c) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Proof. (b) is clear.
To see (c) we compute in $\mathbb{Z}[i]$. Here $(1+i)^2 = 2i$. And

$$1 + i^p \equiv_p (1+i)^p = (1+i)((1+i)^2)^{(p-1)/2} \equiv_p (1+i)2^{(p-1)/2} i^{(p-1)/2} \equiv_p (1+i)\left(\frac{2}{p}\right) i^{(p-1)/2}$$

so $(1+i)\left(\frac{2}{p}\right) i^{(p-1)/2} \equiv_p 1 + i(-1)^{(p-1)/2}$.
If $(p-1)/2$ is even, then this reads as $(1+i)\left(\frac{2}{p}\right)(-1)^{(p-1)/4} \equiv_p (1+i)$. Dividing both sides by $(1+i)$ we obtain $\left(\frac{2}{p}\right) \equiv_p (-1)^{(p-1)/4}$.
If $(p-1)/2$ is odd, then we have $(1+i)\left(\frac{2}{p}\right)(-i)(-1)^{(p+1)/4} \equiv_p 1-i$ and hence $\left(\frac{2}{p}\right)(-i)i(-1)^{(p+1)/4} \equiv_p 1$ because $\frac{1+i}{1-i} = i$. So $\left(\frac{2}{p}\right) \equiv_p (-1)^{(p+1)/4}$.
These two congruences may be summarised as in (c).
(a) Let $\ell^* := (-1)^{(\ell-1)/2}\ell$ be as in Theorem 7.9. We show that

$$\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$$

Then

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

We have $\left(\frac{\ell^*}{p}\right) = 1$ iff p is decomposed in $\mathbb{Q}[\sqrt{\ell^*}] \Leftrightarrow p$ splits in $\mathbb{Q}[\zeta_\ell]$ into an even number of prime ideals. Now $p\mathbb{Z}[\zeta_\ell] = \wp_1 \cdots \wp_s$ with $s = \frac{\ell-1}{f}$ and f minimal such that $p^f \equiv_\ell 1$. So s is even $\Leftrightarrow$

$$f \mid \frac{\ell-1}{2} \Leftrightarrow p^{\frac{\ell-1}{2}} \equiv_\ell 1 \Leftrightarrow \left(\frac{p}{\ell}\right) = 1$$

□

8 Discrete valuation rings.

Definition 8.1. *(a) A* **discrete valuation ring** *R is a local principal ideal domain (commutative, without zero divisors) which is not a field.*
(b) Let K be a field. A **discrete valuation** *of K is a mapping $v : K \to \mathbb{Z} \cup \{\infty\}$ such that*
(o) There is some $x \in K^*$ such that $v(x) \neq 0$.
(i) $v(x) = \infty \Leftrightarrow x = 0$.
(ii) $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$.
(iii) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

Clear: $v(1) = 0$, $v(x^{-1}) = -v(x)$, $v : K^* \to (\mathbb{Z}, +)$ is a group homomorphism.

Remark 8.2. *$v(x+y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.*

Proof. First note that $v(\zeta) = 0$ for any $\zeta \in K$ such that $\zeta^n = 1$ for some n. In particular $v(-1) = 0$ and $v(-y) = v(y)$.
Assume that $v(x) < v(y)$. Then

$$v(x) = v(x+y-y) \geq \min\{v(x+y), v(y)\} \geq \min\{v(x), v(y)\} = v(x).$$

We therefore have equality everywhere and $v(x+y) = v(x)$ (note that $v(y) > v(x)$ by assumption). □

Example 8.3. *Let R be a Dedekind domain $K := \mathrm{Quot}(R)$ and $0 \neq \wp \trianglelefteq R$ a prime ideal. Then the* **localisation** *of R at $\wp$ is*

$$R_{(\wp)} := \{\frac{x}{y} \in K \mid x, y \in R, y \notin \wp\}.$$

Then $R_{(\wp)}$ is a discrete valuation ring with maximal ideal $\wp R_{(\wp)} = \pi R_{(\wp)}$ for any element $\pi \in \wp \setminus \wp^2$.
The prime ideal $\wp$ also defines a valuation $v = v_\wp : K^* \to \mathbb{Z}$ by putting $v(z) = n \in \mathbb{Z}_{\geq 0}$ if $\wp^n \mid zR$ but $\wp^{n+1} \not| zR$ and $v(\frac{x}{y}) = v(x) - v(y)$ for all $z, x, y \in R$. Then $R_{(\wp)} = \{x \in K \mid v(x) \geq 0\}$.

Proposition 8.4. *(a) Let R be a discrete valuation ring with maximal ideal $\wp = \pi R \neq \{0\}$. Then $K := \mathrm{Quot}(R) = \dot{\bigcup}_{i \in \mathbb{Z}} \pi^i R^* \cup \{0\}$ and the mapping $v : K \to \mathbb{Z} \cup \{\infty\}, v(\pi^i R^*) := i, v(0) := \infty$ is a discrete valuation of K.*
(b) If $v : K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, then $R := \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring with maximal ideal $\{x \in K \mid v(x) \geq 1\} =: \wp = \pi R$ for any $\pi \in K$ with $v(\pi) \geq 1$ minimal.

Proof. (a) Since R is a local ring the units are $R^* = R \setminus \wp$. Any element $a \in R$ is either a unit ($a \in R^*$) or a multiple of π and then $a_1 := \pi^{-1} a \in R$. Also a_1 is either a unit or a multiple of π. Continuing like this, we may write any non zero element of R in a unique way as $a = \pi^n u$ with $u \in R^*$ and $n \in \mathbb{Z}_{\geq 0}$. Similarly any element $0 \neq x = \frac{a}{b} \in \mathrm{Quot}(R) = K$ can be written as $\pi^i w$ with $w \in R^*$ and $i \in \mathbb{Z}$ in a unique way. Therefore v is well defined. It clearly satisfies (o), (i) and (ii). So it remains to show the strong triangular inequality. Let $x \in \pi^i R^*$, $y \in \pi^j R^*$, $i, j \in \mathbb{Z}$, $i \geq j$. Then $x+y \in \pi^j R$ and so $v(x+y) \geq j = \min\{v(x), v(y)\}$.
(b) We prove that R is a ring: $0 \in R$, $1 \in R$, $a, b \in R \Rightarrow ab \in R$ and $a + b \in R$.
The unit group of R is $R^* = \{x \in K \mid v(x) \geq 0 \text{ and } -v(x) \geq 0\} = \{x \in K \mid v(x) = 0\}$. In particular $\wp$ is the unique maximal ideal of R. Choose $\pi \in \wp$ such that $v(\pi)$ is minimal. Then for any $z \in \wp$ we have $v(z) \geq v(\pi)$ and hence $z\pi^{-1} \in R$. So $\wp = \pi R$ is a principal ideal. □

Remark 8.5. *Let R be a discrete valuation ring and $x \in K = \mathrm{Quot}(R)$. Then either $x \in R$ or $x^{-1} \in \wp$. In particular $K = R \cup \{x^{-1} \mid 0 \neq x \in \wp\}$.*

Theorem 8.6. *A Noetherian integral domain R is a Dedekind domain if and only if all localizations $R_{(\wp)}$ of R at non-zero prime ideals are discrete valuation rings.*

Proof. (Exercise) □

8.1 Completion

Remark 8.7. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation and $s \in (0,1)$. Then v defines an* **ultra-metric**

$$d : K \times K \to \mathbb{R}_{\geq 0}, d(x,y) := s^{v(x-y)}$$

where $s^{\infty} := 0$. This means that d satisfies the following three axioms:
(i) $d(a,b) = 0$ if and only if $a = b$.
(ii) $d(a,b) = d(b,a)$ for all $a, b \in K$.
(iii) $d(a,c) \leq \max\{d(a,b), d(b,c)\}$ for all $a, b, c \in K$.

Definition 8.8. *A metric space (M,d) is called* **complete***, if any Cauchy sequence in M converges towards a limit in M.*

Theorem 8.9. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of the field K. Put $\mathcal{R}$ the ring of all Cauchy sequences in K and $\mathcal{N}$ the ideal of all sequences in K that converge to 0. Then $\mathcal{N} \trianglelefteq \mathcal{R}$ is a maximal ideal and hence $\overline{K} := \mathcal{R}/\mathcal{N}$ is a field. The valuation v extends to a valuation v of $\overline{K}$ and $\overline{K}$ is complete. The mapping $\varphi : K \hookrightarrow \overline{K}, a \mapsto (a,a,a,a\ldots) + \mathcal{N}$ is injective and the image is dense in $\overline{K}$. The field $\overline{K}$ is called the* **completion** *of K. It is unique up to isomorphism.*

Proof. See the lecture Computeralgebra. □

Theorem 8.10. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of the field K with valuation ring R and maximal ideal πR. Define*

$$S := \lim_{\leftarrow} R/\pi^i R = \{(a_0, a_1, \ldots) \mid a_i \in R/\pi^{i+1}R, a_i + \pi^i R = a_{i-1}\}.$$

Then S is an integral domain and $\varphi : R \to S, a \mapsto (a + \pi R, a + \pi^2 R, \ldots)$ is a ring monomorphism. The valuation v extends uniquely to a valuation v of S, $v(a_0, a_1, \ldots,) := i$ if $a_i \neq 0$, $a_{i-1} = 0$. S is complete with respect to this valuation and $\overline{K} := \mathrm{Quot}(S)$ is the completion of K.

Proof. S is a ring with componentwise operations since the projections $a + \pi^i R \mapsto a + \pi^{i-1} R$ are ring homomorphisms.
φ is injective because $\bigcap_{i=0}^{\infty} \pi^i R = \{0\}$.
It is clear that v is a valuation that extends the valuation of R (exercise).
To see the completeness of S let $(x_n)_{n\geq 0}$ be a Cauchy sequence in S, so $\lim\limits_{n,m\to\infty} v(x_n - x_m) = \infty$ or more concrete that for all $k \geq 0$ there is some $N(k) \in \mathbb{N}$ such that $v(x_n - x_m) > k$ for all $n, m \geq N(k)$. Wlog assume that $(N(n))_{n\geq 0}$ is monotone increasing. Put $x = (x_{N(k),k})_{k\geq 0}$. Then $x \in S$ since

$$x_{N(k),k} + \pi^k R = x_{n,k} + \pi^k R = x_{n,k-1} = x_{N(k-1),k-1}$$

for all $n \geq N(k)$. Similarly one shows that $v(x - x_n) \to \infty$ for $n \to \infty$ so x is the limit of the Cauchy sequence. □

For an example see the lecture Computeralgebra, where we introduced the p-adic numbers $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ at the p-adic valuation v_p.

Example. The completion of $K = \mathbb{Q}[\zeta_3]$ at prime ideals over $2, 3, 7$.

8.2 Hensel's Lemma

Theorem 8.11. *Let K be a discrete valuated complete field with valuation v, valuation ring R. Let $f \in R[X]$ be a polynomial and $a_0 \in R$ such that*

$$v(f(a_0)) > 2v(f'(a_0))$$

Then there is some $a \in R$ such that $f(a) = 0$. More precisely the sequence

$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)} \in R$$

converges towards some $a \in R$ such that $f(a) = 0$ and $v(a - a_0) \geq v(f(a_0)) - v(f'(a_0)) > 0$.

Proof. (see also Computeralgebra) Note that $f(t + x) = f(t) + f_1(t)x + f_2(t)x^2 + \ldots$, for $f_i(t) \in R[t]$, $f_1(t) = f'(t)$. Define $b_0 := -\frac{f(a_0)}{f'(a_0)}$. Then $v\left(\frac{f(a_0)}{f'(a_0)}\right) = v(f(a_0)) - v(f'(a_0)) > v(f'(a_0)) \geq 0$, so $a_1 \in R$.
Moreover $v(f(a_0 + b_0)) \geq \min\{v(f_i(a_0)b_0^i) \mid i \geq 2\}$, since $f(a_0) + f_1(a_0) \cdot b_0 = 0$. Therefore $v(f(a_1)) \geq 2v(b_0) > v(f(a_0))$. Now $f'(t+x) = f'(t)+2xf_2(t)+\ldots$ implies $v(f'(a_1)-f'(a_0)) \geq v(b_0) \geq v(f'(a_0))$, so $v(f'(a_1)) = v(f'(a_0))$.
This shows that $f(a_i)$ converges to 0 $v(f(a_i)) \to \infty)$.
We now show that (a_i) is a Cauchy sequence:
$v(a_{n+1} - a_n) = v(b_n) = v\left(-\frac{f(a_n)}{f'(a_n)}\right) = v(f(a_n)) - v(f'(a_n)) \to \infty$, because that first summand is strictly monotonously increasing (in $\mathbb{Z}$) and the second summand is constant. So if $m > n$: $v(a_m - a_n) = v((a_m - a_{m-1}) + (a_{m-1} - a_{m-2}) + \ldots + (a_{n+1} - a_n)) \geq \min\{v(a_i - a_{i-1}) \mid n < i \leq m\} \to \infty$ which means that (a_i) is a Cauchy sequence. □

To prove a more general version of Hensel's lemma, we need the fact that finite dimensional vector spaces over complete fields are complete.

Theorem 8.12. *(Hensel's Lemma, more general version) Let (K, v) be a complete discrete valuated field with valuation ring R and maximal ideal πR. Put $F := R/\pi R$ and $^- : R[X] \to F[X]$ the natural epimorphism. Let $f \in R[X]$ be monic such that $\overline{f} = h_0 g_0$ with $\gcd(h_0, g_0) = 1$. Then there are $h(X), g(X) \in R[X]$ such that $\overline{h} = h_0$, $\overline{g} = g_0$ and $f = gh$.*

Proof. We use the fact that v can be extended to a complete valuation on the finite dimensional K-algebra $A := K[X]/(f)$ and that also this algebra is complete, so that we may use the usual Hensel procedure to lift zeros of polynomials in A. (see Skript of Computeralgebra).
For a more elementary proof I refer to the exercises (see also Neukirch, Kapitel II, (4.6)).
By Chinese remainder theorem $F[X]/(\overline{f}) = F[X]/(h_0) \oplus F[X]/(g_0)$. Let $e, e' := 1 - e$ be the idempotents in $F[x]/(\overline{f})$ corresponding to this decomposition and let $e_0 \in \Lambda := R[X]/(f)$ be a preimage of e, so $\overline{e_0} = e$.
We want to lift e_0 to an idempotent in Λ. From this we obtain the required factorisation of f in $R[X]$ again by Chinese remainder theorem.
We apply the usual Newton-Hensel Iteration to $p(X) = X^2 - X$.

We have $p(e_0) \in \pi\Lambda$ and $p'(e_0) = 2e_0 - 1 \in \Lambda \setminus \pi\Lambda$.
Put $e_{n+1} := e_n - p(e_n)/p'(e_n)$ modulo $\pi^{2^{n+1}}\Lambda$ to achieve that $e_n^2 - e_n \in \pi^{2^n}\Lambda$. Modulo $\pi^{2^n}\Lambda$ we compute

$$(2e_n - 1)^2 = 4e_n^2 - 4e_n + 1 \equiv 1 \pmod{\pi^{2^n}\Lambda}.$$

Define the sequence $(e_n) \in \Lambda^{\mathbb{N}_0}$ by

$$e_{n+1} := e_n = (e_n^2 - e_n)(2e_n - 1) = e_n + k_n = 3e_n^2 - 2e_n^3$$

where $k_n = (e_n^2 - e_n)(1 - 2e_n)$.
Claim: For all $n \in \mathbb{N}_0$ we have $e_n^2 - e_n \in \pi^{2^n}\Lambda$ and $(2e_n - 1)^2 - 1 \in \pi^{2^n}\Lambda$.
Proof: This is true for $n = 0$. If it holds for n then

$$e_{n+1}^2 - e_{n+1} = (e_n+k_n)^2 - (e_n+k_n) = e_n^2 - 2e_nk_n + k_n^2 - e_n - k_n = (e_n^2 - e_n)(1 + (2e_n - 1)(1 - 2e_n)) + k_n^2 \in \pi^{2^{n+1}}\Lambda.$$

From this computation we obtain that $(e_n)_{n\in\mathbb{N}}$ is a Cauchy sequence since also $k_n \in \pi^{2^n}\Lambda$. Now $K \otimes \Lambda$ is a finite dimensional vector space over the complete field K and hence again complete (say with respect to the maximum norm, $w(\sum a_i\overline{X}^i) := \min\{v(a_i)\}$, but all norms are equivalent) and therefore (e_n) converges to some $e_\infty \in \Lambda$ with $e_\infty^2 = e_\infty$. For this idempotent one gets $\Lambda = e_\infty\Lambda \oplus (1 - e_\infty)\Lambda$.
To obtain the factorization of the polynomial f, let $e_\infty = a(x) + (f) \in \Lambda$, for some $a(x) \in R[x]$, then $g := \mathrm{ggT}(a, f)$ and $h := \frac{f}{g}$ are the required factors of f in $R[x]$. □

As an exercise you prove a little bit more general version that the previous theorem holds also for primitive polymonials in $f \in R[X]$, i.e. it suffices that one of the coefficients of f is a unit in R.

Example. Factorise $p(x) = x^7 - 1$ in $\mathbb{Z}_2[x]$.
In $\mathbb{Z}[x]$ we compute $p(x) = (x - 1)f(x)$ with $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Since $\mathbb{F}_8$ contains a 7th root of unity we obtain

$$\overline{f} = h_0g_0 \in \mathbb{F}_2[x] \text{ with } h_0 = x^3 + x^2 + 1,\ g_0 = x^3 + x + 1.$$

With the Euclidean algorithm one computes

$$1 = \gcd(h_0, g_0) = xg_0 + (1 + x)h_0 \text{ also } e = xg_0.$$

Put $e_1 := x^4 + x^2 + x \in \mathbb{Z}_2[x]$ then $e_1^2 - e_1 \equiv_f -2(x^4 + x^2 + x + 1)$. Put

$$e_2 := 3e_1^2 - 2e_1^3 \equiv -x^4 - x^2 - x - 10 (\text{modulo f})$$

then

$$e_2^2 - e_2 \equiv_f 4(5x^4 + 5x^2 + 5x + 27).$$

Put

$$e_3 := 3e_2^2 - 2e_2^3 \equiv 595x^4 + 595x^2 + 595x + 2178 (\text{modulo f})$$

Since we only need e_3 modulo 16 we may reduce coefficients modulo 16 and work with $e_3 := 3x^4 + 3x^2 + 3x + 2$. Then

$$e_3^2 - e_3 \equiv_f -16.$$

Put

$$e_4 := 3e_3^2 - 2e_3^3 \equiv 99x^4 + 99x^2 + 99x + 50(\text{modulo f})$$

Then $e_4^2 - e_4 \equiv_f -17152 = 2^8 67$. So by accident we have

$$e_n^2 - e_n \equiv_f a_n \in 2^{2^{n-1}}\mathbb{Z}_2$$

and obtain

$$e_{n+1} = 3e_n^2 - 2e_n^3 = -2(e_n^2 - e_n)e_n + e_n^2 \equiv_f (e_n^2 - e_n) + (1-2a_n)e_n \equiv_f a_n + (1-2a_n)e_n$$

from which we obtain the recursion $(a := a_n)$ $a_{n+1} = 4a_n^3 - 3a_n^2$ since $e_{n+1}^2 - e_{n+1} \equiv_f$

$$(a+(1-2a)e_n)^2 - (a+(1-2a)e_n) = a^2 - a + 2a(1-2a)e_n - 2a(1-2a)e_n^2 + (1-2a)(e_n^2 - e_n) = 4a^3 - 3a^2.$$

8.3 Extension of valuations.

Lemma 8.13. *Let (K, v) be a complete discrete valuated field and $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in K[X]$ irreducible. Then $v(a_i) \geq \min\{v(a_0), v(a_n)\}$ for all $0 \leq i \leq n$.*

Proof. Let $t := \min\{v(a_i) \mid 0 \leq i \leq n\}$ and assume that $t < \min\{v(a_0), v(a_n)\}$. Let r be maximal such that $v(a_r) = t$. Then $r \neq 0$ and $r \neq n$ and $g(X) := a_r^{-1}f(X) = b_0X^n + b_1X^{n-1} + \ldots + b_{n-1}X + b_n \in R[X]$, $b_r = 1$, $b_{r+1}, \ldots, b_n \in \pi R$ and also $g(X) \in R[X]$ is irreducible.
The reduction of g modulo π is

$$\overline{g} = \underbrace{X^{n-r}}_{g_0} \underbrace{(1 + \overline{b}_{r-1}X + \ldots + \overline{b}_0X^r)}_{h_0} \in R/\pi R[X]$$

with $\gcd(g_0, h_0) = 1$. This contradicts the general version of Hensel's lemma for primitive polynomials. □

Theorem 8.14. *Let K be a complete discrete valuated field and L/K finite extension of degree $n = [L : K]$ Then there is a unique discrete valuation $w : L \to \frac{1}{n}\mathbb{Z} \cup \{\infty\}$ that extends the valuation of K. This valuation is given by $w(\alpha) := \frac{1}{n}v(N_{L/K}(\alpha))$ for all $\alpha \in L$ and L is complete.*

Proof. Let $R := R_v \subseteq K$ be the valuation ring of K and $O := \text{Int}_R(L)$ the integral closure of R in L. So

$$O = \{a \in L \mid \exists f \in R[X] \text{ monic, such that } f(a) = 0\} = \{a \in L \mid \mu_a \in R[X]\}.$$

We claim that $O = \{a \in L \mid N_{L/K}(a) \in R\} = \{a \in L \mid w(a) \geq 0\}$.
If $a \in L$, then $\mu_a \in K[X]$ monic and irreducible, so by Lemma 8.13

$$\mu_a \in R[X] \Leftrightarrow \mu_a(0) \in R \Leftrightarrow N_{L/K}(a) \in R.$$

We now show that the map w above is a discrete valuation of L (it clearly extends the valuation of K). The conditions (o), (i), (ii) are clearly fulfilled by the multiplicativity of the norm. To show the strong triangle inequality let we need to show that for all $\alpha, \beta \in L$

$$w(\alpha+\beta) \geq \min\{w(\alpha), w(\beta)\}$$

This is clear if one of them is 0, so assume that both are nonzero and that $w(\alpha) \geq w(\beta)$. Then by (ii) $w(\frac{\alpha}{\beta}) \geq 0$ and hence $\frac{\alpha}{\beta} \in O$. But then also $\frac{\alpha}{\beta}+1 \in O$ and therefore $w(\frac{\alpha}{\beta}+1) = w(\alpha+\beta) - w(\beta) \geq 0$ which proves (iii).
So we have established the existence.
For the uniqueness we need the following Lemma

Lemma 8.15. *Let $f(X) = X^n + a_1X^{n-1} + \ldots + a_n \in K[X]$ irreducible. Then $v(a_k) \geq \frac{k}{n} v(a_n)$ for all $1 \leq k \leq n$.*

Proof. Let L be the splitting field of f and $w : L \to \mathbb{R} \cup \{\infty\}$ be the extension of v to L constructed above. If $f(X) = \prod_{i=1}^n (X - \beta_i) \in L[X]$, then $w(\beta_i) = \frac{1}{n} v(a_n)$ for all i. The coefficient a_k is a homogeneous polynomial in the β_i of degree k, so

$$v(a_k) = w(a_k) \geq kw(\beta_i) = \frac{k}{n} v(a_n).$$

Now assume that there is a second (different) extension w' of the valuation v and choose $\alpha \in L$ such that $w(\alpha) \neq w'(\alpha)$. Wlog we may assume that $w(\alpha) < w'(\alpha)$ (otherwise replace α by α^{-1}). Let $\mu_\alpha := X^m + a_1X^{m-1} + \ldots + a_m \in K[X]$, then $w(\alpha) = \frac{1}{m} v(a_m)$ and all coefficients satisfy $v(a_k) \geq \frac{k}{m} v(a_m) = kw(\alpha)$. Then

$$w'(a_k\alpha^{m-k}) = (m-k)w'(\alpha) + v(a_k) > mw(\alpha) = v(a_m) \text{ for all } k = 0, \ldots, m-1.$$

But $a_m = -a_{m-1}\alpha - \ldots - a_1\alpha^{m-1} - \alpha^m$ and therefore

$$w'(a_m) = v(a_m) \geq \min\{w'(a_k\alpha^{m-k}) \mid k = 0, \ldots, m-1\} > v(a_m)$$

a contradiction. □

Definition 8.16. *Let (K, v) be complete, $R = R_v$, $k = R/\pi R$ the residue field. Let L/K be a finite extension, $w : L^* \to \mathbb{R}$ the extension of v, $O = R_w$ the valuation ring with maximal ideal $\wp O$ and residue field $\ell := O/\wp O$. Then $k \leq \ell$, $v(K^*) \leq w(L^*)$.*
$[\ell : k] =: f = f(w/v)$ is called the **inertia degree** *and*
$[w(L^*) : v(K^*)] =: e := e(w/v)$ the **ramification index** *of w over v.*

Theorem 8.17. *In the situation of the definition above we have $\pi O = \wp^e O$ and $[L : K] = ef$.*

Proof. Clearly $w(L^*) \leq \frac{1}{n}\mathbb{Z}$, so $w(L^*) = \frac{1}{e}\mathbb{Z}$ for some divisor e of n and any element $\wp \in L$ with $w(\wp) = \frac{1}{e}$ is a prime element of O. So $\pi O = \wp^x O$ with $x = w(\pi)/w(\wp) = e$.
To see that $[L : K] = ef$ we construct a K-basis if L. Let $(b_1, \ldots, b_f) \in O$ such that their images form a k-basis of ℓ. We claim that

$$(\wp^i b_j \mid 0 \leq i \leq e-1, 1 \leq j \leq f) \text{ is a } K\text{-basis of } L.$$

These elements are linearly independent: Assume that there are $a_{ij} \in K$ such that $\sum_{i,j} a_{ij} \wp^i b_j = 0$ such that not all a_{ij} are zero. Put $s_i := \sum_j a_{ij} b_j$. Then not all s_i are 0 (choose $a_{ij} \in R$ and not all in πR and use the fact that the b_j form a basis of $O/\wp O$) and if $s_i \neq 0$ then $w(s_i) \in v(K^*)$.
From the fact that $\sum_{i=0}^{e-1} s_i \wp^i = 0$ and $w(s_i \wp^i) \neq w(s_j \wp^j)$ for all $i \neq j$ for which $s_i s_j \neq 0$ we obtain that the nonzero summands have distinct valuations and therefore $w(\sum_{i=0}^{e-1} s_i \wp^i) = \min\{w(s_i \wp^i) \mid 0 \leq i \leq e-1\} < \infty$ a contradiction.
Generating set: Put $M := \langle \wp^i b_j \mid 0 \leq i \leq e-1, 1 \leq j \leq f \rangle_R$. We claim that $M = O$ and hence $(\wp^i b_j \mid 0 \leq i \leq e-1, 1 \leq j \leq f)$ is an integral basis of L.
Clearly $M + \pi O = O$ so

$$O = M + \pi O = M + \pi(M + \pi O) = M + \pi^2 O = \ldots = M + \pi^n O \text{ for all } n \in \mathbb{N}.$$

So M is dense in O, R complete and M finitely generated R-module, so also M is complete and so $M = O$. □

9 p-adic number fields

Definition 9.1. *A* **p-adic number field** *is a finite extension of* $\mathbb{Q}_p$.

Note that any p-adic number field K is a complete discrete valuated field. We assume in the following that K is a p-adic number field with valuation w extending v_p and valuation ring R and prime element π. The inertia degree is denoted by f and the ramification index by e. So

$$d = ef = [K : \mathbb{Q}_p], F_K := R/\pi R \cong \mathbb{F}_{p^f}, pR = \pi^e R.$$

Theorem 9.2. *Let K be a p-adic number field with valuation ring R and prime element π. Then*

$$K^* = \langle \pi \rangle \times \langle \mu_{q-1} \rangle \times U^{(1)} = \langle \pi \rangle \times R^*$$

where $q = |R/\pi R|$, $\mu_{q-1} = \{z \in K \mid z^{q-1} = 1\} \cong C_{q-1}$, $\langle \pi \rangle = \{\pi^k \mid k \in \mathbb{Z}\} \cong \mathbb{Z}$ and $U^{(1)} = 1 + \pi R = \ker(R^* \to (R/\pi)^*)$.

Proof. It suffices to show that $C_{q-1} \cong \mu_{q-1} \subset K^*$. The polynomial $X^{q-1} - 1$ splits completely in $q-1$ distinct linear factors in the residue field $F_K = R/\pi R$. By Hensels lemma this implies that all zeros of $X^{q-1} - 1 \in R[X]$ already lie in R, so $R*$ contains all $q-1$ roots of 1. □

We now aim to obtain an analogue of Dirichlet's unit theorem for the structure of the unit group of R.

Theorem 9.3. *There is a unique continous group homomorphism* $\log : K^* \to K$ *such that* $\log(p) = 0$ *and* $\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$ *for all* $1 + x \in U^{(1)}$.

Proof. Since $(K, +)$ has no torsion, we have $\log(\mu_{q-1}) = \{0\}$ for any group homomorphism log. To show that the series for $\log(1 + x)$ converges note that for $1 + x \in U^{(1)}$ we have $w(x) > 0$ and so

$$w(\frac{x^n}{n}) = nw(x) - v_p(n) \to \infty \text{ for } n \to \infty$$

because $nw(x)$ grows linearly in n but $v_p(n)$ only logarithmically. Therefore $(\frac{x^n}{n})_{n\in\mathbb{N}}$ tends to zero which is (because of the nice properties of an ultra metric) equivalent to the convergence of the series. The homomorphism property follows from the identity of formal power series

$$\log((1+x)(1+y)) = \log(1+x) + \log(1+y).$$

Any $\alpha \in K^*$ can be written uniquely as

$$\alpha = \pi^{ew(\alpha)} \underbrace{\epsilon(\alpha)}_{\in\mu_{q-1}} \underbrace{\tilde{\alpha}}_{\in U^{(1)}}.$$

To define $\log(\pi)$ we first note that the prime element π is not unique, but we have the equation $p = \pi^e \epsilon(p)\tilde{p}$ and then put $\log(\pi) := \frac{-1}{e}\log(\tilde{p})$ and hence

$$\log(\alpha) = ew(\alpha)\log(\pi) + \log(\tilde{\alpha}).$$

This defines a continous group homomorphism with $\log(p) = 0$.
To see the uniqueness let $\lambda : K^* \to K$ be a second logarithm such that $\lambda_{|U^{(1)}} = \log_{|U^{(1)}}$ and $\lambda(p) = 0$. Then $\lambda(\mu_{q-1}) = \{0\}$ and

$$0 = \lambda(p) = e\lambda(\pi) + \lambda(\tilde{p}) = e\lambda(\pi) + \log(\tilde{p}) \text{ implies } \lambda(\pi) = \log(\pi).$$

□

On $U^{(n)}$ the logarithm has a continous inverse, the exponential:

Theorem 9.4. *For any $n > \frac{e}{p-1} =: m$ the mappings*

$$\begin{array}{ll} \exp : \pi^n R \to U^{(n)}, & x \mapsto 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots = \sum_{i=0}^{\infty} \frac{x^i}{i!} \\ \log : U^{(n)} \to \pi^n R, & 1 + x \mapsto \sum_{i=1}^{\infty} \frac{x^i}{i} \end{array}$$

are mutually inverse continuous group isomorphisms.

Proof. Let w be the unique contiuation of the p-adic valuation v_p to K and $v := ew$ be the corresponding normed valuation, so $v(p) = e$, $v(\pi) = 1$.
(a) log is well defined: We need to show that for $v(x) \geq n$ and $i \in \mathbb{N}$ also $v(\frac{x^i}{i}) \geq n$.
For $i = p^a i'$ we have $v(i) = ev_p(i) = ea$. For $a > 0$ (and hence $i > 1$) we obtain

$$\frac{v_p(i)}{i-1} = \frac{a}{p^a i' - 1} \leq \frac{a}{p^a - 1} = \frac{1}{p-1}\frac{a}{p^{a-1} + p^{a-2} + \ldots + 1} \leq \frac{1}{p-1}$$

hence $v_p(i) \leq \frac{i-1}{p-1}$ and so $v(i) = ev_p(i) \leq m(i-1)$ with $m = \frac{e}{p-1}$ as above. Therefore

$$v(\frac{x^i}{i}) \geq in - m(i-1) = (n-m)i + m \geq n \text{ since } i \geq 1, n > m.$$

(b) exp is convergent and maps $\pi^n R$ into $U^{(n)}$.
Let $i = a_0 + pa_1 + \ldots + p^r a_r$ with $0 \leq a_i < p$, $s_i := \sum_{j=0}^{r} a_i \geq 1$. Then

$$v_p(i!) = \frac{i - s_i}{p-1} \Rightarrow v(i!) = \frac{e}{p-1}(i - s_i) = m(i - s_i)$$

and so $v(\frac{x^i}{i!} = iv(x) - m(i - s_i) = i(v(x) - m) + s_i m \geq \frac{i}{p-1}$ and therefore $\exp(x)$ is convergent. Moreover for $i \geq 1$

$$v(\frac{x^i}{i!}) = iv(x) - m(i - s_i) = v(x) + (i-1)v(x) - (i - s_i)m \underbrace{\geq}_{s_i \geq 1} v(x) + (i-1)(v(x) - m) \underbrace{\geq}_{v(x) \geq n > m} v(x)$$

so $\exp(\pi^n R) \subseteq U^{(n)}$.
Now $\exp \circ \log = \mathrm{id}$ and $\log \circ \exp = \mathrm{id}$ since this is an identity of formal power series and hence correct, whenever the series converge. □

Theorem 9.5. *As a $\mathbb{Z}_p$-module the group $U^{(1)} = 1 + \pi R \leq R^*$ is canonically isomorphic to*

$$U^{(1)} \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d \text{ where } \mathbb{Z}/p^a\mathbb{Z} = \{x \in R \mid x^{p^*} = 1\} \text{ torsion of } U^{(1)}$$

as a $\mathbb{Z}_p$ module.

Proof. We first obtain the (continous) $\mathbb{Z}_p$-module structure of $U^{(1)}$:
The group $U^{(1)}$ is an abelian group and hence a $\mathbb{Z}$-module. Let $U^{(i)} := 1 + \pi^i R \leq U^{(1)}$. Then

$$U^{(1)} > U^{(2)} > \dots \text{ and } U^{(i)}/U^{(i+1)} \cong (R/\pi R, +)$$

since $(1 + \pi^i a)(1 + \pi^i b) = 1 + \pi^i(a + b) + \pi^{2i}ab$. So the mapping $(1 + \pi^i a)U^{(i+1)} \mapsto a + \pi R$ defines a group isomorphism $U^{(i)}/U^{(i+1)} \cong (R/\pi R, +)$. Now $R/\pi R$ is a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$-module, so $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/p^n\mathbb{Z}$-module and therefore

$$U^{(1)} = \lim_{\leftarrow} U^{(1)}/U^{(n+1)} \text{ is a } \mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} \text{ module.}$$

More precisely the $\mathbb{Z}_p$-action of $z = (z_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$, $z_i \in \mathbb{Z}/p^i\mathbb{Z}$ on $U^{(1)}$ is given by

$$z * (1 + x) := (1 + x)^z := \lim_{i \to \infty} (1 + x)^{z_i}.$$

For any $x \in \pi R$ the mapping $z \mapsto (1 + x)^z, \mathbb{Z}_p \to U^{(1)}$ is continous: If $z \equiv z' \pmod{p^n}$, then $(1 + x)^z \equiv (1 + x)^{z'} \pmod{U^{(n+1)}}$.
To obtain the rank of the $\mathbb{Z}_p$-module $U^{(1)}$ note that for $n > m = \frac{e}{p-1}$ the mapping $\log : U^{(n)} \to \pi^n R$ is a continous group homomorphism and also a $\mathbb{Z}_p$-module homomorphism, since $\log((1+x)^z) = z \log(1+x)$. So $U^{(n)} \cong \pi^n R \cong \mathbb{Z}_p^d$ as $\mathbb{Z}_p$-module. Since $[U^{(1)} : U^{(n)}] < \infty$ we have $U^{(1)} \cong \mathbb{Z}_p^d \oplus T$ with T finite. Torsion in K^* are roots of unity, and the roots of unity in $U^{(1)}$ are those that map to 1 mod π and hence these are the p-power roots of unity. □

Remark 9.6. *$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ as $\mathbb{Z}_p$-module. Any $\mathbb{Z}_p$-module generating system of K^* is called a* **topological generating system**.

Example. (Proofs as exercise !!)
(a) Let $p > 2$ be an odd prime. Then $\mathbb{Z}_p^* = \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p$ with $\mathbb{Z}_p \cong U^{(1)} = \langle 1 + p \rangle_{\mathbb{Z}_p}$.

$e = 1, p-1 > 1$ so $n = 1 > \frac{e}{p-1}$ works here.
(b) For $p = 2$ there are 2-power roots of 1 in $\mathbb{Z}_2^*$ and

$$\mathbb{Z}_2^* = \langle -1 \rangle \times U^{(2)} = \langle -1 \rangle \times \langle 1+4 \rangle_{\mathbb{Z}_2} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2$$

(c) Let $K = \mathbb{Q}_5[\sqrt{2}]$, so $f = 2$, $e = 1$, $R = \mathbb{Z}_5[\sqrt{2}]$. Then $K^* \cong \langle 5 \rangle \times \langle \zeta_{24} \rangle \times U^{(1)}$ with

$$U^{(1)} = \langle \log(1+5), \log(1+5\sqrt{2}) \rangle \cong 5R = \langle 5, 5\sqrt{2} \rangle$$

indeed $U^{(1)} = \langle 1+5, 1+5\sqrt{2} \rangle_{\mathbb{Z}_5}$.
(d) Let $K = \mathbb{Q}_5[\sqrt{5}]$, so $f = 1$, $e = 2$, $\frac{e}{p-1} < 1$ and therefore

$$K^* = \langle \sqrt{5} \rangle \times \langle \zeta_4 \rangle \times \langle 1+\sqrt{5}, 1+5 \rangle_{\mathbb{Z}_5}.$$

(e) Let $K = \mathbb{Q}_3[\sqrt{3}]$, so $f = 1$, $e = 2$, $\frac{e}{p-1} = 1$ and

$$K^* = \langle \sqrt{3} \rangle \times \langle -1 \rangle \times U^{(1)}$$

but we only know $U^{(2)} = \langle 1+3, 1+3\sqrt{3} \rangle_{\mathbb{Z}_3}$ from the theory. $U^{(1)}/U^{(2)} = \{1, 1+\sqrt{3}, 1-\sqrt{3}\} = \langle 1+\sqrt{3} \rangle \cong C_3$ with $(1+\sqrt{3})^3 = 1 + 3\sqrt{3} + 3\sqrt{3}^2 + \sqrt{3}^3 \equiv 1 + 6\sqrt{3}$ modulo $U^{(3)}$, so

$$U^{(1)} = \langle 1+\sqrt{3}, 1+3 \rangle$$

(f) Let $K = \mathbb{Q}_3[\sqrt{-3}]$, so $f = 1$, $e = 2$, $\frac{e}{p-1} = 1$ and

$$K^* = \langle \sqrt{-3} \rangle \times \langle -1 \rangle \times U^{(1)}$$

but we only know $U^{(2)} = \langle 1+3, 1+3\sqrt{-3} \rangle_{\mathbb{Z}_3}$ from the theory. $U^{(1)}/U^{(2)} = \{1, 1+\sqrt{-3}, 1-\sqrt{-3}\} = \langle 1+\sqrt{-3} \rangle \cong C_3$. But now $(1+\sqrt{-3})^3 = 1 + 3\sqrt{-3} + 3\sqrt{-3}^2 + \sqrt{-3}^3 = -8$ so here $U^{(1)} \cong C_3 \times U^{(2)}$.

Corollary 9.7. *For $n \in \mathbb{N}$ we have*
(a) $[K^* : (K^*)^n] = np^{dv_p(n)}|\mu_n(K)|$.
(b) $[R^* : (R^*)^n] = p^{dv_p(n)}|\mu_n(K)|$.

As Exercise: explicit examples with $n = 2$ and $n = 3$.

9.1 Unramified extensions

Definition 9.8. *Let K be a p-adic number field with valuation ring O_K, prime element π_K, residue field $O_K/\pi_K O_K =: F_K$ of characteristic p, discrete valuation v_K such that $v_K(K^*) = \mathbb{Z}$. Let L/K be a finite extension of K, with valuation ring O_L, prime element π_L, residue field $O_L/\pi_L O_L =: F_L$ of characteristic p, discrete valuation v_L such that $(v_L)_{|K} = v_K$.*

(a) $e(L/K) := v_L(\pi_L)^{-1} = [v_L(L^*) : v_L(K^*)]$ is called the **ramification index** *of L over K.*

(b) $f(L/K) := [F_L : F_K]$ *is called the* **inertia degree** *of* L *over* K*.*

(c) L/K *is called* **unramified***, if* $e(L/K) = 1$*.*

(d) L/K *is called* **purely ramified***, if* $f(L/K) = 1$*.*

(e) L/K *is called* **tamely ramified***, if* $p \not| e(L/K)$*.*

(f) L/K *is called* **wildly ramified***, if* $p \mid e(L/K)$*.*

Theorem 9.9. *Let* L/K *be a finite extension of* p*-adic fields,* $q := |F_K|$*,* $q^f := |F_L|$*. Then there is a unique subfield* $K \leq T \leq L$ *such that* T/K *is unramified and* $[T : K] = f = [F_T : F_K]$*.* $T := T_{L/K}$ *is called the* **inertia field** *of* L/K*. The field* $T = \mathrm{Zerf}_K(X^{q^f} - X)$ *is a Galois extension of* K *with Galois group* $\mathrm{Gal}(T/K) \cong \mathrm{Gal}(F_T/F_K) \cong C_f$*. Any unramified subfield* $K \leq M \leq L$ *with* $e(M/K) = 1$ *is contained in* T*.*

Proof. By Hensel's Lemma all roots of unity in the residue field F_L lift to roots of unity in L and hence $T := \mathrm{Zerf}_K(X^{q^f} - X) \leq L$. This extension has degree f over K and is totally unramified. Totally unramified subfields of L are generated by certain $q^f - 1$ roots of unity (not necessarily primitive) and hence contained in T. □

Theorem 9.10. *Let* K *be a* p*-adic number field,* $|F_K| = q$*. For any* $f \in \mathbb{N}$ *there is a unique unramified extension* $L = T_{L/K}$ *of* K *of degree* f*. This is a galois extension given as* $L = \mathrm{Zerf}_K(X^{q^f} - X)$ *and Galois group* $\cong C_f$*. The restriction map*

$$\alpha : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F_L/F_K) = \langle \mathrm{Frob}_q \rangle, \sigma \mapsto \sigma_{|O_L} \ mod\ \pi_L O_L$$

is a group isomorphism. The preimage $\widetilde{\mathrm{Frob}}_q$ *of* Frob_q *is a generator of* $\mathrm{Gal}(L/K)$ *and called the* **Frobeniusautomorphism** *of* L *over* K*.*

Proof. Clear. The lifting of the Galois automorphisms is proven similarly as in the number field case. □

Theorem 9.11. *If* L/K *is tamely ramified and* $T := T_{L/K}$ *denotes the inertia field of* L/K*, then there is some prime element* $\pi_T \in T$ *such that* $L = T[\sqrt[e]{\pi_T}]$*.*

Proof. Assume wlog that $K = T$ and let w be an extension of v_K to L. Then $[w(L^*) : v_K(K^*)] = e = [L : K]$ and for any prime element π_L of L we have $w(\pi_L) = \frac{1}{e}$. Note that any prime element π_L generates L. We have $\pi_L^e = \pi_K \epsilon$ for some unit $\epsilon \in O_L^*$. Since $F_K = F_L$ there is some unit $b \in O_K^*$ and $u \in 1 + \pi_L O_L$ such that $\epsilon = bu$, so $\pi_L^e = (b\pi_K)u = \pi_K' u$. The polynomial $f(X) := X^e - u \in O_L[X]$ has a zero modulo π_L (take 1). Since e is prime to the characteristic of F_L, the derivative $f'(X) = eX^{e-1}$ satisfies $f'(1) = e \in O_L^*$. By Hensel, we may hence lift 1 to a zero $\beta \in O_L^*$ of $f(X)$, so $\beta^e = u$. Then $\pi_L' := \pi_L \beta^{-1}$ satisfies $(\pi_L')^e = \pi_K'$. It is a zero of the Eisenstein polynomial $(X^e - \pi_K') = \mu_{\pi_L'}$ and hence $L = K[\pi_L']$. □

Remark 9.12. *The compositum of tamely ramified extensions is again tamely ramified and hence any extension L/K contains a maximal tamely ramified subfield $V_{L/K}$.*

$$L \underbrace{\geq}_{p^a} V_{L/K} \underbrace{\geq}_{e'} T_{L/K} \underbrace{\geq}_{f} K$$

with $f = f(L/K)$, $e = e(L/K) = p^a e'$.

So the tamely ramified extensions of K with ramification index e and inertia degree f correspond to $O_T^*/(O_T^*)^e \cong \langle \mu_{q-1} \rangle / \langle \mu_{q-1}^e \rangle$ where T is the unramified extension of degree f of K and $q = p^f$, $p = |F_K|$.

Examples $K = \mathbb{Q}_5$:
Extensions of degree 2: $\mathbb{Q}_5[\sqrt{2}]$ (f=2,e=1), $\mathbb{Q}_5[\sqrt{5}]$, $\mathbb{Q}_5[\sqrt{10}]$.
Extensions of degree 3 $\mathbb{Q}_5[\zeta_{124}]$ (f=3,e=1), $\mathbb{Q}_5[\sqrt[3]{5}]$ since $\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^3 = 1$.
Exercise: Classify all extensions of degree 4 of $\mathbb{Q}_5$.

10 Different and discriminant

Let K be a p-adic number field with valuation ring O_K, prime element π_K and residue field $F_K = O_K/\pi_K O_K$. Let L/K be a finite extension.

Definition 10.1. $S_{L/K} : L \to K, x \mapsto \text{trace}(\text{mult}_x)$ *is called the* **trace** *of L over K.*
$S : L \times L \to K, S(x, y) := S_{L/K}(xy)$ *is called the* **trace bilinear form**.
$O_L^{\#} := \{x \in L \mid S(x, \alpha) \in O_K$ *for all* $\alpha \in O_L\}$ *is called the* **inverse different** *of L/K.*
$O_L^{\#}$ *is a fractional O_L-ideal in L, so $O_L^{\#} = \pi_L^d O_L$ for some $d \in \mathbb{Z}$, $d \leq 0$.*
The **different** *of L/K is $\mathcal{D}(L/K) := \pi_L^{-d} O_L$ and the* **discriminant** *of L/K is the norm*

$$D(L/K) := N_{L/K}(\mathcal{D}(L/K)) = \{N_{L/K}(a) \mid a \in \mathcal{D}(L/K)\} = \pi_K^{-fd} O_K \trianglelefteq O_K.$$

Theorem 10.2. *If L/K is unramified then $\mathcal{D}(L/K) = O_L$, $D(L/K) = O_K$.*

Proof. Let $B := (b_1, \ldots, b_n) \in O_L^n$ be a lift of some F_K-basis of F_L. Since the trace bilinear form of F_L over F_K is non degenerate, the determinant of the Gram matrix of B with respect to S is not a multiple of π_L and hence in O_L^*. Therefore $O_L = O_L^{\#}$. □

Theorem 10.3. *Let $K \subseteq L \subseteq M$. Then*

$$\mathcal{D}(M/K) = \mathcal{D}(M/L)\mathcal{D}(L/K).$$

Proof. Let $O_L^{\#} := \mathcal{D}(L/K)^{-1} = \pi_L^a O_L$, $O_M^{\#} := \mathcal{D}(M/K)^{-1} = \pi_M^c O_M$, and $\mathcal{D}(M/L)^{-1} = \pi_M^b O_M$. For $z \in M$ we compute $S_{M/K}(zO_M) = S_{L/K}(S_{M/L}(zO_M)O_L)$ so

$$\begin{aligned} & z \in \mathcal{D}(M/K)^{-1} \Leftrightarrow S_{M/K}(zO_M) \subseteq O_K \Leftrightarrow S_{M/L}(zO_M) \subseteq \mathcal{D}(L/K)^{-1} = \pi_L^a O_L \\ & \Leftrightarrow S_{M/L}(z\pi_L^{-a} O_M) \subseteq O_L \Leftrightarrow z\pi_L^{-a} \in \mathcal{D}(M/L)^{-1} = \pi_M^b O_M \Leftrightarrow z \in \pi_L^a \pi_M^b O_M \end{aligned}$$

So $\pi_M^c O_M = \pi_L^a \pi_M^b O_M = \pi_M^{b + a \cdot e(M/L)} O_M$. □

Corollary 10.4. *Let $T := T_{L/K}$. Then $\mathcal{D}(L/K) = \mathcal{D}(L/T)$.*

Theorem 10.5. *Assume that $O_L = O_K[\alpha]$ for some $\alpha \in L$ and let $f := \sum_{i=0}^n a_i X^i \in O_K[X]$ denote the minimal polynomial of α over K. Then $\mathcal{D}(L/K) = f'(\alpha)O_L$.*

Proof. Write

$$\frac{f(X)}{X-\alpha} = b_0 + b_1 X + \ldots + b_{n-1}X^{n-1} \in L[X].$$

Then $b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \ldots + a_{n-i+1} \in O_L$ for all i and $(b_0, \ldots, b_{n-1})$ is also an O_K-basis of O_L. Then we claim that the dual basis of $(1, \alpha, \ldots, \alpha^{n-1})$ is given by $\frac{1}{f'(\alpha)}(b_0, \ldots, b_{n-1})$ to deduce that $O_L^{\#} = \frac{1}{f'(\alpha)}O_L$, from which we obtain the theorem. If $\alpha_1, \ldots, \alpha_n$ are the roots of f then

$$S_{L/K}(\frac{f(X)}{X-\alpha}\frac{\alpha^r}{f'(\alpha)}) = \sum_{i=1}^n \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)} = X^r \text{ for } 0 \leq r \leq n-1$$

as the difference is a polynomial of degree $\leq n-1$ with zeros $\alpha_1, \ldots, \alpha_n$. Comparing coefficients we find that

$$S_{L/K}(\frac{b_j}{f'(\alpha)}\alpha^i) = \delta_{ij}.$$

for $0 \leq i, j \leq n-1$. □

Corollary 10.6. *Let L/K be a totally ramified extension, $[L : K] = e(L/K) =: e$ and let w denote the normalized valuation of L. Then $\mathcal{D}(L/K) = \pi_L^s O_L$ with $s = e-1$ if p does not divide e and*

$$e \leq s \leq e - 1 + w(e), \text{ if } p \text{ divides } e.$$

Proof. We have $O_L = O_K[\pi_L]$ for any prime element π_L of L. Moreover $w(\pi_L) = 1$ and $w(K^*) = e\mathbb{Z}$. Let $f := \sum_{i=0}^e a_i X^i$ be the minimal polynomial of π_L over K. Then f is an Eisenstein Polynomial, i.e. $a_e = 1$, $w(a_0) = w(N_{L/K}(\pi_L)) = e$ and the irreducibility of f allows to apply Lemma 8.15 to deduce that $w(a_i) \geq e$ for all $0 \leq i < e$. Theorem 10.5 says that $s = w(f'(\pi_L))$ with

$$f'(\pi_L) = a_1 + 2a_2\pi_L + \ldots + (e-1)a_{e-1}\pi_L^{e-2} + e\pi_L^{e-1}.$$

The w-valuations of the summands lie in different congruence classes modulo $e\mathbb{Z}$ and hence $w(f'(\pi_L))$ is the minimum of these valuations. If $w(e) = 0$ (i.e. the tamely ramified case) then this minimum is $e-1$. Otherwise this minimum s satisfies $e \leq s \leq e - 1 + w(e)$. □

Corollary 10.7. *If L/K is ramified of degree $ef = n$, $e = [L/T_{L/K}]$ then $\mathcal{D}(L/K) = \pi_L^{e-1}O_L$ if L/K is tame. If L/K is wildely ramified, then $\mathcal{D}(L/K) = \pi_L^s O_L$ with $e \leq s \leq e-1+w(e)$ where $w : L^* \to \mathbb{Z}$ is the normalized valuation of L.*

Proof. Because of Corollary 10.4 we may assume that $K = T_{L/K}$ and L/K is totally ramified of degree e. □

Corollary 10.8. *L/K is ramified if and only if $D(L/K) \neq O_K$.*

(i). $\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3$ is tamely ramified and $v_3(D(\mathbb{Z}_3[\sqrt{3}]/\mathbb{Z}_3)) = v_3(12\mathbb{Z}_3) = 1$.

(ii). $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$ is wildly ramified and $v_2(D(\mathbb{Z}_2[\sqrt{3}]/\mathbb{Z}_2)) = v_2(12\mathbb{Z}_2) = 2$.

(iii). $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is wildly ramified and $v_2(D(\mathbb{Z}_2[\sqrt{2}]/\mathbb{Z}_2)) = v_2(8\mathbb{Z}_2) = 3$.

10.1 Cyclotomic p-adic fields

Theorem 10.9. *Let $m \geq 1$ and $\zeta := \zeta_{p^m}$. Then*

(a) $\mathbb{Q}_p[\zeta]/\mathbb{Q}_p$ *is totally ramified of degree* $e = [\mathbb{Q}_p[\zeta] : \mathbb{Q}_p] = \varphi(p^m) = (p-1)p^{m-1}$.

(b) $\mathrm{Gal}(\mathbb{Q}_p[\zeta]/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$.

(c) $\pi := (\zeta - 1)$ *is a prime element of* $\mathbb{Q}_p[\zeta]$ *with norm* $N(\pi) = p$.

(d) $v_p(D(\mathbb{Q}_p[\zeta]/\mathbb{Q}_p)) = p^{m-1}(mp - m - 1)$.

(e) $\mathcal{D}(\mathbb{Q}_p[\zeta]/\mathbb{Q}_p) = \pi^s\mathbb{Z}_p[\zeta]$ *with* $s = p^{m-1}(mp - m - 1) = w(e) + e - p^{m-1}$.

(f) $U^{(1)} = \langle\zeta\rangle \times \langle 1 + \pi^i \mid 2 \leq i \leq p^m, p \not| i \text{ falls } i \neq p^m\rangle$

Proof. ζ is a zero of

$$h(X) := X^{(p-1)p^{m-1}} + X^{(p-2)p^{m-1}} + \ldots + 1 \in \mathbb{Q}_p[X].$$

Put $g(X) := h(X+1)$. Then $g(\pi) = h(\zeta) = 0$, $g(0) = h(1) = p$. As

$$h(X) = (X^{p^m} - 1)/(X^{p^{m-1}} - 1) \equiv (X-1)^{(p-1)p^{m-1}} \pmod{p\mathbb{Z}_p[X]}$$

the polynom g is an Eisenstein polynomial and hence irreducible. We hence conclude (a) and (c). Also (b) follows from the irreducibility of h, as the zeros of h are exactly the powers ζ^a with $a \in \{1, \ldots, p^m\}$ not divisible by p. The valuation ring of $\mathbb{Q}_p[\zeta]$ is $\mathbb{Z}_p[\pi] = \mathbb{Z}_p[\zeta]$, so we may compute the discriminant as $\mathcal{D}(\mathbb{Q}_p[\zeta]/\mathbb{Q}_p) = h'(\zeta)\mathbb{Z}_p[\zeta]$. Now $h(X) = (X^{p^m} - 1)/(X^{p^{m-1}} - 1)$ so

$$h'(X) = \frac{1}{X^{p^{m-1}} - 1}(p^m X^{p^m - 1} - p^{m-1}X^{p^{m-1}-1}h(X))$$

and $h'(\zeta) = \frac{p^m\zeta^{p^m-1}}{\zeta^{p^{m-1}}-1}$. Now $\eta := \zeta^{p^{m-1}}$ is a primitive p-th root of unity, so $N_{\mathbb{Q}_p[\eta]/\mathbb{Q}_p}(\eta - 1) = p$ and hence $N_{\mathbb{Q}_p[\zeta]/\mathbb{Q}_p}(\eta - 1) = p^{p^{m-1}}$. Therefore $v_p(N(h'(\zeta)) = p^{m-1}(p-1)m - p^{m-1} = p^{m-1}(mp - m - 1)$.

To conclude the last statement note that $\mathcal{D}(Q_p[\zeta]/\mathbb{Q}_p) = \pi^s\mathbb{Z}_p[\zeta]$ with $s = p^{m-1}(mp-m-1)$ by (d). Now $e = p^m - p^{m-1}$, so $w(e) = (m-1)w(p) = (m-1)(p^m - p^{m-1})$ and

$$w(e) + e - p^{m-1} = (m-1)(p^m - p^{m-1}) + p^m - p^{m-1} - p^{m-1} = mp^m - mp^{m-1} - p^{m-1}.$$

□

Corollary 10.10. *Let $n = p^m k \in \mathbb{N}$ such that p does not divide k and ζ_n be a primitive n-th root of unity..*

(a) $\mathbb{Z}_p[\zeta_n]$ is the valuation ring of $\mathbb{Q}_p[\zeta_n]$.

(b) $T := T(\mathbb{Q}_p[\zeta_n]/\mathbb{Q}_p) = \mathbb{Q}_p[\zeta_n^{p^m}]$ is the maximal unramified subfield.

(c) $f = [T : \mathbb{Q}_p]$ is the order of p in $(\mathbb{Z}/k\mathbb{Z})^*$.

(d) $e(\mathbb{Q}_p[\zeta_n]/\mathbb{Q}_p) = (p-1)p^{m-1}$.

(e) $V(\mathbb{Q}_p[\zeta_n]/\mathbb{Q}_p) = \mathbb{Q}_p[\zeta_n^{p^{m-1}}]$ is the maximal tamely ramified subfield.

11 Application to algebraic number fields

11.1 Completion and field extensions

Let (K, v) be a discretely valuated field with completion K_v. Then $v : K_v \to \mathbb{Z} \cup \{\infty\}$ has a unique extension to a valuation $\overline{v}$ of the algebraic closure $\overline{K_v}$. Now let L/K be a finite extension. Any embedding $\tau : L \to \overline{K_v}$ defines a valuation $w_\tau = \overline{v} \circ \tau$ of L that extends v.

Theorem 11.1. *All extensions of v to L are of the form $w_\tau = \overline{v} \circ \tau$. We have that $w_\tau = w_{\tau'}$ if and only if $\tau' = \sigma \circ \tau$ for some $\sigma \in \mathrm{Aut}_{K_v}(\overline{K_v})$ (then we say that τ and τ' are conjugate over K_v).*

Proof. Let w be an extension of v to L with corresponding completion L_w; view w as the valutaion of L_w extending $v : K_v \to \mathbb{Z} \cup \infty$. As L_w is an algebraic extension of K_v and the uniqueness of extension of valuations for complete fields, we have $w = \overline{v} \circ \tau$ for all embeddings $\tau \in \mathrm{Hom}_{K_v}(L_w, \overline{K_v})$. Any other such embedding is of the form $\sigma \circ \tau$ as in the theorem. □

Assume that L/K is separable with primitive element $\alpha \in L$, so $L = K(\alpha)$. Let $f := \mu_{\alpha,K} \in K[X]$ denote the minimal polynomial of α. Then $f = g_1 \cdots g_r \in K_v[X]$.

Corollary 11.2. *The valuations $\{w_1, \ldots, w_r\}$ of L that extend v are in bijection with the irreducible factors of $f \in K_v[X]$. For $a \in L$ we have*

$$L \otimes_K K_v = \bigoplus_{i=1}^r L_{w_i}, \;\; N_{L/K}(a) = \prod_{i=1}^r N_{L_{w_i}/K_v}(a), \;\; \text{and } S_{L/K}(a) = \sum_{i=1}^r S_{L_{w_i}/K_v}(a).$$

Proof. Any K-linear embedding of L into $\overline{K}$ is uniquely determined by mapping α to some zero β of f. Two such embeddings are conjugate over K_v if and only if these zeros are zeros of the same irreducible factor g_i. Clearly

$$L \otimes_K K_v \cong K_v[X]/((f(X)) \cong \bigoplus_{i=1}^r K_v[X]/(g_i(X)) \cong \bigoplus_{i=1}^r L_{w_i}.$$

The characteristic polynomial of any $a \in L$ is the product of the characteristic polynomials of the corresponding elements $a_i \in L_{w_i}$ where $(a_1, \ldots, a_r)$ denotes the image of $a \otimes 1$ under the above isomorphism. From this we obtain the equations for norm and trace. □

Let K be an algebraic number field with ring of integers R. Any prime ideal $P \trianglelefteq R$ of R defines a valuation

$$v_P : K^* \to \mathbb{Z},\ v_P(\alpha) := \max\{a \in \mathbb{Z} \mid \alpha \in P^a\}$$

with valuation ring $R_{(P)} := \{\frac{a}{b} \in K = \mathrm{Quot}(R) \mid b \notin P\}$. The completion K_P of K at v_P is a p-adic number field, where $p\mathbb{Z} = P \cap \mathbb{Z}$. If $P(R)$ denotes the set of all maximal ideals of R, then

$$R = \bigcap_{P \in P(R)} R_{(P)}.$$

Remark 11.3. *Let $P \trianglelefteq R$ be a maximal ideal of R. Then*

$$P\mathbb{Z}_L = \wp_1^{e_1} \ldots \wp_r^{e_r}$$

for pairwise distinct prime ideals $\wp_i \trianglelefteq \mathbb{Z}_L$ and the inequivalent valuations of L that extend $v := v_P$ are

$$w_1 = \frac{1}{e_1} v_{\wp_1}, \ldots, w_r = \frac{1}{e_r} v_{\wp_r}.$$

Then e_i is the ramification index of L_{w_i} over K_v and $f_i := [\mathbb{Z}_L/\wp_i : \mathbb{Z}_K/P]$ the inertia degree of L_{w_i} over K_v. As $[L_{w_i} : K_v] = e_i f_i$ we re-obtain the formula

$$[L : K] = \sum_{i=1}^{r} [L_{w_i} : K_v] = \sum_{i=1}^{r} e_i f_i.$$

11.2 A review of Hilbert's ramification theory

Let $L \supseteq K$ be algebraic number fields and assume that L/K is Galois. Let $G := \mathrm{Gal}(L/K)$ denote the Galois group. Let P be a prime ideal of $\mathbb{Z}_K$. Then G acts transitively on the set of prime ideals of $\mathbb{Z}_L$ that contain P and as in Section 6.2

$$P\mathbb{Z}_L = (\wp_1 \cdots \wp_r)^e.$$

Let $\wp := \wp_1$ and put

$$G_\wp := \{\sigma \in G \mid \sigma(\wp) = \wp\}$$

the decomposition group of $\wp$ and $Z := Z_\wp := \mathrm{Fix}_{G_\wp}(L) := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G_\wp\}$ the decomposition field of $\wp$.

Denote by $\wp_Z := \wp \cap Z$. Then $\wp_Z \mathbb{Z}_L = \wp^e$, $f_{L/Z}(\wp) = f_{L/K}(\wp)$, $e_{L/Z}(\wp) = e_{L/K}(\wp) = e$ and $e_{Z/K}(\wp_Z) = f_{Z/K}(\wp_Z) = 1$.

Corollary 11.4. *Let $\nu := \nu_{\wp_Z} : Z \to \mathbb{Z} \cup \{\infty\}$ denote the $\wp_Z$-adic valuation of Z. Then $\omega := \frac{1}{e}\nu_\wp$ is the unique extension of ν to L.*

$I_\wp := \{\sigma \in G_\wp \mid \sigma(x) \equiv x \pmod{\wp} \text{ for all } x \in \mathbb{Z}_L\}$ the inertia group with fixed field $T_\wp := \mathrm{Fix}(I_\wp)$. Then $T_\wp/Z_\wp$ is a Galois extension with Galois group C_f.

Definition 11.5. *For $s \in \mathbb{N}_0$ we put*

$$G_s := G_s(\wp) := \{\sigma \in G_\wp \mid \sigma(x) \equiv x \pmod{\wp^{s+1}} \text{ for all } x \in \mathbb{Z}_L\}$$

the higher decomposition groups.

Remark 11.6. *$G_0 = I_\wp$ and $G_s \trianglelefteq G_\wp$ for all s.*

Let $L_\wp$ denote the completion of L at $\nu_\wp$, $Z_{\wp_Z}$ the completion of Z at $\nu_{\wp_Z}$. Let R be the valuation ring of $L_\wp$ andπ be a prime element of R.

Remark 11.7. Gal$(L_\wp/Z_{\wp_Z}) \cong G_\wp$. *The completion T of $T_\wp$ at $\wp_Z$ is the maximal unramified subfield and $L_\wp = T[\pi]$ is totally ramified over T.*

Recall that $R^\times \geq U^{(1)} \geq U^{(2)} \geq \ldots \geq U^{(i)} = 1 + \pi^i R$.

Theorem 11.8. *Let $s \geq 1$. Then there is an injective group homomorphism*

$$G_s/G_{s+1} \to U^{(s)}/U^{(s+1)}, \sigma G_{s+1} \mapsto \sigma(\pi)\pi^{-1}U^{(s+1)}.$$

In particular G_1 is the unique Sylow p-subgroup of $G_\wp$ and the fixed field of G_1 is the unique tamely ramified subfield of L/Z.

Proof. As $L_\wp = T[\pi]$ any element in $\sigma \in G_s$ is uniquely determined by $\sigma(\pi)$. If $\sigma \in G_s$ then $\sigma(x) \equiv x \pmod{\pi^{s+1}}$ for all $x \in R$. In particular $\sigma(\pi) \equiv \pi \pmod{\pi^{s+1}}$ so $\sigma(\pi)\pi^{-1} \in U^{(s)}$. The set $\{\sigma \in G_s \mid \sigma(\pi)\pi^{-1} \in U^{(s+1)}\} = G_{s+1}$. Now let $\sigma, \tau \in G_s$. Then

$$(\sigma(\tau(\pi)))\pi^{-1} = (\sigma(\tau(\pi))\tau(\pi)^{-1})(\tau(\pi)\pi^{-1})$$

and the homomorphism property follows from the fact that

$$(\sigma(\tau(\pi))\tau(\pi)^{-1})U^{(s+1)} = \sigma(\pi)\pi^{-1}U^{(s+1)}.$$

To see this write $\sigma(\pi) = \pi + x\pi^{s+1}$, $\tau(\pi) = \pi + y\pi^{s+1}$. Then $\sigma(\tau(\pi)) = \sigma(\pi) + \sigma(y)\sigma(\pi)^{s+1} = \pi + (x + \sigma(y))\pi^{s+1} + z\pi^{s+2}$ and $\sigma(\tau(\pi))\tau(\pi)^{-1} =$

$$(\pi + (x + \sigma(y))\pi^{s+1} + z\pi^{s+2})(\pi + y\pi^{s+1})^{-1} = (1 + (x + \sigma(y))\pi^s + z\pi^{s+1})(1 + y\pi^s)^{-1} \equiv 1 + (x + \sigma(y) - y)\pi^s)$$

modulo $U^{(s+1)}$. Now $\sigma(y) \equiv y \pmod{\pi^s}$ in particular $\sigma(\pi)\pi^{-1} = 1 + x\pi^s \equiv \sigma(\tau(\pi))\tau(\pi)^{-1} \pmod{U^{(s+1)}}$. □

11.3 Local properties

Let R be a Dedekind domain and $K = \text{Quot}(R)$. For a prime ideal $\wp$ the **localization** of R at $\wp$ is

$$R_{(\wp)} := \{\frac{r}{s} \in K \mid s \notin \wp\}.$$

This is the discrete valuation ring with respect of the $\wp$-adic valuation of K,

$$\nu_\wp : K \to \mathbb{Z} \cup \{\infty\}, \nu_\wp(a) = i \Leftrightarrow aR = \wp^i A$$

for some fractional ideal A "prime to $\wp$". We also denote by $K_\wp$ the completion of K at $\wp$ with complete discrete valuation ring $R_\wp$.

Let V be a K-vector space and L an R-lattice in V. The **localization** of L is $R_{(\wp)}L$ and an $R_{(\wp)}$-lattice in V. The **completion** of L at $\wp$ is $R_\wp L$.

Definition 11.9. *A property is called a* **local property***, if it holds for an R-module M if and only if it holds for all the localisations $R_\wp M$ if and only if it holds for all completions $R_\wp M$ for all prime ideals $\wp$ of R.*

Equality of lattices is a local property:

Theorem 11.10. *Let R be a Dedekind domain with field of fractions K. Let V be a finite dimensional K-vector space and let L, M be two R-lattices in V. Then the following are equivalent:*
(1) $L = M$.
(2) $L_{(\wp)} := R_{(\wp)}L = M_{(\wp)}$ for all maximal ideals $\wp \trianglelefteq R$.
(3) $R_\wp \otimes L = R_\wp \otimes M$ for all maximal ideals $\wp \trianglelefteq R$.

Note that a **lattice** is an R-submodule of V that is finitely generated and contains a basis of V. In particular if L and M are R-submodules of V such that $L \leq M$ and $\mathrm{Ann}(M/L) \neq \{0\}$ then if one of L or M is a lattice then so is the other.
Proof. (1) ⇒ (2) ⇒ (3) is clear.
To see that (3) implies (1) we use contraposition:
So assume that $L \neq M$, wlog $L \not\subseteq M$ and let $\ell \in L \setminus M$. Multiply ℓ with some element of R to achieve that $\ell \notin M$ but $\wp\ell \subseteq M$ for some maximal ideal $\wp$ of R. Then $\ell \notin R_\wp \otimes M$ so $R_\wp \otimes L \neq R_\wp \otimes M$ for this prime ideal $\wp \trianglelefteq R$. □

Theorem 11.11. *Let R be a Dedekind domain, V a K-vectorspace and L some R-lattice in V.*
(a) For any R-lattice M in V we have $M_{(\wp)} = L_{(\wp)}$ for all but finitely may maximal ideals $\wp$ of R.
(b) Let $X(\wp)$ be $R_{(\wp)}$-lattices in V for all maximal ideals $\wp$ of R such that $X(\wp) = L_{(\wp)}$ for all but finitely may $\wp$. Then $M := \bigcap_\wp X(\wp)$ is a lattice in V such that $M_{(\wp)} = X(\wp)$ for all $\wp$.
(c) Let $L_\wp$ denote the completion $L_\wp := R_\wp \otimes L$ which is an $R_\wp$-lattice in $V_\wp := K_\wp \otimes V$. Then
(i) $L = V \cap (\bigcap_\wp L_\wp)$.
(ii) Let $\hat{X}(\wp)$ be an $R_\wp$-lattice in $V_\wp$ for all maximal ideals $\wp$ of R such that $\hat{X}(\wp) = L_\wp$ for all but finitely may $\wp$. Then $M := V \cap \bigcap_\wp \hat{X}(\wp)$ is a lattice in V such that $M_\wp = \hat{X}(\wp)$ for all $\wp$.
(d) Let $\wp$ be some maximal ideal in R. Then there are bijections

$$\{M \leq L \mid L/M \textit{ is } \wp\textit{-torsion}\} \to \{M \leq L_{(\wp)} \mid M \textit{ full lattice}\} \to \{M \leq L_\wp \mid M \textit{ full lattice}\}$$

$M \mapsto M_{(\wp)} \mapsto M_\wp$ with inverse mapping $M_{(\wp)} \mapsto L \cap M_{(\wp)}$ and similarly $M_\wp \mapsto L \cap M_{(\wp)}$.

Proof. (a) $Y := L + M/L \cap M$ is an R-module of finite length. Let $A := \mathrm{Ann}_R(Y)$. Then $A \trianglelefteq R$ and for all prime ideals $\wp$ with $A \not\subseteq \wp$ we have $L_{(\wp)} = M_{(\wp)}$.
(b) For all but finitely many $\wp$ we have $X(\wp) = L_{(\wp)}$. For the other (finitely many) maximal ideals $\wp$ with have

$$X(\wp) \cap L_{(\wp)} \subseteq X(\wp), L_{(\wp)} \subseteq X(\wp) + L_{(\wp)}.$$

As both are $R_{(\wp)}$-lattices in V, we have that $\mathrm{Ann}((X(\wp)+L_{(\wp)})/(X(\wp)\cap L_{(\wp)})) = \wp^{a_\wp}$ for some $a_\wp \in \mathbb{Z}_{\geq 0}$. So

$$L \cap M \subseteq M, L \subseteq L + M$$

and $\mathrm{Ann}((L+M)/(L\cap M)) = \prod \wp^{a_\wp}$ is a finite product of prime ideals and hence an ideal in R. As L is a lattice, so is M.
(c) follows from (b) by noting that $V \cap L_\wp = L_{(\wp)}$
(d) Is a consequence of (b) and (c). □

11.4 The discriminant of an algebraic number field

Corollary 11.12. *Let $M := \mathbb{Z}_L$, $R = \mathbb{Z}_K$ $P\mathbb{Z}_L = \wp_1^{e_1}\ldots\wp_r^{e_r}$ as before. Then*

$$R_P \otimes_R \mathcal{D}(M/R) = \prod_{i=1}^{r} \mathcal{D}(M_{w_i}/R_P)$$

and

$$\mathcal{D}(M/R) = \prod_{\wp \in P(M)} M \cap \mathcal{D}(M_\wp/R_{\wp\cap R}).$$

In particular one may read of the $\wp$-component of $\mathcal{D}(M/R)$ from $\mathcal{D}(M_\wp/R_{\wp\cap R})$.

From Corollary 10.7 we now get:

Corollary 11.13. *Let L/K be an extension of algebraic number fields and $\wp$ a prime ideal of $\mathbb{Z}_L$. Then $\wp$ ramifies in L/K if and only if $\wp$ divides $\mathcal{D}(L/K)$. Let $\wp^s$ be the maximal $\wp$-power dividing $\mathcal{D}(L/K)$ and e be the ramification index of $\wp$ in L/K. Then*

(i) If $e \notin \wp$ (so $\wp$ is tamely ramified) then $s = e-1$.

(ii) If $e \in \wp$ (so $\wp$ is wildly ramified) then $e \leq s \leq e-1+\nu_\wp(e)$.

As an application of the Geometry of Numbers we obtain explicit bounds on the discriminant:

Theorem 11.14. *(see Neukirch Satz III (2.14)) Using Exercise 2 on Sheet 4 one can prove that $|d_K|^{1/2} \geq \frac{n^n}{n!}\frac{\pi}{4}^{n/2}$ where $n = [K:\mathbb{Q}]$. In particular there are no unramified extensions of degree $n > 1$ of $\mathbb{Q}$.*

Theorem 11.15. *Let S be a finite set of prime ideals of the algebraic number field K. Then there are only finitely many extensions L/K of given degree $n = [L:K]$ that are unramified outside of S.*

Index