Algebraic Number Theory
Vorlesung 2011

Prof. Dr. G. Nebe, Lehrstuhl D für Mathematik, RWTH Aachen

Contents

Literatur:

Neukirch, Algebraische Zahlentheorie
Reiner, Maximal Orders
Stichtenoth, Algebraic Function Fields (Seminar)

Chapter 1

Commutative Theory.

All rings are associative and have a unit.

1.1 The ring of integers

1.1.1 The integral closure

Definition 1.1.1. *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 1.1.2. *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 1.1.3. *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 1.1.4. *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 $A[b]$ 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 1.1.5. *Let B be a commutative A-algebra and*

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

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_1b_2. □

Theorem 1.1.6. *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 1.1.7. *Let A be an integral domain with field of fraction $K := Quot(A)$.*

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

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 1.1.8. *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 1.1.9. *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.

1.1.2 Norm, Trace and Discriminant.

Remark 1.1.10. *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* $\chi_{\alpha,K} = X^n - a_1X^{n-1} + \ldots + (-1)^{n-1}a_{n-1}X + (-1)^n a_n \in K[X]$, *then* $N_{L/K}(\alpha) = a_n$ *and* $S_{L/K}(\alpha) = a_1$.

Proof. Exercise. □

Theorem 1.1.11. *Assume that* L/K *is a finite separable extension and let* $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ *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* $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\} = \{\alpha_1, \ldots, \alpha_d\}$ *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 1.1.10 (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 $\varphi_1, \ldots, \varphi_d$ 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 of K into the algebraic closure 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 $j = 1, \ldots, d$ and let $\{\tau_1, \ldots, \tau_{n/d}\} = \mathrm{Hom}_{K(\alpha)}(E, \overline{K})$. Then

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

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

Corollary 1.1.12. *Let* $K \subseteq L \subseteq M$ *be a tower of separable field extensions of finite degree. Then*

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

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

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

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

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 1.1.13. *Let L/K be a separable extension an 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 1.1.14. *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 1.1.15. *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 1.1.16. *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 1.1.17. *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.

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

Definition 1.1.18. *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 1.1.19. *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.

1.1.3 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 1.1.20. *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 1.1.21. *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 1.1.22. *Any finite integral domain R is a field.*

Proof. Let $0 \neq a \in R$, then $\text{mult}_a : R \to R$ 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 $\text{mult}_a(x) = 1$. □

Definition 1.1.23. *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**

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

is the ideal generated by A and B.

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

Main theorem 1.1.24. *Any ideal $0 \neq I \trianglelefteq R$ in R has a unique factorization into prime ideals,*

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

For the proof we need two lemmata:

Lemma 1.1.25. *If $0 \neq I \trianglelefteq R$ then there are 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 1.1.26. *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 1.1.27. *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 1.1.24
Existence. Let $\mathcal{M} := \{\mathcal{A} \trianglelefteq R \mid 0 \neq \mathcal{A} \neq R, \mathcal{A} \neq \wp_1 \dots \wp_s \text{ for all prime ideals } \wp_1, \dots, \wp_s \text{ and all } s \in \mathbb{N}\}$. 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 1.1.26 that if a prime ideal $\wp$ divides the product of two ideals, then it divides one of the factors

$$I_1I_2 \subseteq \wp \Rightarrow I_1 \subseteq \wp \text{ or } I_2 \subseteq \wp.$$

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

Remark 1.1.29. *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 $J = \langle \alpha_1, \ldots, \alpha_n \rangle_R$, $\alpha_i = \frac{\beta_i}{\gamma_i} \in K$ wit $\beta_i, \gamma_i \in R$. Let $\gamma := \gamma_1 \ldots \gamma_n$. Then $\mathcal{A} := \gamma J \trianglelefteq R$ and $J = \gamma^{-1}\mathcal{A}$. □

Theorem 1.1.30. *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 1.1.31. *Any fractional ideal $\mathcal{A}$ of R has a unique factorization*

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

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

Definition 1.1.32. *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

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

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

1.2 Geometry of numbers.

Definition 1.2.1. *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*

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

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 1.2.2. *$E(B)$ 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 1.2.3. *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 1.2.4. *(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

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

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

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 1.2.5. *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

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

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 1.2.6. *The mappings*

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

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

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

*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 1.2.8. *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 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 1.2.9. *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 1.2.10. *For any two nonzero integral ideals $\mathcal{A}, \mathcal{B}$ we have*

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

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 $\mathcal{A}\mathcal{B} = \mathcal{A} \cap \mathcal{B}$ and by Chinese Remainder Theorem $\mathbb{Z}_K/\mathcal{A}\mathcal{B} \cong \mathbb{Z}_K/\mathcal{A} \times \mathbb{Z}_K/\mathcal{B}$ has order

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

(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 $|\mathbb{Z}_K/\wp^n| = \prod_{i=1}^n |\wp^{i-1}/\wp^i| = N(\wp)^n$. □

1.3 Finiteness of the ideal class group.

Remark 1.3.1. *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 $[K : \mathbb{Q}] = r + 2s = n$,

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

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

Theorem 1.3.2. *Let $0 \neq \mathcal{A} \trianglelefteq \mathbb{Z}_K$ be an ideal. For any $i \in \{1, \ldots, r+s\}$ 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 $X := \{(x_1, \ldots, x_n) \in K_{\mathbb{R}} \mid |x_i| \leq c_i \text{ for all } 1 \leq i \leq n\}$. Then X and its image $m(X)$ is convex and centrally symmetric, where $m : K_{\mathbb{R}} \to \mathbb{R}^{r+2s}$,

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

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

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

$(\prod_{i=1}^{r} 2c_i) \prod_{j=1}^{s} 2\pi c_{r+j}^2 = 2^{r+s}\pi^s \prod_{i=1}^{n} c_i > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} N(\mathcal{A}) = 2^{r+2s} \,\text{vol}(\mathbb{R}^n/\Gamma)$ 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 1.3.3. *Recall that the class group of K is $\text{Cl}_K := J_K/P_K$ 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 $[\mathcal{A}] \in \text{Cl}_K$ 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, $h_K := |\operatorname{Cl}_K|$ *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 1.3.2 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 $\mathcal{A}$ 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 $\operatorname{Cl}_K = \langle [\wp_2] \rangle \cong C_2$.

Remark 1.3.4. *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 1.3.5. *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.

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 1.4.1. *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 1.4.2. *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 1.4.3. *Let $\lambda := \ell \circ j : \mathbb{Z}_K^* \to \mathbb{R}^{r+s}$. Then λ is a group homomorphism with*

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

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 1.4.4. *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 1.4.5. *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 $X := \{(x_1, \ldots, x_r, y_1, \ldots, y_s, \overline{y}_1, \ldots, \overline{y}_s) \in K_{\mathbb{R}} \mid |x_i| < c_i, |y_j|^2 < d_j\}$. 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

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

We then claim that $U = \cup_{\epsilon \in \mathbb{Z}_K^*} Tj(\epsilon)$.
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 1.4.6. *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 1.4.7. *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 1.4.8. *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. □

1.5 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 1.5.1. *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 1.5.2. *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 1.5.3. *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 1.5.4. *Let $O \subset K$ be an order. Then*

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

Theorem 1.5.5. *$\mathcal{M}(O)$ 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 1.5.1 (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 1.5.1 (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 1.5.6. *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 1.5.7. *(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 $N_{K/\mathbb{Q}}(\epsilon) = -1$.
(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 1.5.8. *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*

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

Proof. $\Rightarrow$: 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

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

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

Definition 1.5.9. *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 1.5.8 immediately implies

Theorem 1.5.10. *Let $\Gamma_i = \langle 1, \gamma_i \rangle \in \mathcal{M}(O)$, γ_i admissible $i = 1, 2$. Then*

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

Definition 1.5.11. *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 1.5.12. *$\mathrm{Cl}_0(O_f)$ 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 $\gamma \in \mathbb{Q}[\sqrt{disc(F)}] = \mathbb{Q}[\sqrt{f^2 d_K}] = K$. □

1.5.1 Imaginary quadratic number fields.

Theorem 1.5.13. *Let $D = f^2 d_K < 0$. Then*

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

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 $a \le c$ 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 1.5.14. *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 1.5.15. *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 1.5.16. *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 1.5.17. $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2 \cong \Omega_2(\mathrm{Cl}(K)) = \{[I] \mid [I]^2 = 1\} \cong C_2^{g-1}$ *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 1.5.18. *(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 1.5.19. *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 1.5.20. *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 1.5.21. *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.

1.6 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 1.6.1. *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 1.6.2. *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. □

1.6.1 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 1.6.3. *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 1.6.4. *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*

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

Proof. 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 1.6.5. *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 $\mathbb{Z}_L$. $d_L = 1600$, $\text{disc}(f) = 14400 = 9d_L$.

f	(mod 2)	$(X^2 + X + 1)^2$	$(2) = \wp_2^2$	$e = f = 2$
f	(mod 3)	$(X + 2)^2(X^2 + X + 2)$		
f	(mod 5)	$(X^2 + X + 2)^2$	$(5) = \wp_5^2$	$e = f = 2$
f	(mod 7)	$(X^2 + 4)(X^2 + 2X + 5)$	$(7) = \wp_7\wp'_7$	$e_1 = e_2 = 1, f_1 = f_2 = 2$

1.6.2 Hilbert's theory of ramification for Galois extensions.

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

Remark 1.6.6. *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 1.6.7. *The Galois group acts transitively on the set of prime ideals of $\mathbb{Z}_L$ that contain a given prime ideal $\wp$ of $\mathbb{Z}_K$:*

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

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 1.6.8. $e_1 = \dots = e_r =: e$, $f_1 = \dots = f_r =: f$ *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 1.6.9. *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 $Z_\wp := \text{Fix}_{G_\wp}(L) := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G_\wp\}$ is called the* **decomposition field** *of $\wp$.*

Theorem 1.6.10. *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 1.6.11. *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 1.6.12.

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

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 1.6.13. *$T_\wp/Z_\wp$ 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 $5\mathbb{Z}_Z = p_5 p_5'$ 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 $2\mathbb{Z}_L = \wp_2^3 = (\sqrt[3]{2})^3$, $T_{\wp_2} = \mathbb{Q}[\zeta_3]$, $Z_{\wp_2} = \mathbb{Q}$, $G_{\wp_2} = G$, $e = 3, f = 2$.

1.7 Cyclotomic fields.

Definition 1.7.1. *The* **cyclotomic polynomials** *are defined recursively by*

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

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

Remark 1.7.2. *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) $\Phi_n(X) = \prod_{d\in(\mathbb{Z}/n\mathbb{Z})^*} \zeta_n^d$ *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 1.7.3. *(cyclotomic units)*
(a) Assume that $n = p^a$ is a prime power and let $i, j \in \mathbb{N}$ such that $p \nmid ij$. 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 1.7.4. *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

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

where $s = p^{a-1}(ap - a - 1)$. □

Theorem 1.7.5. *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 1.7.6. *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 prime in K_n.

Theorem 1.7.7. *Let $n = p_1^{a_1} \cdots p_s^{a_s} \in \mathbb{N}$. For any prime p define $v_p(n) := a$ if $n = p^a b$ with $p \not| b$. Let $f_p \in \mathbb{N}$ be minimal such that $p^{f_p} \equiv 1 \pmod{n/p^{v_p(n)}}$. Then*

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

Proof. We need to factorise $\overline{\Phi}_n(X) \in \mathbb{F}_p[X]$. Let $n = p^a m$ with $p \not| m$, $a = v_p(n)$. If $\{\alpha_i \mid 1 \leq i \leq \varphi(p^a)\}$ is the set of primitive p^a-th roots of unity and $\{\beta_i \mid 1 \leq i \leq \varphi(m)\}$ is the set of primitive m-th roots of unity then

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

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

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

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_p. □

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

1.7.1 Quadratic Reciprocity.

Theorem 1.7.9. *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 1.7.10. *Let $2 \neq p$ be a prime, $a \in \mathbb{Z}$ such that $p \nmid a$.*

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

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

Remark 1.7.11. *(a)* $\left(\frac{a}{p}\right) = 1 \Leftrightarrow (a + p\mathbb{Z}) \in (\mathbb{Z}/p\mathbb{Z}^*)^2 \Leftrightarrow a^{(p-1)/a} \equiv_p 1$.
(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
(c) Let $a \in \mathbb{Z}$ 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 1.7.12. *(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

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

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 1.7.9. 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 $\Leftrightarrow$

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

□

1.8 Discrete valuation rings.

Definition 1.8.1. *(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 1.8.2. *$v(x+y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.*

Proof. First note that $v(\zeta) = 0$ for any $\zeta \in R$ 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 1.8.3. *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 1.8.4. *(a) Let R be a discrete valuation ring with maximal ideal $\wp = \pi R \neq \{0\}$. Then $K := \mathrm{Quot}(R) = \dot{\cup}_{i \in \mathbb{Z}} \pi^i R^* \cup \{0\}$ 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 1.8.5. *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 1.8.6. *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) □

1.8.1 Completion

Remark 1.8.7. *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 1.8.8. *A metric space (M,d) is called* **complete***, if any Cauchy sequence in M converges towards a limit in M.*

Theorem 1.8.9. *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 1.8.10. *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 $a + \pi^i R \mapsto a + p^{i-1}R$ are ring homomorphisms.
φ is injective because $\bigcup_{i=0}^{\infty} \pi^i R = \{0\}$.
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 $2, 3, 7$.

1.8.2 Hensel's Lemma

Theorem 1.8.11. *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. □

Theorem 1.8.12. *(Hensel's Lemma, more general version) Let (K, v) be a complete discrete valuated field with valuation ring R and maximal ideal πR. Put $F := R/\pi R$ $^-$: $R[X] \to F[X]$ 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

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

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 $R[x]$. □

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

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

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 $e_{n+1}^2 - e_{n+1} \equiv_f$

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

1.8.3 Extension of valuations.

Lemma 1.8.13. *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. □

Theorem 1.8.14. *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 $O := \mathrm{Int}_R(L)$ 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 1.8.13

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

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 1.8.15. *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 1.8.16. *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 1.8.17. *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 $s_is_j \neq 0$ 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 $M + \wp O = O$ 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 $M = O$. □

1.9 p-adic number fields

Definition 1.9.1. *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 1.9.2. *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 1.9.3. *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 1.9.4. *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 $U^{(n)}$ into $\pi^n R$.
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 $v(\frac{x^i}{i!} = iv(x) - m(i - s_i) = i(v(x) - m) + s_i m \geq i$ and therefore $\exp(x)$ is convergent.
Moreover for $i \geq 1$

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

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 1.9.5. *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 1.9.6. *$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ 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 1.9.7. *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 $n = 3$.

1.9.1 Unramified extensions

Definition 1.9.8. *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 1.9.9. *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 1.9.10. *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 $\tilde{\mathrm{Frob}}_q$ 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 1.9.11. *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 1.9.12. *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 $\mathbb{Q}_5$.

1.10 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 1.10.1. $S_{L/K} : L \to K, x \mapsto \mathrm{trace}(\mathrm{mult}_x)$ *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**.
$O_L^\# := \{x \in L \mid S(x,\alpha) \in O_K \text{ for all } \alpha \in O_L\}$ *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 $d \in \mathbb{Z}$, $d \le 0$.*
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 1.10.2. *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 1.10.3. *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 $\pi_M^c O_M = \pi_L^a \pi_M^b O_M = \pi_M^{b+e(M/L)} O_M$. □

Corollary 1.10.4. *Let $T := T_{L/K}$. Then $\mathcal{D}(L/K) = \mathcal{D}(L/T)$.*

Corollary 1.10.5. *If L/K is tamely ramified of degree $ef = n$, $e = [L/T_{L/K}]$ then $\mathcal{D}(L/K) = \pi_L^{e-1} O_L$.*

Proof. Because of the last corollary we may assume that $K = T_{L/K}$ and L/K is totally ramified of degree e prime to p. Then $L = K[\sqrt[e]{\pi_K}]$ for some prime element π_K of K and with $\pi_L := \sqrt[e]{\pi_K}$ the basis $B := (1, \pi_L, \ldots, \pi_L^{e-1})$ is an integral basis of L/K. The Gram matrix of B is $A := (S_{L/K}(\pi_L^{i+j}))_{i,j}$ with $S_{L/K}(\pi_L^k) \neq 0$ if k is a multiple of e. So

$$A = \begin{pmatrix} e & 0 & \ldots & 0 \\ 0 & 0 & \ldots & e\pi_K \\ \vdots & & \ddots & \\ 0 & e\pi_K & \ldots & 0 \end{pmatrix}$$

has determinant in $\pi_K^{e-1} O_K^*$. □

Theorem 1.10.6. *(without proof) If L/K is totally ramified of index e such that $p \mid e$ then $\mathcal{D}(L/K) \subseteq \pi_L^{2e-1} O_L$.*

Corollary 1.10.7. *L/K is ramified if and only if $D(L/K) \neq O_K$.*

Applying this corollary to the completion of a number field $K/\mathbb{Q}$ at some prime $\wp$ of K we obtain

Corollary 1.10.8. *Let K be an algebraic number field. Then the rational prime p ramifies in K if and only if p divides the discriminant of K.*

Note the difference between tame and wild ramification in the example of quadratic number fields. If an odd prime p is ramified, then v_p of the discriminant is exactly 1. If 2 ramifies, then $K = \mathbb{Q}[\sqrt{d}]$ with squarefree integral d such that $d \equiv_4 2, 3$ and then $d_K = 2^2 d$ has either valuation 2 or 3.

Chapter 2

Non-commutative theory.

2.1 Central simple algebras.

This section recalls some of the relevant theory on simple algebras. For more details I refer to the Algebra skript, in particular to Section 5.

2.1.1 Simple algebras.

Let K be a field and A a finite dimensional K-algebra. Then A is called a **division algebra**, if any non-zero element in A has an inverse. A is called **simple**, if A has no non-trivial 2-sided ideals and **central simple**, if additionally $Z(A) = K$. The center of any simple K-algebra is an extension field of K, so any simple K-algebra A is a central simple $Z(A)$-algebra.

One frequently used fact is the following quite easy remark:

Definition 2.1.1. *Let A be a K-algebra. Then A is also a left A-module ${}_AA$, called the left* **regular module**. *The left* **regular representation** $\rho_A : A \to \mathrm{End}_K(A)$ *is defined by* $\rho_A(a) : x \mapsto ax$. *The* **regular norm** *is* $N_{A/K} : A \to K, a \mapsto \det(\rho_A(a))$ *and the* **regular trace** *is* $T_{A/K} : A \to K, a \mapsto \mathrm{trace}(\rho_A(a))$.

Remark 2.1.2. $A \cong \mathrm{End}_A({}_AA)^{op}$ *by* $a \mapsto (x \mapsto xa)$.

Theorem 2.1.3. *Any simple K-algebra A is semi-simple, more precisely $A \cong D^{n\times n}$ for some division algebra D, $n \in \mathbb{N}$.*

Proof. Let $M \leq_A A$ be a simple submodule of the regular left A-module ${}_AA$. Then for any $a \in A$ the image $Ma = 0$ or simple. Moreover $\sum_{a\in A} Ma \trianglelefteq A$ is a non-zero two-sided ideal of A. Since A is simple $\sum_{a\in A} Ma = A$. So ${}_AA$ is the sum of simple modules and hence completely decomposable, i.e. a semi-simple A-module. This implies that A is semisimple. By Wedderburns characterisation of semisimple algebras we hence obtain $A \cong \bigoplus_{i=1}^{s} D_i^{n_i\times n_i}$ for division algebras D_i. But A is simple, so $s = 1$.

Many facts follow from the useful "double-centralizer-theorem":

Theorem 2.1.4. *Let B be a semisimple subalgebra of the matrix ring $K^{n\times n}$. Let*

$$C = C_{K^{n\times n}}(B) := \{x \in K^{n\times n} | xb = bx \text{ for all } b \in B\}$$

be the centralizer of B in $K^{n\times n}$. Then

(i) C *is semi-simple.*

(ii) $B \cap C = Z(B)$.

(iii) $C_{K^{n\times n}}(C) = B$ *(double-centralizer-theorem)*

(iv) B *simple* $\Leftrightarrow$ C *simple.*

(v) If $B \cong D^{\beta\times\beta}$ *simple, then* $C \cong (D^{op})^{\gamma\times\gamma}$ *for some* $\gamma \in \mathbb{N}$ *and* $Z := B \cap C = Z(B) = Z(D)$. *Moreover*

$$B \cdot C = \langle b \cdot c \mid b \in B, c \in C \rangle$$

is a simple subalgebra of $K^{n\times n}$ *with* $B \cdot C \cong Z^{k\times k}$ *for some* $k \in \mathbb{N}$ *(*$k = \beta\gamma\ell^2$*, where* $\ell^2 = \dim_Z(D)$*).*

Proof. The proof is somehow technical, I refer to the algebra skript or the literature. □

If A_1 and A_2 are K-algebras then also the tensor product $A_1 \otimes A_2$ is a K-algebra, where the multiplication is defined by the bilinear extension of

$$(a_1 \otimes a_2)(a_1' \otimes a_2') := a_1a_1' \otimes a_2a_2'.$$

Examples

$$A_1 = K^{n\times n}, A_2 = K^{m\times m} \Rightarrow A_1 \otimes A_2 \cong K^{nm\times nm}(\text{Kronecker product})$$

$$D \otimes_K K^{n\times n} \cong D^{n\times n}$$

If A/K is a finite Galois extension of degree n, then

$$A \otimes_K A \cong A \oplus \cdots \oplus A$$

$$a \otimes b \mapsto (a\sigma_1(b), \cdots, a\sigma_n(b))$$

where $Gal(A/K) = \{\sigma_1, \cdots, \sigma_n\}$.
e.g. $A = K[x]/(p(x))$

$$A \otimes A \cong A \otimes_K K[x]/(p(x)) \cong A[x]/(p(x)) \cong \bigoplus_i A[x]/(x - x_i)$$

if $p(x) = \prod(x - x_i)$ in $A[x]$. In particular $A \otimes_K A$ is not simple (if $n > 1$).

Lemma 2.1.5. *Let* A, B *be simple* K*-algebras,* $Z(A) = K \cdot 1$ *Then* $A \otimes_K B$ *is simple.*

Proof. For a proof I refer to the algebra skript. □

Corollary 2.1.6. *The dimension of any central simple* K*-division algebra* D *is a square:* $\dim_K D = n^2$. *The number* n *is called the* **index** *of* D.

Proof. Let $\overline{K}$ be the algebraic closure of K. Then $\overline{K} \otimes_K D$ is a $dim_K(D)$-dimensional simple $\overline{K}$-algebra, so isomorphic to $X^{n\times n}$ for some n and some finite dimensional $\overline{K}$-divisionsalgebra X. Since $\overline{K}$ is algebraically closed, any such divisionalgebra is isomorphic to $\overline{K}$ (the matrix describing the left multiplication by $a \in D$ on ${}_DD$ has an eigenvalue). So $\overline{K} \otimes_K D \cong \overline{K}^{n\times n}$ and $\dim_K(D) = n^2$. □

In particular the dimension of any central simple K-algebra is a square. $A = D^{k\times k} \Rightarrow dimA = k^2(Index(D))^2$.

Theorem 2.1.7. *Let D be a division algebra with $Z(D) = K$ and $\dim_K(D) = n^2$. Then any subfield of D is contained in some maximal subfield of D. Let $L \leq D$ be such a maximal subfield. Then*

(i) $C_D(L) = L$

(ii) $D \otimes_K L \cong_{L-Algebra} L^{n\times n}$ *(L is a* **splitting field***).*

(iii) $dim_K L = n$

Proof. (i) Let L_1 be a subfield of D. If L_1 is not maximal, then $C_D(L_1) \supsetneq L_1$. Choose $x \in C_D(L_1) - L_1$, $L_2 = L_1[x]$ etc. until $C_D(L_i) = L_i$.
(ii) and (iii) follow from the double centraliser theorem. (Exercise)

2.1.2 The theorem by Skolem and Noether.

Theorem 2.1.8. *(Skolem-Noether) Let A be a central simple K-algebra, B_1, B_2 simple subalgebras of A and $\varphi : B_1 \to B_2$ an algebra homomorphism. Then there is some $a \in A^*$, such that $\varphi(b_1) = a^{-1}b_1a$ for all $b_1 \in B_1$.*

Proof. Let V be a simple A-module, $D^{op} := \mathrm{End}_A(V)$. Wlog $V = D^{k\times 1}$, $\dim_K(D) = d$, $n = dk$, so $B_1 \subseteq A \hookrightarrow K^{n\times n}$. Let $C := C_{K^{n\times n}}(A) \cong D^{op}$. Then V is a simple AC-module and $AC \cong K^{n\times n}$. Turn V into a B_1C-module in two different ways:

(i). $(b_1c)v := b_1cv$ for all $v \in V, b_1 \in B_1, c \in C$

(ii). $(b_1c)v := \varphi(b_1)cv$ for all $v \in V, b_1 \in B_1, c \in C$

Since B_1C is simple, there is up to isomorphism a unique module of given dimension. So there is some $a \in K^{n\times n}$, such that

$$a^{-1}b_1ca = \varphi(b_1)c \text{ for all } b_1 \in B_1, c \in C.$$

Choosing $b_1 = 1$, one gets $a \in C_{K^{n\times n}}(C) = A$ and choosing $c = 1$ yields $a^{-1}b_1a = \varphi(b_1)$ for all $b_1 \in B_1$.

One important consequence is the following theorem (also attributed to Wedderburn).

Theorem 2.1.9. *(Wedderburn) Any finite dimensional division algebra over a finite field is commutative.*

Proof. Let $D \neq Z(D) = \mathbb{F}_q$ be a finite division algebra. Any element of D is contained in some maximal subfield (of order q^n). Any two maximal subfields are isomorphic, so by the theorem of Skolem and Noether these are conjugate in D^*. Hence the finite group D^* is a union of conjugacy classes of subgroups. But for a general finite group G we have

$$G = \bigcup_{g \in G} H^g, H \leq G, [G : H] < \infty \Rightarrow G = H$$

since there are $[G : N_G(H)]$ conjugate subgroups of H and $|\bigcup_{g\in G} H^g| \leq 1 + (|H| - 1)\frac{|G|}{|H|} = 1 + |G| - \frac{|G|}{|H|} < |G|$ if $H \neq G$. □

2.1.3 The Brauer group of K

To define the Brauer group of K we need the following two properties:

Theorem 2.1.10. *Let A, B be central simple K-algebras. Then also the tensor product $A \otimes_K B$ is a central simple K-algebra.*

Lemma 2.1.11. *Let D be a central simple K-divisionalgebra. Then*

$$D \otimes_K D^{op} \cong K^{n\times n}$$

Proof. ${}_D D = V$, $D \subseteq End_K(V) \equiv K^{n\times n}$, $C := C_{K^{n\times n}}(D) \cong D^{op}$, $D \otimes_K D^{op} \cong D \cdot C = K^{n\times n}$ □

We now define the Brauer group of K. The elements are the Morita equivalence classes of central simple K-algebras. The multiplication is given by the tensor product.

Definition 2.1.12. *Let A and B be central simple K-algebras. $A \sim B$ are called* **Brauer-equivalent***) $\Leftrightarrow$ there are $n, m \in N$ such that $A^{n\times n} \cong B^{m\times m}$.*

$$\mathrm{Br}(K) := \{[A] \mid A \text{ central simple } K\text{-algebra } \}$$

is called the **Brauergroup** *of K. The multiplication on $\mathrm{Br}(K)$ is defined as $[A][B] := [A \otimes_K B]$.*

Theorem 2.1.13. $\mathrm{Br}(K)$ *is a commutative group with*

$$[A]^{-1} = [A^{op}] \ , \ [K] = 1$$

Any element of $\mathrm{Br}(K)$ is represented by a unique division algebra.

Some examples:
If K s algebraically closed then $\mathrm{Br}(K) = \{1\}$.
If K is finite, then $\mathrm{Br}(K) = \{1\}$.
$\mathrm{Br}(\mathbb{R}) \cong C_2$. (Exercise.)

Remark 2.1.14. *Let L/K be an extension of fields. Then there is a group homomorphism*

$$\mathrm{Br}(K) \to \mathrm{Br}(L), [A] \mapsto [L \otimes_K A].$$

Its kernel is called the **relative Brauer group**

$$\mathrm{Br}(L/K) := \{[A] \in \mathrm{Br}(K) \mid L \otimes_K A \cong L^{n\times n} \text{ for some } n\}$$

Example. Let D be a central K-division algebra and L a maximal subfield of D. Then $[D] \in \mathrm{Br}(L/K)$.

Ende am 10.10.11

2.2 Orders in separable algebras.

Definition 2.2.1. *A K-algebra A is called* **separabel** *over K, if there is some separable extension field L of K such that $L \otimes_K A \cong_{L-Algebra} \bigoplus_{i=1}^k L^{n_i\times n_i}$. Then $Sp : A \to L : a \mapsto \sum_{i=1}^k Sp(a_i)$ ($a_i \in L^{n_i\times n_i}$) is called the* **reduced trace** *and $N : a \to L : a \mapsto \prod_{i=1}^k \det(a_i)$ the* **reduced norm**.

Remark: Reduced norm and trace take only values in K.
Remark: Separable algebras are those semisimple algebras $A = \bigoplus_{i=1}^s D_i^{n_i\times n_i}$ for which all $Z_i = Z(D_i)$ are separable over K.

Let R be a Noetherian integral domain with field of fractions K and A a finite dimensional K-algebra. We assume that R is **integrally closed** in K, so

$$R = \mathrm{Int}_R(K) = \{a \in K \mid a \text{ is integral over } R\} = \{a \in K \mid R[a] \text{ is finitely generated } R-\text{module}\}.$$

One typical example is the ring of integers in a number field. The other example is a discrete valuation ring.

Definition 2.2.2. *Let V be a finite dimensional K-vector space. An R-***lattice** *L in V is a finitely generated R-submodule of V, that spans V as a K-vector space.*
*An R-***order** *Λ in A is a lattice in A that is also a subring (multiplicatively closed).*
An R-order Λ is called a **maximal R-order**, *if for any order Γ in A with $\Lambda \leq \Gamma$ it holds that $\Lambda = \Gamma$.*

Remark 2.2.3. *Any K-algebra contains R-orders: Let $B := (b_1, \ldots, b_n)$ be some K-basis of A and put $L := \langle b_1, \ldots, b_n\rangle_R$ the R-lattice generated by this basis. Then the* **left-order**

$$O_l(L) := \{a \in A \mid aL \subseteq L\}$$

of L is an R-order in A, similarly the **right-order** $O_r(L) := \{a \in A \mid La \subseteq L\}$.

Note that L is an order $\Leftrightarrow L = O_r(L) = O_l(L)$.

Definition 2.2.4. *An element $a \in A$ is called* **integral over** *R, if $R[a]$ is a finitely generated R-module.* $\mathrm{Int}_R(A) := \{a \in A \mid a \text{ integral over } R\}$ *is called the* **integral closure** *of R in A.*

In general $\mathrm{Int}_R(A)$ is not a ring. It is a ring, if A is commutative. It is also a ring if A is a division algebra over a complete field (see below).

Remark 2.2.5. *For any R-order Λ and any element $\lambda \in \Lambda$ the ring $R[\lambda] \subseteq \Lambda$ is a submodule of the f.g. module Λ and hence again finitely generated. In particular any element of Λ is integral over R.*

Theorem 2.2.6. *Let $\lambda \in A$. Then λ is integral over R if and only if the minimal polynomial of λ lies in $R[X]$.*

Proof. Let $R[\lambda] = \langle b_1, \ldots, b_n \rangle_R$ and $\lambda b_i = \sum_{j=1}^n a_{ij} b_j$ with $M := (a_{ij}) \in R^{n \times n}$. Since $1 \in R[\lambda]$ the minimal polynomial of M is equal to the minimal polynomial of λ. As a monic divisor of the characteristic polynomial of M, which is a monic polynomial in $R[X]$, also this minimal polynomial is in $R[X]$. □

Theorem 2.2.7. *Any separable algebra has some maximal order.*

Proof. Let Λ be some R-order in A. Then

$$\Lambda \subseteq \Lambda^{\#} := \{a \in A \mid Sp(ax) \in R \text{ für alle } x \in \Lambda\}.$$

Any overorder Δ of Λ is also an integral lattice with respect to the trace bilinear form, so

$$\Lambda \subseteq \Delta \subseteq \Delta^{\#} \subseteq \Lambda^{\#}.$$

Not $\Lambda^{\#}/\Lambda$. is a finitely generated R-module and hence does not contain infinite extending chains of submodules since R is Noetherian. Therefore there is some maximal order that contains Λ. □

Example. $A = \langle 1, i, j, k \rangle_{\mathbb{Q}}$ with $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$. $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$, $\Lambda^{\#} = \frac{1}{2}\Lambda$, $\Gamma = \langle 1, i, j, \frac{1}{2}(1 + i + j + k) \rangle$ is maximal order of A that contains Λ.

In the non-separable algebra $A = \Delta_2(\mathbb{Q}) = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\} \leq \mathbb{Q}^{2\times 2}$ does not contain maximal orders: The $\mathbb{Z}$-orders

$$\Lambda_n := \begin{pmatrix} \mathbb{Z} & \frac{1}{2^n}\mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix}$$

form an infinite ascending chain of orders in A.

2.2.1 Being a maximal order is a local property

In this section we show that for a Dedekind domain R any R-order Λ (in the separable K-algebra A) is maximal if and only if all its **localizations**

$$(R \setminus \wp)^{-1}\Lambda := \{\frac{r}{s}\lambda \mid r, s \in R, s \notin \wp, \lambda \in \Lambda\}$$

at all prime ideals $\wp \trianglelefteq R$ are maximal orders if and only if all its **completions** $\hat{R}_\wp\Lambda$ are maximal orders for all prime ideals $\wp$ of R.

Recall that any prime ideal $\wp$ defines a discrete valuation $v_\wp : K^* \to \mathbb{Z}$, such that the corresponding discrete valuation ring is the localisation

$$R_\wp := (R \setminus \wp)^{-1}R = R_{v_\wp} = \{x \in K \mid v_\wp(x) \geq 0\}.$$

The completion of $R_\wp$ is denoted by $\hat{R}_\wp$.

Definition 2.2.8. *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 $(R \setminus \wp)^{-1}M$ if and only if it holds for all completions $\hat{R}_\wp M$ for all prime ideals $\wp$ of R.*

Equality of lattices is a local property:

Theorem 2.2.9. *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) $L_\wp := (R \setminus \wp)^{-1}L = (R \setminus \wp)^{-1}M =: M_\wp$ for all maximal ideals $\wp \trianglelefteq R$.
(3) $\hat{R}_\wp \otimes L = \hat{R}_\wp \otimes M$ for all maximal ideals $\wp \trianglelefteq R$.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (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 $\ell \notin \hat{R}_\wp \otimes M$ so $\hat{R}_\wp \otimes L \neq \hat{R}_\wp \otimes M$ for this prime ideal $\wp \trianglelefteq R$. □

Theorem 2.2.10. *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 an $R_\wp$-lattice 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 $\hat{L}_\wp$ denote the completion $\hat{L}_\wp := \hat{R}_\wp \otimes L$ which is a lattice in $V_\wp := \hat{K}_\wp \otimes V$. Then
(i) $L = V \cap (\bigcap_\wp \hat{L}_\wp)$.
(ii) Let $\hat{X}(\wp)$ be an $\hat{R}_\wp$-lattice in $\hat{V}_\wp$ for all maximal ideals $\wp$ of R such that $\hat{X}(\wp) = \hat{L}_\wp$ for all but finitely may $\wp$. Then $M := V \cap \bigcap_\wp \hat{X}(\wp)$ is a lattice in V such that $\hat{M}_\wp = \hat{X}(\wp)$ for all $\wp$.
(d) Let $\wp$ be some maximal ideal in R. Then there are bijections

$$\{M \leq L \mid L/M \text{ is } \wp\text{-torsion}\} \to \{M \leq L_\wp \mid M \text{ full lattice}\} \to \{M \leq \hat{L}_\wp \mid M \text{ full lattice}\}$$

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

Proof. (Exercise, see Theorem (4.22) and (5.3) in Reiner's book.) □

Theorem 2.2.11. *Let R be a Dedekind domain with field of fractions K and let A be a separable K-algebra. Let Λ be an R-order in A. Then the following are equivalent:*
(1) Λ is a maximal R-order in A.
(2) $(R \setminus \wp)^{-1}\Lambda$ is a maximal $R_\wp$-order in A for all maximal ideals $\wp \trianglelefteq R$.
(3) $\hat{R}_\wp \otimes \Lambda$ is a maximal $\hat{R}_\wp$-order in $\hat{K}_\wp \otimes A$ for all maximal ideals $\wp \trianglelefteq R$.

Proof. Now (3) $\Rightarrow$ (1) is clear so we need to show (1) $\Rightarrow$ (2) $\Rightarrow$ (3).
Assume that Λ is a maximal R-order in A and that there is some maximal ideal $\wp \trianglelefteq R$ such that $\Lambda_\wp = (R \setminus \wp)^{-1}\Lambda$ is not a maximal order, so there is some $R_\wp$-order Γ that properly contains $\Lambda_\wp$. Choose $\alpha \in R$ such that $\alpha\Gamma \subseteq \Lambda_\wp$. Then $\Delta := \Lambda \cap \alpha\Gamma$ is a submodule of Λ such that Λ/Δ is $\wp$-torsion. Since $\alpha\Gamma$ is a two-sided $\Lambda_\wp$-ideal, also Δ is a two-sided Λ-ideal in Λ. Since Λ is a maximal order, the right order $O_r(\Delta)$ conincides with Λ. Hence

$$\Lambda_\wp = O_r(\Delta)_\wp \overset{exerc}{=} O_r(\Delta_\wp) = \Gamma.$$

To see that (2) implies (3) we show that $\Lambda_\wp$ is a maximal $R_\wp$-order in A if and only if $\hat{\Lambda}_\wp$ is a maximal $\hat{R}_\wp$-order in $A \otimes \hat{K}_\wp$. Again the maximality of $\hat{\Lambda}_\wp$ implies the one of $\Lambda_\wp$. On the other hand assume that there is some $\hat{R}_\wp$-order $\hat{\Gamma} \supseteq \hat{\Lambda}_\wp$. Then $\Gamma := \hat{\Gamma} \cap A$ is an $R_\wp$-order in A that contains $\Lambda_\wp$, hence $\Gamma = \Lambda_\wp$. Since $\hat{\Gamma}$ is just the completion of $\hat{\Gamma} \cap A$ we obtain $\hat{\Gamma} = \hat{\Lambda}_\wp$. □

2.3 Division algebras over complete discrete valuated fields.

2.3.1 General properties.

Let (K, v) be a complete discrete valuated field, $v(K^*) = \mathbb{Z}$, $R = R_v := \{x \in K \mid v(x) \geq 0\}$ the corresponding valuation ring with prime element $\pi \in R$, $v(\pi) = 1$ and maximal ideal πR. Let D be a K-division algebra with $[D : K] = m$.

Definition 2.3.1. *Define $\omega : D \to \frac{1}{m}\mathbb{Z} \cup \{\infty\}$ by $\omega(a) := m^{-1}v(N_{D/K}(a))$ where $N_{D/K}$ is the regular norm.*

Remark 2.3.2. *Let $0 \neq a \in D$ and μ_a be the minimal polynomial of $\rho_D(a)$. Then $\omega(a) = [K(a) : K]^{-1}v(\mu_a(0)) = [K(a) : K]^{-1}v(N_{K(a)/K}(a))$.*

Proof. Since D is a skew field, the minimal polynomial μ_a is irreducible and $\chi_a = \mu_a^{m/n}$ with $n = [K(a) : K]$. Then $N_{D/K}(a) = (-1)^m\mu_a(0)^{m/n}$ and

$$\omega(a) = \frac{1}{m}v(N_{D/K}(a)) = \frac{1}{n}v(\mu_a(0)) = [K(a) : K]^{-1}v(N_{K(a)/K}(a)).$$

□

Theorem 2.3.3. *An element $a \in D$ is integral over R, if and only if $N_{D/K}(a) \in R$, if and only if $\omega(a) \geq 0$.*

Proof. $\Rightarrow$ is clear.
$\Leftarrow$: Assume that $\omega(a) \geq 0$, so $N_{D/K}(a) \in R$ and hence $\mu_a = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n \in K[x]$ satisfies that $a_n \in R$. Since D is a division algebra, the minimal polynomial is irreducible, so by 1.8.13 all coefficients satisfy $v(a_i) \geq \min\{v(a_0), v(a_n)\} \geq 0$ for all $0 \leq i \leq n$ and hence $\mu_a \in R[x]$. □

Theorem 2.3.4. *$\omega : D \to \frac{1}{m}\mathbb{Z}$ is a discrete valuation of D that extends v.*

Proof. Clearly ω is a well defined map that extends v. To show that ω is a discrete valuation (on the not necessarily commutative division algebra D) we need to show that

(i) $\omega(a) = \infty$ if and only if $a = 0$.

(ii) $\omega(ab) = \omega(a) + \omega(b)$ for all $a, b \in D$.

(iii) $\omega(a + b) \geq \min(\omega(a), \omega(b))$ for all $a, b \in D$.

The first property follows from the fact that for non zero a $N_{D/K}(a)N_{D/K}(a^{-1}) = 1$ and hence $N_{D/K}(a) = 0$ if and only if $a = 0$. The second porperty follows because the norm is multiplicative. To see (iii) we may assume that a and b are non-zero, $\omega(b) \geq \omega(a)$ and divide by a, so we assume that $a = 1$ and $\omega(b) \geq 0$. But then b is integral over R, so also $1 + b$ is integral over R, i.e. $\omega(1 + b) \geq 0 = \min(\omega(1), \omega(b))$. □

Theorem 2.3.5. *ω is the unique valuation on D that extends v.*

Proof. Assume that there is a second (different) extension ω' of the valuation v and choose $\alpha \in D$ such that $\omega(\alpha) \neq \omega'(\alpha)$. Wlog we may assume that $\omega(\alpha) < \omega'(\alpha)$ (otherwise replace α by α^{-1}). Let $\mu_\alpha := X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$, then $\omega(\alpha) = \frac{1}{n}v(a_n)$ and by Lemma 1.8.15 all coefficients satisfy $v(a_k) \geq \frac{k}{n}v(a_n) = k\omega(\alpha)$. Then

$$\omega'(a_k\alpha^{n-k}) = (n-k)\omega'(\alpha) + v(a_k) > n\omega(\alpha) = v(a_n) \text{ for all } k = 0, \ldots, n-1.$$

But $a_n = -a_{n-1}\alpha - \ldots - a_1\alpha^{n-1} - \alpha^n$ and therefore

$$\omega'(a_n) = v(a_n) \geq \min\{\omega'(a_k\alpha^{n-k}) \mid k = 0, \ldots, n-1\} > v(a_n)$$

a contradiction. □

Definition 2.3.6. *Let $\Delta := \{a \in D \mid \omega(a) \geq 0\}$ be the valuation ring of ω.*

Corollary 2.3.7. *$\Delta = \mathrm{Int}_R(D)$ is the unique R-maximal order in D.*

Definition 2.3.8. *The unique value $e \in \mathbb{N}$ such that $\omega(D^*) = \frac{1}{e}\mathbb{Z}$ is called the* **ramification index** *of D over K, $e = e(D/K)$.*
The valuation $v_D := e\omega : D \to \mathbb{Z} \cup \{\infty\}$ is called the **normalized valuation** *of ω.*
Let $\pi_D \in D$ be a prime element, i.e. $v_D(\pi_D) = 1$. Then π_D generates the unique maximal ideal of Δ and $\overline{\Delta} := \Delta/\pi_D\Delta$ is a skew field. The dimension of $\overline{\Delta}$ over $\overline{R} := R/\pi R$ is called the **inertia degree** *of D over K.*

Similarly as Theorem 1.8.17 we obtain the following result, the proof of which is left as an exercise:

Theorem 2.3.9. *$ef = [D : K] = m$. More precisely let $(a_1, \ldots, a_f) \in \Delta$ such that $(\overline{a_1}, \ldots, \overline{a_f})$ form an $\overline{R}$-basis of $\overline{\Delta}$. Then*

$$(a_i \pi_D^j \mid 1 \leq i \leq f, 0 \leq j \leq e-1)$$

is an R-basis of Δ.

Proof: Either blackboard or exercise.

Example. $D = \langle 1, \omega, i, i\omega \rangle_{\mathbb{Q}_3}$ such that $\omega^2+\omega+1 = 0$, $i^2 = -1$, $\omega^i = \omega^2$. Then $e = f = 2$ and $\Delta = \langle 1, \omega, i, i\omega \rangle_{\mathbb{Z}_3}$ with prime element $\pi_D = 1 - \omega$.

With respect to the $\mathbb{Z}_3$-basis $(1, \pi_D, i, i\pi_D)$ the right-regular representation (mapping $a \in \Delta$ to $\rho(a) : x \mapsto xa \in \mathrm{End}_{\mathbb{Z}_3}(\Delta) \cong \mathbb{Z}_3^{4\times 4}$) is given by

$$\rho(\pi_D) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -3 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -3 & 3 \end{pmatrix}, \ \rho(i) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & -1 \\ -1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \end{pmatrix}, \ \rho(i\pi_D) = \rho(i)\rho(\pi_D) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 \\ 0 & -1 & 0 & 0 \\ -3 & 0 & 0 & 0 \end{pmatrix}$$

and the regular norm

$$\begin{array}{ll} N_{D/\mathbb{Q}_3}(a_0 + a_1\pi_D + a_2 i + a_3 i\pi_D) = & \det(a_0 + a_1\rho(\pi_D) + a_2\rho(i) + a_3\rho(i\pi_D) = \\ (a_0^2 + 3a_0a_1 + 3a_1^2 + a_2^2 + 3a_2a_3 + a_3^2)^2 = & N(a_0 + a_1\pi_D + a_2 i + a_3 i\pi_D)^2 \end{array}$$

In particular the regular norm lies in $\mathbb{Z}_3$ if and only if the reduces norm is in $\mathbb{Z}_3$. Let $L := (\Delta, N)$ denote the $\mathbb{Z}_3$-lattice in the quadratic space $(D \cong \mathbb{Q}_3^4, N)$. Then the Grammatrix of the associated bilinear form

$$(x, y) \mapsto N(x + y) - N(x) - N(y) = Sp(x\overline{y})$$

with respect to the basis above is given as

$$\begin{pmatrix} 2 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 3 & 6 \end{pmatrix} \sim_{\mathbb{Z}_3} \mathrm{diag}(2, 3, 2, 3).$$

In particular $L^\#/L \cong \mathbb{F}_3^2$ is a quadratic $\mathbb{F}_3$-space with induced quadratic form x^2+y^2. This is anisotropic (i.e. there is no non-zero $(x, y) \in \mathbb{F}_3^2$ such that $x^2 + y^2 = 0$) so for any $a \in \Delta^\# \setminus \Delta$ the reduced norm $N(a)$ does not lie in $\mathbb{Z}_3$ and therefore $L = (\Delta, N)$ is a maximal integral lattice and in particular Δ is a maximal order in D.

2.3.2 Finite residue class fields.

In the case where $\overline{R} = R/\pi R$ is finite we obtain many more nice properties since then $\Delta/\pi_D\Delta$ is a finite skew field, hence a field of which the isomorphism type is determined by its dimension.

So assume from now on that (K, v) is a complete discrete valuated field, $v(K^*) = \mathbb{Z}$, $R = R_v := \{x \in K \mid v(x) \geq 0\}$ the corresponding valuation ring with prime element $\pi \in R$, $v(\pi) = 1$ and maximal ideal πR. Assume additionally that $\overline{R} = R/\pi R$ is finite, so $\overline{R} \cong \mathbb{F}_q$. Let D be a K-division algebra with $[D : K] = n$ and ramification index e and let

$$\omega : D^* \to \frac{1}{e}\mathbb{Z},\ \omega(a) := n^{-1}v(N_{D/K}(a))$$

be the unique extension of v to D. Then D is a complete discretely valuated skew field with valuation ring

$$\Delta := \{a \in D \mid \omega(a) \geq 0\} = \mathrm{Int}_R(D)$$

the unique maximal R-order in D. Choose $\pi_D \in \Delta$ with $\omega(\pi_D) = \frac{1}{e}$. Then $\pi_D\Delta$ is the unique maximal ideal in Δ and $\overline{\Delta} := \Delta/\pi_D\Delta$ is a finte skew field of dimension $f = m/e$ over $\mathbb{F}_q$, so $\overline{\Delta} \cong \mathbb{F}_{q^f}$ is a field.

From algebraic number theory I we know the following structure theorem in the commutative case, which will be also relevant in the non-commutative case (including the proof).

Theorem 2.3.10. *Assume that D is commutative, hence an extension field of K. Then*
(1) There is a unique subfield $K \leq L \leq D$ with $[L : K] = f(L/K) = f(D/K) = f$ (the maximal unramified subfield or inertia field of the extension). $L \cong K[\zeta_{q^f-1}]$ is the splitting field of the polynomial $X^{q^f-1} - 1 \in K[X]$.
(2) In particular if $f = m$, then $D = L \cong K[\zeta_{q^f-1}]$ and the regular norm $N_{D/K}$ yields a group epimorphism $N_{D/K} : \Delta^* \to R^*$.
(3) Let L be as in (1). Then D/L is totally ramified, $e(D/L) = e(D/K) = [D : L] = e$, $D = L[\pi_D]$ and the minimal polynomial of $\pi_D \in L[X]$ is an Eisensteinpolynomial

$$\mu_{\pi_D} = X^e + a_1X^{e-1} + \ldots + a_{e-1}X + a_e \in \mathbb{Z}_L[X],\ \pi \mid a_i \text{ for all } i, \pi^2 \not| a_e.$$

For a proof we refer to the algebraic number theory I course or the exercises.

We now treat the case where $Z(D) = K$, so D is a central simple K-division algebra.

2.3.3 The central simple case: analysis

Theorem 2.3.11. *Assume that $Z(D) = K$.*
(a) $[D : K] = m^2$ and $e(D/K) = f(D/K) = m$.
*(b) The maximal totally unramified subfields (***inertia fields***) of D are conjugate in D and of degree m over K.*

Proof. (a) Let $a \in \Delta$ be such that $\overline{\Delta} = \overline{R}[\overline{a}]$. Then $K[a]$ is a commutative subfield of D, so $[K[a] : K] \leq m$. On the other hand

$$m \geq [K[a] : K] \geq [\overline{R}[\overline{a}] : \overline{R}] = f$$

so $f \leq m$. Similarly

$$m \geq [K[\pi_D] : K] \geq [\omega(K[\pi_D]^*) : \omega(K^*)] = e.$$

Since $ef = m^2$ we obtain $e = f = m$.
(b) $\overline{\Delta} \cong \mathbb{F}_{q^f} = \mathbb{F}_q[\overline{a}]$ for some $a \in \Delta$ such that $\overline{a}$ is a primitive $q^f - 1$ root of unity. Since $\overline{\Delta}$ is complete we obtain as in the commutative case (using Hensels Lemma) an element $z \in R[a] \subseteq \Delta$ with $\overline{z} = \overline{a}$ and $z^{q^f-1} = 1$, so z is a primitive $q^f - 1$ root of 1 in Δ. The field $L := K[z]$ is a maximal subfield of D that is totally unramified over K.
Now let M be any unramified subfield of D, $f' := [M : K]$. Then $F_{q^{f'}} = R_M/\pi R_m \leq \Delta/\pi_D\Delta$ so f' divides f and M is isomorphic to the unique subfield L' with $K \leq L' \leq L$ and $[L' : K] = f'$. By the theorem of Skolem and Noether there is some $a \in D^*$, such that $aMa^{-1} = L'$. Then $a^{-1}La \cong L$ is a maximal subfield of D that is totally unramified, conjugate to L and contains M. □

Theorem 2.3.12. *Assume that $Z(D) = K$, $[D : K] = m^2$, and let $\zeta \in D$ be a primitive $q^m - 1$-st root of unity. Then there is some prime element $\pi'_D \in \Delta$ such that*

$$(\pi'_D)^m = \pi \text{ and } \pi'_D\zeta(\pi'_D)^{-1} = \zeta^{q^r} \text{ for some } 1 \leq r \leq m, \gcd(r, m) = 1$$

The value of r does not depend on the choice of ζ, π'_D, and π and hence only depends on D. $\frac{r}{m}$ is called the **Hasse-invariant** *of D.*

Proof. (1) By Skolem-Noether there is some $\alpha \in D^*$ such that $\alpha\zeta\alpha^{-1} = \zeta^q$. Wlog

$$\alpha \in \Delta,\ v_D(\alpha) = m\omega(\alpha) =: j \in \{0, \ldots, m-1\}.$$

Put $h := \frac{m}{\gcd(j,m)}$ and $h := 1$ if $j = 0$ (which will not happen). Then $\alpha^h = \epsilon\pi^b$ for some $b \in \mathbb{N}_0, \epsilon \in \Delta^*$ and h is minimal with this property. We compute

$$\zeta^{q^h} = \alpha^h\zeta\alpha^{-h} = \epsilon\zeta\epsilon^{-1} \overset{*}{=} \zeta$$

$*$ because this equality holds in the residue class field $\overline{\Delta}$, and ζ is the unique power of ζ that is congruent to ζ modulo $\pi_D\Delta$. Since $1 \leq h \leq m$ and ζ is a primitive $q^m - 1$ root of unity, this implies that $h = m$ and hence $\gcd(j, m) = 1$.
(2) Put $\tilde{\pi}_D := \pi^{-t}\alpha^r$ where $r, t \in \mathbb{Z}$ such that $rj - tm = 1$. Then $v_D(\tilde{\pi}_D) = 1$ and $\tilde{\pi}_D\zeta\tilde{\pi}_D^{-1} = \zeta^{q^r}$. We want to achieve that $\tilde{\pi}_D^m = \pi$.
(3) By (2) the element $\tilde{pi}_D^m$ commutes with ζ and $\tilde{\pi}_D$ and hence

$$\tilde{\pi}_D^m \in Z(\langle\zeta, \tilde{\pi}_D\rangle_{K-algebra}) = Z(D) = K.$$

Comparing valuations we obtain $\tilde{\pi}_D^m = \pi\epsilon \in \pi R^*$ for some $\epsilon \in R^*$. (not the same as in (1)). For any $\lambda \in K[\zeta] = C_D(K[\zeta])$ the element $\tilde{\pi}_D\lambda$ also satisfies

$$\tilde{\pi}_D\lambda\zeta\lambda^{-1}\tilde{\pi}_D^{-1} = \tilde{\pi}_D\zeta\tilde{\pi}_D^{-1} = \zeta^{q^r}$$

Moreover

$$(\tilde{\pi}_D\lambda)^m = (\tilde{\pi}_D\lambda)^{m-2}\tilde{\pi}_D^2(\tilde{\pi}_D^{-1}\lambda\tilde{\pi}_D)\lambda = \ldots = N_{K[\zeta]/K}(\lambda)\tilde{\pi}_D^m.$$

Since $N(R[\zeta]^*) = R^*$ (see Theorem 2.3.10) there is some $\lambda \in R[\zeta]$ such that $N_{K[\zeta]/K}(\lambda) = \epsilon^{-1}$. Put $\pi'_D := \tilde{\pi}_D\lambda$, then this element has the desired properties and we have shown the existence of such a π'_D.

(4) Uniqueness:
(a) r is independent of the choice of ζ:
Let ζ' be a second primitive q^m-1 root of unity. Then by the Theorem of Skolem and Noether there is some $\beta \in D^*$ such that $\beta\zeta\beta^{-1} = \zeta'$. Put $\pi''_D := \beta\pi'_D\beta^{-1}$.
(b) r is independent of the choice of π'_D and π:
Let $\pi''_D \in \Delta$ be some prime element such that

$$\pi''_D\zeta(\pi''_D)^{-1} = \zeta^{q^s}(1 \leq s \leq m).$$

Then $\pi''_D = \gamma\pi'_D$ for some $\gamma \in \Delta^*$. Then

$$\zeta^{q^s} = (\gamma\pi'_D)\zeta(\gamma\pi'_D)^{-1} = \gamma\zeta^{q^r}\gamma^{-1} \equiv \zeta^{q^r} \pmod{\pi_D\Delta}$$

and so $r = s$. □

2.3.4 The central simple case: synthesis

Theorem 2.3.13. *Let $1 \leq r \leq m$, $\gcd(r,m) = 1$, K complete discretely valuated field with finite residue class field. Then there is up to isomorphism a unique central K-division algebra D with $[D:K] = m^2$ and Hasse invariant $(D) = \frac{r}{m}$.*

Proof. **Uniqueness.** This is clear since $D = \langle\zeta, \pi_D\rangle_{K-algebra}$ is uniquely determined by the relations $\zeta = \zeta_{q^m-1}$, $\pi_D^m = \pi$ and $\pi_D\zeta\pi_D^{-1} = \zeta^{q^r}$.
Existence. Let $\zeta \in \overline{K}$ be a primitive q^m-1 root of unity and $L := K[\zeta]$. Then L is a maximal subfield of D and therefore also a splitting field of D and we construct D as a K-subalgebra of $L^{m\times m}$ as follows:
Let $\theta \in \mathrm{Gal}(L/K)$ such that $\theta(\zeta) = \zeta^{q^r}$ and π be some prime element of R. Then $\langle\theta\rangle = \mathrm{Gal}(L/K)$ since $\gcd(r,m) = 1$. Define

$$^* : L \to L^{m\times m}, \alpha \mapsto \alpha^* := \mathrm{diag}(\alpha, \theta(\alpha), \theta^2(\alpha), \ldots, \theta^{m-1}(\alpha)).$$

Then * is a K-algebra isomorphism and $N_{L/K}(\alpha) = \det(\alpha^*)$. Define

$$\pi_D := \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & 1 \\ \pi & 0 & \ldots & \ldots & 0 \end{pmatrix}.$$

Then $\pi_D^m = \mathrm{diag}(\pi, \ldots, \pi)$ and $\pi_D\zeta^*\pi_D^{-1} = (\zeta^*)^{q^r}$. Let D be the K-subalgebra of $L^{m\times m}$ generated by π_D and ζ^*. Then

$$B := ((\zeta^*)^k\pi_D^j \mid k = 0, \ldots, m-1, j = 0, \ldots, m-1)$$

is a K-linear generating set of D.
(a) B is a K-basis of D: Let $\alpha_j \in L$ such that $a = \sum_{j=0}^{m-1} \alpha_j^* \pi_D^j \in D$. Then

$$a = \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{m-1} \\ \pi\theta(\alpha_{m-1}) & \theta(\alpha_0) & \ddots & \theta(\alpha_{m-2}) \\ & \ddots & \ddots & \ddots \\ \pi\theta^{m-1}(\alpha_1) & \dots & \pi\theta^{m-1}(\alpha_{m-1}) & \theta^{m-1}(\alpha_0) \end{pmatrix}.$$

If $a = 0$ then the first row of this matrix is 0 and so all α_j are 0. So $(\pi_D^j \mid j = 0, \dots, m-1)$ is independent over L, therefore as an L-vectorspace (not an L-algebra) D has dimension m and hence

$$\dim_K(D) = \dim_K(L) \dim_L(D) = m \cdot m = m^2.$$

(b) D has no zero divisors: Assume that a as above is a zero divisor. Replace a by $\pi^l a$ so that all α_j lie in R_L and $\alpha_k \notin \pi R_L$ for some k ($R_L = R[\zeta] \subseteq L$). Then $\det(a) = 0$. But $\det(a) \equiv N_{L/K}(\alpha_0) \pmod{\pi R_L}$ so $\pi \mid \alpha_0$. But then $\det(a) \equiv \pi N_{L/K}(\alpha_1) \pmod{\pi^2 R_L}$ so $\pi \mid \alpha_1$ etc. until we obtain $\pi \mid \alpha_j$ for all j which contradicts our assumption.
(c) $Z(D) = K$. This is easy: $C_D(L) = \{$ diagonal matrices in $D\} = L$, so L is a maximal subfield of D and $Z(D) = C_L(\pi_D) = K$ since θ generates the full Galois group of L over K.
(d) The Hasse invariant of D is $\frac{r}{m}$ by construction. □

Corollary 2.3.14. *Let K be a complete discretely valuated field with finite residue class field. Then the Hasse invariant defines a bijection* $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

2.3.5 The inverse different.

Definition 2.3.15. *Let $S : D \times D \to K$, $S(a,b) := S(ab)$ be the reduced trace bilinear form. Then $\Delta^\# := \{x \in D \mid S(x, \lambda) \in R \text{ for all } \lambda \in \Delta\}$ is called the* **inverse different** *of Δ.*

Remark 2.3.16. *$\Delta^\#$ is a fractional two-sided Δ-ideal in D, so $\Delta^\# = \pi_D^{-d}\Delta$ for some $d \in \mathbb{N}$.*

Theorem 2.3.17. *$\Delta^\# = \pi_D^{1-m}\Delta$ and $d(\Delta/R) := |\Delta^\#/\Delta| = |R/\pi^{m(m-1)}R| = q^{m(m-1)}$.*

Proof. Let $L = K[\zeta]$ be an inertia field in D and $R_L = R[\zeta]$. Then there is some $\epsilon \in R_L$ such that $S_{L/K}(\epsilon) = \mathrm{trace}(\epsilon^*) = 1$. Moreover $\Delta = \bigoplus_{j=0}^{m-1} R_L \pi_D^j$ and $\mathrm{trace}(\pi_D^j) = 0$ if j is not a multiple of m. Since $\mathrm{trace}(\epsilon^*) = 1$ we have $\mathrm{trace}(\pi_D^{-m}\epsilon^*) = \pi^{-1}$ and therefore $\Delta^\# \subseteq \pi_D^{1-m}\Delta$. So we only need to show that $\pi_D^{1-m} \in \Delta^\#$:
For $j = 0, \dots, m-1$ one computes

$$\mathrm{trace}(R_L \pi_D^j \pi_D^{1-m}) = \mathrm{trace}(R_L \pi_D^{j+1-m}) = \begin{cases} 0 & j \neq m-1 \\ S_{L/K}(R_L) & j = m-1 \end{cases}$$

Since this trace is in R, we get $\Delta^\# = \pi_D^{1-m}\Delta$. To compute the order note that $\Delta/\pi_D\Delta \cong R_L/\pi R_L \cong (R/\pi R)^m$. □

2.3.6 Matrix rings.

Theorem 2.3.18. *Let Γ be some maximal R-order in $D^{n\times n}$. Then there is a matrix $a \in \mathrm{GL}_n(D) = (D^{n\times n})^*$ such that $a\Gamma a = \Delta^{n\times n}$.*

Proof. In the exercises we have shown that $\Delta^{n\times n}$ is a maximal order in $A := D^{n\times n}$.
Let $\Gamma = \langle \gamma_1, \ldots, \gamma_s \rangle_R$ with $s = \dim_K(D^{n\times n})$ be an R-basis of Γ. Let $0 \neq v \in V = D^{n\times 1}$ be some non zero element in the unique simple $A = D^{n\times n}$-module. Let Δ^{op} be the maximal R-order in $D^{op} = \mathrm{End}_A(V)$. Consider the Δ^{op}-submodule

$$L := \langle \gamma_1 v, \ldots, \gamma_s v \rangle_{\Delta^{op}}.$$

Then L is a full R-lattice in V that is invariant under Γ. It is also a right Δ^{op}-module, so is a D^{op}-basis $B := (b_1, \ldots, b_n)$ of V such that

$$L = b_1\Delta^{op} \oplus \ldots \oplus b_n\Delta^{op}$$

(any $\Delta^{op}/\wp$-basis of L lifts to such a basis). Then

$$\Gamma \leq \mathrm{End}_{\Delta^{op}}(L) \cong \Delta^{n\times n}$$

Since Γ is maximal, equality holds and any base change matrix from the standard basis to B is such a conjugating matrix a. □

2.4 Crossed product algebras

2.4.1 Factor systems

Let L/K be some finite Galois extension with Galois group $G := \mathrm{Gal}(L/K)$. (E.g. $L = \mathbb{Q}_p[\zeta_{p^f-1}]$, $K = \mathbb{Q}_p$, $G = \langle F \rangle \cong C_f$.) We want to construct a K-algebra $A = \bigoplus_{\sigma\in G} u_\sigma L$ such that $(u_\sigma : \sigma \in G)$ is an L-basis of A and such that

$$xu_\sigma = u_\sigma x^\sigma \text{ for all } \sigma \in G, x \in L \text{ and } u_\sigma u_\tau = u_{\sigma\tau} \underbrace{f_{\sigma,\tau}}_{\in L} \text{ for all } \sigma, \tau \in G$$

The fact that A is associative yields conditions on the mapping $f : G \times G \to L, (\sigma, \tau) \mapsto f_{\sigma,\tau}$:

$$\begin{array}{llll} (u_\sigma u_\tau)u_\rho = & u_{\sigma\tau} f_{\sigma,\tau} u_\rho = & u_{\sigma\tau} u_\rho f_{\sigma,\tau}^\rho = & u_{\sigma\tau\rho} f_{\sigma\tau,\rho} f_{\sigma,\tau}^\rho \\ u_\sigma(u_\tau u_\rho) = & u_\sigma u_{\tau\rho} f_{\tau,\rho} = & u_{\sigma\tau\rho} f_{\sigma,\tau\rho} f_{\tau,\rho} & \end{array}$$

Definition 2.4.1. *A map $f : G \times G \to L^*$ such that $f_{\sigma\tau,\rho} f_{\sigma,\tau}^\rho = f_{\sigma,\tau\rho} f_{\tau,\rho}$ for all $\sigma, \tau, \rho \in G$ is called* **factor system** *or* **2-cocycle** *of G with values in L^*.*
$Z^2(G, L^*) := \{ f \mid f \text{ is factor system } \}$.

Remark 2.4.2. *$Z^2(G, L^*)$ is an abelian group via $(fg)_{\sigma,\tau} = f_{\sigma,\tau} g_{\sigma,\tau}$.*

Proof. Show that the map $(\sigma,\tau) \mapsto f_{\sigma,\tau}g_{\sigma,\tau}$ is again a 2-cocycle. This is immediate by the commutativity of L^*. □

Of course the algebra above is not changed if we replace u_σ by $u_\sigma c_\sigma$ with $c_\sigma \in L^*$. The product is then

$$(u_\sigma c_\sigma)(u_\tau c_\tau) = u_\sigma u_\tau c_\sigma^\tau c_\tau = u_{\sigma\tau} c_{\sigma\tau} f_{\sigma,\tau} c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1}$$

Remark 2.4.3. *$B^2(G,L^*) := \{f : G \times G \to L^* \mid \exists c_\sigma \in L^* (\sigma \in G)$ such that $f_{\sigma,\tau} = c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1}\}$ is a subgroup of $Z^2(G,L^*)$, the group of* **2-coboundaries**, *and the factor group*

$$H^2(G,L^*) := Z^2(G,L^*)/B^2(G,L^*)$$

is called the second **cohomology group** *of G with values in L^*.*
Two cocycle f, g are called **equivalent**, *if they represent the same class in $H^2(G,L^*)$.*

Proof. Need to show that $(\sigma,\tau) \mapsto c_\sigma^\tau c_\tau c_{\sigma\tau}^{-1}$ is a 2-cocycle and that $Z^2(G,L^*)$ is closed under product (easy) and inverse (easy). □

Remark 2.4.4. *Any 2-cocycle $f \in Z^2(G,L^*)$ is equivalent to a* **normalized 2-cocycle** *f such that $f_{\sigma,1} = f_{1,\sigma} = 1$ for all $\sigma \in G$.*

Proof. Choose $c_\sigma := f_{1,\sigma}^{-1}$. □

2.4.2 Crossed product algebras

Theorem 2.4.5. *Let $G = \mathrm{Gal}(L,K)$, $f \in Z^2(G,L^*)$, $A = (L/K,f) = \bigoplus_{\sigma\in G} u_\sigma L$ as above. Then A is called a* **crossed product algebra**. *A is a central simple K-algebra and $L = C_A(L)$ is a maximal subfield of A. Moreover two such crossed product algebras $(L/K,f)$ and $(L/K,g)$ are isomorphic if and only if the factor systems f and g are equivalent.*

Proof. It is clear that equivalent factor systems construct isomorphic algebras. So we may assume that f and g are normalized.
Then $u_1 = 1_A$ and $L \cong u_1 L = L u_1 \hookrightarrow A$. Since conjugation by any element in $u_\sigma L$ induces the Galois automorphism σ on L, we obtain $L = C_A(L)$, so L is a maximal subfield of A.
Also $Z(A) = \{\ell \in L \mid u_\sigma \ell = \ell u_\sigma\} = K$.
We now show that A is simple:
Let $0 \neq X \trianglelefteq A$ be some 2-sided ideal, choose $0 \neq x \in X$

$$x = u_{\sigma_1} a_1 + \ldots + u_{\sigma_r} a_r \text{ such that } r \text{ is minimal.}$$

If $r > 1$ the we may choose $b \in L$ such that $b^{\sigma_1} \neq b^{\sigma_2}$ and replace x by $y = x - bx(b^{\sigma_1})^{-1} \in X$ which has a smaller representation

$$y = x - bx(b^{\sigma_1})^{-1} = u_{\sigma_2} b_2 + \ldots + u_{\sigma_r} b_r.$$

So $r = 1$ and there is some $x = u_{\sigma_1} a_1 \in X$. Since $a_1 \in L^*$ is a unit in A and also $u_\sigma \in A^*$ this implies that $X = A$.

Now let $g \in Z^2(G, L^*)$ and $B = \bigoplus_{\sigma\in G} v_\sigma L = (L/K, g)$. Assume that $A \cong B$ and let $\Phi : A \to B$ be some isomorphism. Then $\Phi(1) = 1$, so $\Phi(u_1) = v_1$ (since we assumed both factor systems to be normalized). Therefore $\Phi(u_1 L) = v_1 L'$ for some subfield $L' \leq B$ that is isomorphic to L. By the theorem of Skolem and Noether, there is some $b \in B^*$ such that

$$b^{-1}\Phi(u_1 x)b = v_1 x \text{ for all } x \in L.$$

Put $w_\sigma := b^{-1}\Phi(u_\sigma)b \in B$ for all $\sigma \in G$. Then $B = \bigoplus w_\sigma L$, $xw_\sigma = w_\sigma x^\sigma$ and $w_\sigma w_\tau = w_{\sigma\tau} f_{\sigma,\tau}$. Hence $v_\sigma^{-1} w_\sigma =: c_\sigma \in C_B(L) = L$ for all σ defines a cocycle that shows that $f \sim g$. □

Example. $L = K[\zeta_{q^f-1}]$, K complete field with valuation ring R and residue class field $\mathbb{F}_q = R/\pi R$. $\mathrm{Gal}(L/K) \cong C_f = \langle F\rangle$. Define $u_{F^n} := (u_F)^n$ for $n = 2, \ldots, f-1$. So any normalized factor system

$$\varphi : \langle F\rangle \times \langle F\rangle \to L^*$$

is determined by $a := (u_F)^f$, namely

$$\varphi_{F^i,F^j} = \begin{cases} 1 & i+j < f \\ a & i+j \geq f \end{cases} \quad (0 \leq i, j \leq f-1).$$

(This is a general fact for so called **cyclic algebras**, crossed product algebras for which $\mathrm{Gal}(L/K)$ is cyclic, see exercises.)

Corollary 2.4.6. *$(L/K, f) \cong K^{n\times n}$ if and only if $f \sim 1$.*

Proof. It is enough to show that $(L/K, 1) \cong K^{n\times n}$.
$(L/K, 1) = \bigoplus_{\sigma\in G} u_\sigma L$ with $u_\sigma u_\tau = u_{\sigma\tau}$. Define

$$\psi : (L/K, 1) \to \mathrm{End}_K(L), u_\sigma x \mapsto (\ell \mapsto \ell^\sigma x).$$

Then ψ is a K-algebra homomorphism.
ψ is injective, since $(L/K, 1)$ is simple and surjective by comparing dimensions. Therefore $(L/K, 1) \cong \mathrm{End}_K(L) \cong K^{n\times n}$ with $n = \dim_K(L)$. □

Example. Let D be a central simple $\mathbb{Q}$-algebra of dimension 4. Then any maximal subfield L of D is a quadratic extension $L = \mathbb{Q}[\sqrt{a}]$ for some $a \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^2$. The Galois group $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle \cong C_2$ and any normalized factor system is given by

$$f : G \times G \to L^*, f_{1,1} = f_{1,\sigma} = f_{\sigma,1} = 1,\ f_{\sigma,\sigma} =: b \in L^*.$$

Since $u_\sigma^2 = b$ commutes with u_σ, the value b lies in $\mathbb{Q}^*$ and

$$D = \langle\sqrt{a}, u_\sigma\rangle = \left(\frac{a, b}{\mathbb{Q}}\right) = \langle 1, i, j, k\rangle \text{ with } i^2 = a, j^2 = b, ij = -ji = k.$$

The factor system is trivial, if and only if there is some $x \in \mathbb{Q}[\sqrt{a}]$ such that $xx^\sigma = b$.

Theorem 2.4.7. *Let $[L : K] = n$, $G = \mathrm{Gal}(L/K)$. Then $(L/K, f) \otimes_K (L/K, g) \cong (L/K, fg)^{n\times n}$.*

Proof. Let $A := (L/K, f)$ and $B := (L/K, g)$ with L-basis $(u_\sigma \mid \sigma \in G)$ resp. $(v_\sigma \mid \sigma \in G)$ such that the factor systems f and g are normalized. Then the subalgebra u_1L of A is isomorphic to $v_1L \leq B$. In particular $C := A \otimes_K B$ contains a subalgebra

$$(\star_0) \quad S := u_1L \otimes v_1L \cong L \otimes_K L \cong \bigoplus_{\sigma\in G} L, (u_1x \otimes v_1y) \mapsto (x^\sigma y)_{\sigma\in G}.$$

We use this to construct an idempotent $e \in S$ such that $eCe \cong (L/K, fg)$. Then the theorem follows, since we already know that the tensor product of two central simple algebras is again central simple and by comparing dimensions.
To this aim choose a primitive element $a \in L$, so $L = K(a)$ and put

$$e := \prod_{1\neq\sigma\in G} \frac{u_1a \otimes v_1 - u_1 \otimes v_1a^\sigma}{u_1(a - a^\sigma) \otimes v_1}.$$

Then $e \mapsto (1, 0, \ldots, 0)$ under the map in $(\star_0)$ (calculation at blackboard) and $e^2 = e \in S$ is an idempotent. Moreover $(u_1x \otimes v_1)e = e(u_1 \otimes v_1x)$ for all $x \in L$.
We now compare eCe and $(L/K, fg)$:

$$eCe = \sum_{\sigma,\tau\in G} e(u_\sigma \otimes v_\tau)(L \otimes L)e = \sum_{\sigma,\tau\in G} \underbrace{e(u_\sigma \otimes v_\tau)e}_{\star} \underbrace{e(1 \otimes L)ee(L \otimes 1)e}_{L'\cong L}$$

$$\star : e(u_\sigma \otimes v_\tau)e = u_\sigma \otimes v_\tau \prod_{\psi\in G\setminus 1} \frac{a^\sigma \otimes 1 - 1 \otimes a^{\psi\tau}}{(a^\sigma - a^{\psi\sigma}) \otimes 1} e = u_\sigma \otimes v_\tau e \underbrace{\prod_{\psi\in G\setminus 1} \frac{a^\sigma - a^{\psi\tau}}{a^\sigma - a^{\psi\sigma}}}_{=1,\tau=\sigma,=0,\tau\neq\sigma}$$

So $eCe = \bigoplus_{\sigma\in G} w_\sigma L'$ with $w_\sigma = e(u_\sigma \otimes v_\sigma)e$ and $L' = e(1 \otimes L)e \cong L$. Moreover

$$e(x \otimes 1)ew_\sigma = e(x \otimes 1)e(u_\sigma \otimes v_\sigma)e = w_\sigma e(x^\sigma \otimes 1)e$$

and

$$w_\sigma w_\tau = e(u_\sigma \otimes v_\sigma)(u_\tau \otimes v_\tau)e = e(u_{\sigma\tau} \otimes v_{\sigma\tau})ee(f_{\sigma,\tau} \otimes g_{\sigma,\tau})e = w_{\sigma\tau}(f_{\sigma,\tau}g_{\sigma,\tau}).$$

□

2.4.3 Splitting fields.

Definition 2.4.8. *Let A be a central simple K-algebra. An extension field L/K is called a* **splitting field** *for A, if $A \otimes_K L \cong L^{n\times n}$ for some $n \in \mathbb{N}$.*

So L is a splitting field if and only if $[A] \in \mathrm{Br}(L/K) = \ker(\mathrm{Br}(K) \to \mathrm{Br}(L), [A] \mapsto [A \otimes_K L]$.

Example. If $A = (L/K, f)$ then L is a splitting field for A.
Maximal subfields of division algebras are splitting fields.

Theorem 2.4.9. *Let D be a central K-division algebra with $m^2 = [D : K]$ and let E/K be some finite field extension.*
(a) If E is a splitting field for D, then m divides $[E : K]$.
(b) Let r be minimal such that $E \hookrightarrow D^{r\times r}$. Then E splits D, if and only if E is a maximal subfield of $D^{r\times r}$, if and only if $C_{D^{r\times r}}(E) = E$.

Proof. Let $S := E \otimes_K D$. Then $Z(S) = E$ and S is a central simple E-algebra.
Note that E splits D if and only if $S \cong E^{m\times m}$. In general $S \cong D'^{m'\times m'}$ for some E-division algebra D' with center $Z(D') = E$ and some $m' \in \mathbb{N}$.
Let $V \cong (D')^{m'}$ be the simple S-module. Then

$$E \subseteq \mathrm{End}_D(V) \cong D^{r\times r} =: B$$

for some $r \in \mathbb{N}$ and r is minimal with $E \hookrightarrow D^{r\times r}$. Note that we should have worked with D^{op} here to get $D^{r\times r}$. But the maximal subfields of D and D^{op} are the same, also the Schur index m. The minimality of r follows from the fact that all matrix rings over D arise as endomorphism rings of some D-module W. If E embeds into $\mathrm{End}_D(W)$, then W is an $E \otimes_K D$-module. Let $E' := C_B(E)$. Then

$$E \subseteq E' = \mathrm{End}_S(V) = (D')^{op}$$

and $[E : K][E' : K] = [B : K] = m^2r^2$ by the double centralizer theorem.
Now E splits D if and only if $D' = E$ if and only if $E' = E$ and then $E = C_B(E)$ is a maximal subfield of B. If $E' \neq E$, then in any case $E \subseteq Z(E')$ and any $x \in E' \setminus E$ generates a subfield $E[x]$ of B that properly contains E. □

Example. Let $E := \mathbb{Q}[\zeta_5]$, $D = \left(\frac{-2,-5}{\mathbb{Q}}\right)$. Then $E \otimes_{\mathbb{Q}} D \cong E^{2\times 2}$, so E is a splitting field of D but the unique subfield $\mathbb{Q}[\sqrt{5}]$ of E with $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$ is not a spitting field for D.

Corollary 2.4.10. *If $[D : K] = m^2$ and $[E : K] = m$, then E is a splitting field for D if and only if E is a maximal subfield of D.*

Theorem 2.4.11. *Any central simple K-algebra has some splitting field that is Galois over K, so*

$$\mathrm{Br}(K) \cong \bigcup_{L/K \ Galois} \mathrm{Br}(L/K).$$

Proof. As we have seen in the algebra class, any central simple K-algebra A has some maximal subfield L' that is separable over K. Take L to be the normal closure of L' over K. Then L/K is Galois and L splits A. □

Theorem 2.4.12. *Let $G = \mathrm{Gal}(L/K)$. Then $H^2(G, L^*) \cong \mathrm{Br}(L/K), [f] \mapsto [(L/K, f)]$.*

Proof. The map is a well defined injective group homomorphism, as we have seen before. So we need to prove surjectivity. Let $[A'] \in \mathrm{Br}(L/K)$. Then there is some central simple K-algebra A representing the same class in the Brauer group as A' such that L is a maximal subfield of A.
Claim: $A = (L/K, f)$ for some $f \in Z^2(G, L^*)$:

For $\sigma \in G$ the map $\ell \mapsto \ell^\sigma$ is a K-algebra homomorphism $L \to A$, so by the Theorem of Skolem and Noether, there is some $u_\sigma \in A^*$ such that $\ell^\sigma = u_\sigma^{-1}\ell u_\sigma$ for all $\ell \in L$. We show that $A = \bigoplus_{\sigma\in G} u_\sigma L$. To see this, it is enough to prove that $(u_\sigma \mid \sigma \in G)$ is linearly independent over L, then equality follows by comparing K-dimensions. Let $(a_{\sigma_1}, \ldots, a_{\sigma_k}) \in (L^*)^k$ such that $s := \sum_{i=1}^k u_{\sigma_i} a_{\sigma_i} = 0$ and choose such a relation with minimal k. Then $k \neq 1$, since $u_\sigma \in A^*$ for all $\sigma \in G$. Hence there is some $b \in L^*$ such that $b^{\sigma_1} \neq b^{\sigma_2}$ and $0 = sb^{\sigma_1} - bs$ yields a shorter relation. □

2.4.4 Field extensions.

Ground field extensions.

Let L/K be some Galois extension, E/K arbitrary finite field extension. Then LE/E is Galois. Let $F := E \cap L$. Then

$$\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/F) =: H \leq G := \mathrm{Gal}(L/K).$$

Theorem 2.4.13. *Let $f : G \times G \to L^*$ and $f' := f_{|H}$ the restriction of f to H. Then $f' : H \times H \to L^*$ is a factor system and*

$$E \otimes_K (L/K, f) \cong (EL/E, f').$$

Proof. As above let $F := L \cap E$. We show that
(a) $F \otimes_K (L/K, f) \sim (L/F, f')$ and
(b) $E \otimes_F (L/F, f') \sim (EL/E, f')$.
(a) Let $F' := C_{(L/K,f)}(F)$.
Claim: $F' = (L/F, f')$.
Proof: $(L/F, f') = \bigoplus_{\sigma\in H} u_\sigma L$. For any $a \in F, \sigma \in H$ we have $u_\sigma a = a u_\sigma$, so $(L/F, f') \subseteq F'$. On the other hand for any $x \in F$:

$$x \sum_{\sigma\in G} u_\sigma a_\sigma = \sum_{\sigma\in G} u_\sigma a_\sigma x^\sigma \stackrel{!}{=} \sum_{\sigma\in G} u_\sigma a_\sigma x$$

if and only if $x = x^\sigma$ for all $\sigma \in G$ such that $a_\sigma \neq 0$, because the $(u_\sigma : \sigma \in G)$ form an L-basis of $(L/K, f)$. So equality holds for all $x \in F$ if and only if $a_\sigma = 0$ for all $\sigma \in G \setminus H$.
By the double centralizer theorem $F \otimes_K (L/K, f) \cong (F')^{s\times s}$ which shows (a).
(b) Clearly $E \otimes_F L \cong EL, e \otimes \ell \mapsto e\ell$. So

$$E \otimes_F (L/F, f') = \bigoplus_{\sigma\in H} u_\sigma (E \otimes_F L) = \bigoplus_{\sigma\in \mathrm{Gal}(EL/E)} u_\sigma EL = (EL/E, f').$$

□

Field extensions of L.

We now assume that $E \supseteq L \supseteq K$ is a tower of Galois extensions, $G := \mathrm{Gal}(E/K)$ and $H := \mathrm{Gal}(E/L) \trianglelefteq G$ so that $G/H = \overline{G} = \mathrm{Gal}(L/K)$. For any factor system $f : \overline{G} \times \overline{G} \to L^*$ let $\tilde{f} : G \times G \to L^*$ be the factor system defined by $\tilde{f}_{g,h} := f_{\overline{g},\overline{h}}$ ("obtained by inflation").

Theorem 2.4.14. *$(E/K, \tilde{f}) \cong (L/K, f)^{r\times r} =: B$, with $r = [E : L]$.*

Proof. Let

$$B := (L/K, f)^{r\times r} = (L/K, f) \otimes_K K^{r\times r} = \bigoplus_{\sigma\in\overline{G}} u_\sigma L^{r\times r}.$$

$$\begin{array}{rcl} (E/L, 1) = \bigoplus_{h\in H} v_h E & \xrightarrow{\sim} & \mathrm{End}_L(E) = L^{r\times r} \\ v_h & \mapsto & (x \mapsto x^h) \\ e & \mapsto & T(e) : x \mapsto xe \end{array}$$

For any L-basis $(e_1, \ldots, e_r)$ of E and $\sigma \in G$ also $(e_1^\sigma, \ldots, e_r^\sigma)$ is an L-basis of E so there is some $P(\sigma) \in \mathrm{GL}_r(L)$ such that

$$P(\sigma) \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} e_1^\sigma \\ \vdots \\ e_r^\sigma \end{pmatrix}.$$

Moreover for $\sigma, \rho \in G$ we compute $P(\sigma\rho) = P(\sigma)^\rho P(\rho)$:

$$\begin{pmatrix} e_1^{\sigma\rho} \\ \vdots \\ e_r^{\sigma\rho} \end{pmatrix} = \left(P(\sigma) \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} \right)^\rho = P(\sigma)^\rho P(\rho) \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix}.$$

Here a matrix $^\rho$ means that one applies ρ to all entries of the matrix. For any $e \in E$ let $T(e) \in \mathrm{GL}_r(L)$ denote the matrix of $x \mapsto xe$ with respect to the chosen basis. Then

$$T(e^\sigma) = \text{ matrix of } x \mapsto x(e^\sigma) = P(\sigma)^{-1} T(e)^\sigma P(\sigma).$$

Put $u_\sigma := u_{\overline{\sigma}} P(\sigma)$ for $\sigma \in G$. Then $B = \bigoplus_{\sigma\in G} u_\sigma E$ with

$$\begin{aligned} u_\sigma u_\tau &= u_{\overline{\sigma}} P(\sigma) u_{\overline{\tau}} P(\tau) = u_{\overline{\sigma}} u_{\overline{\tau}} P(\sigma)^\tau P(\tau) \\ &= u_{\overline{\sigma\tau}} f_{\overline{\sigma},\overline{\tau}} P(\sigma\tau) = u_{\overline{\sigma\tau}} P(\sigma\tau) f_{\overline{\sigma},\overline{\tau}} = u_{\sigma\tau} f_{\overline{\sigma},\overline{\tau}}. \end{aligned}$$

For $x \in E$ and $\sigma \in G$ we compute

$$T(x) u_\sigma = T(x) u_{\overline{\sigma}} P(\sigma) = u_{\overline{\sigma}} T(x)^\sigma P(\sigma) = u_{\overline{\sigma}} P(\sigma) T(x^\sigma) = u_\sigma T(x^\sigma).$$

Therefore $B \cong (E/K, \tilde{f})$. □

We hence have the following commutative diagrams for a tower of fields $L \supseteq F \supseteq K$:

$$\begin{array}{ccc} H^2(G, L^*) & \overset{\mathrm{res}^G_H}{\to} & H^2(H, L^*) \\ \cong\downarrow & & \downarrow\cong \\ \mathrm{Br}(L/K) & \overset{\otimes_K F}{\to} & \mathrm{Br}(L/F) \end{array} \quad \text{and} \quad \begin{array}{ccc} H^2(\overline{G}, F^*) & \overset{\mathrm{infl}^G}{\to} & H^2(G, L^*) \\ \cong\downarrow & & \downarrow\cong \\ \mathrm{Br}(F/K) & \hookrightarrow & \mathrm{Br}(L/K) \end{array}$$

Here $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/F)$. For the second diagram we need to assume that $H \trianglelefteq G$ and put $\overline{G} := G/H$.

2.4.5 A group isomorphism $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Let K be a complete field with valuation ring R and residue class field $\mathbb{F}_q = R/\pi R$. Let $F \in \mathrm{Aut}(unr(K))$ denote the Frobenius automorphism of the maximal totally unramified extension of K, mapping any p'-root of unity ζ to ζ^q.

Theorem 2.4.15. *Let D be some central K-division algebra with Hasse invariant $\frac{r}{m}$. Then $D \cong (L/K, \sigma, \pi) \cong (L/K, F, \pi^s)$ with $L = K[\zeta_{q^m-1}]$, $\sigma = F^{-r}$, $sr \equiv -1 \pmod m$.*
Define $\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}, (L/K, F, \pi^s) \mapsto \frac{s}{m}$.

Proof. Choose some maximal subfield $L \leq D$ isomorphic to $K[\zeta_{q^m-1}]$ and put $u := \pi_D$, so that $\pi_D^m = \pi$ and $\zeta := \zeta_{q^m-1}$ so that $\pi_D \zeta \pi_D^{-1} = \zeta^{q^r}$ as in Theorem 2.3.12. Then $D = \bigoplus_{j=0}^{m-1} \pi_D^j L \cong (L/K, F^{-r}, \pi)$ since $\zeta\pi_D = \pi_D(\pi_D^{-1}\zeta\pi_D) = \pi_D\zeta^{q^{-r}} = \pi_D\zeta^\sigma$. Therefore conjugation by π_D^s induces the Frobenius automorphism on L. □

Theorem 2.4.16. $\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}, (L/K, F, \pi^s) \mapsto \frac{s}{m}$ *is a group isomorphism.*

Proof. The bijectivity of this map follows from the bijectivity of the Hasse invariant, which is not a group homomorphism. We need to show the homomorphism property:
So let $\mathrm{inv}(D) = \frac{s}{m}$, $\mathrm{inv}(D') = \frac{s'}{m'}$ we need to show that $\mathrm{inv}(D \otimes D') = \frac{s}{m} + \frac{s'}{m'}$.
Let $m'' = lcm(m, m')$ and $L'' := K[\zeta_{q^{m''}-1}]$
Then $[D]$, $[D']$ and hence also $[D \otimes D']$ are in $\mathrm{Br}(L''/K)$.

$$D = (L/K, F, \pi^s) \sim (L''/K, F'', \pi^{s_1}) \text{ and } D' = (L'/K, F', \pi^{s'}) \sim (L''/K, F'', \pi^{s_2})$$

with $s_1 = s[L'' : L] = s\frac{m''}{m}$ and $s_2 = s'[L'' : L'] = s'\frac{m''}{m'}$. So the tensor product

$$D \otimes D' \sim (L''/K, F'', \pi^{s_1+s_2}) \text{ and } \frac{s_1 + s_2}{m''} = \frac{s}{m} + \frac{s'}{m'}.$$

□

Corollary 2.4.17. *If $A = D^{n\times n}$ with a central K-division algebra D of index m, then $[A] = [D]$ has order m in* $\mathrm{Br}(K)$.

Concerning field extensions we obtain from the preceeding sections the following commutative diagram

Theorem 2.4.18. *Let E/K be a finite extension of degree $d := [E : K]$. Then*

$$\begin{array}{ccc} \mathrm{Br}(K) & \stackrel{\mathrm{inv}_K}{\to} & \mathbb{Q}/\mathbb{Z} \\ E\otimes_K \downarrow & & \downarrow \cdot d \\ \mathrm{Br}(E) & \stackrel{\mathrm{inv}_E}{\to} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative.

Proof. Let $W := K[\zeta_{q^m-1}]$ and put $A = (W/K, F, \pi^s)$, so that $\mathrm{inv}_K(A) = \frac{s}{m}$. Let $L := E/capW$. Then L/K is an unramified extension of degree, say, d. Let $m' \in \mathbb{N}$ be such that $m = m'd$. Then

$$E \otimes_K A \sim (EW/E, F^d, \pi^s) =: B.$$

We want to compute $\mathrm{inv}_E(B)$. Let $e := e(E/K)$ be the ramificatin index and $f := f(E/K) = df'$ the inertia degree. Then the Frobenius over E is F^f and $B \cong (EW/E, F^{df'}, \pi^{sf'})$, so

$$\mathrm{inv}_E(B) = \frac{v_E(\pi^{sf'})}{m'} = \frac{sf'e}{m'} = \frac{s}{m}fe.$$

□

Corollary 2.4.19. *Let D be a central K-division algebra of index m. Then a finite extension field E of K splits D if and only if m divides $[E : K]$. And E is a maximal subfield of D, if and only if $[E : K] = m$.*

Corollary 2.4.20. *If $[E : K] = n$, then $\mathrm{Br}(E/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong C_n$. Moreover $\mathrm{Br}(E/K) = \{[A] \in \mathrm{Br}(K) \mid [A]^n = 1\}$.*

2.5 Division algebras over global fields.

Global fields are either finite extensions of $\mathbb{Q}$ (algebraic number fields) or function fields over finite fields. Though most of the theory is parallel for both sorts of global fields, we will restrict to the algebraic number fields, which have been introduced in the first part of this lectures.

So let K be an algebraic number field with ring of integers R. A **place** of K is either a finite place given by a maximal ideal $\wp \trianglelefteq R$ or an infinite place, i.e. an embedding $\sigma : K \to \mathbb{C}$. An infinite place is called **real**, if $\sigma(K) \subseteq \mathbb{R}$. For a place $\wp$ let $K_\wp$ denote the completion of K at $\wp$. If $\wp$ is real then $K_\wp = \mathbb{R}$, for complex places $K_\wp = \mathbb{C}$ and for finite places this is a p-adic number field.

Theorem 2.5.1. *Let A be a central simple K-algebra. Then $[A_\wp] \neq 0$ only for finitely many places $\wp$ of K.*

Proof. Let $\Lambda \subseteq A$ be some R-order in A. Then there are only finitely many prime ideals $\wp \trianglelefteq R$ that divide the discriminant of Λ. For any prime $\wp$ not dividing the discriminant of Λ the order $\Lambda_\wp \leq A_\wp$ is a maximal $R_\wp$-order of discriminant 1. For all these places $[A_\wp] = 0$. □

Remark 2.5.2. $\mathrm{Br}(K) \to \bigoplus_{\wp \ place} \mathrm{Br}(K_\wp), [A] \mapsto [A_\wp]$ *where $A_\wp =: A \otimes_K K_\wp$ is a group homomorphism.*

For finite places we have seen that $\mathrm{Br}(K_\wp) \cong \mathbb{Q}/\mathbb{Z}$ via the variant of the Hasse invariant that is a group homomorphism. Moreover $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ where $\mathrm{inv}([\mathbb{H}]) = \frac{1}{2}$ and $\mathrm{Br}(\mathbb{C}) = \{0\}$.

Definition 2.5.3. *Define a group homomorphism*

$$\text{inv} : \text{Br}(K) \to \bigoplus_{\wp \text{ finite}} \mathbb{Q}/\mathbb{Z} \oplus \bigoplus_{\sigma \text{ real}} \frac{1}{2}\mathbb{Z}/\mathbb{Z}, [A] \mapsto (\text{inv}[A_\wp])_{\wp \text{ finite}} + (\text{inv}[A \otimes_{\sigma(K)} \mathbb{R}])_{\sigma \text{ real}}$$

and $\text{inv}_\wp : \text{Br}(K) \to \mathbb{Q}/\mathbb{Z}, [A] \mapsto \text{inv}[A_\wp]$, *for* $\wp \trianglelefteq R$ *and* $\text{inv}_\sigma : \text{Br}(K) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}, [A] \mapsto \text{inv}[A \otimes_{\sigma(K)} \mathbb{R}]$ *for any real place* σ *and* $\text{inv}_\tau : \text{Br}(K) \to \{0\}$ *for the complex places* τ *of* K.

We want to prove a local-global principle for central simple K-algebras (see Theorem 2.5.6 below). To prove this theorem we need one result the proof of which needs class field theory, so goes beyond the scope of this lecture:

Theorem 2.5.4. *(***Hasse Norm Theorem***) Let* L *be a finite cyclic extension (so* $\text{Gal}(L/K)$ *is cyclic) of the number field* K *and let* $a \in K$. *For any place* $\wp$ *of* K *we choose some place* P *of* L *that extends* $\wp$. *Then for* $a \in K$ *it holds that*

$$a \in N_{L/K}(L) \Leftrightarrow a \in N_{L_P/K_\wp}(L_P) \text{ for all } \wp.$$

Note that the condition on the right hand side also includes the infinite places.
The theorem is false, without the assumption that L/K be cyclic.
The direction $\Rightarrow$ is almost trivial (see blackboard).

Corollary 2.5.5. *Let* $A = (L/K, \sigma, a)$ *be a cyclic algebra. Then* $[A] = [K] \in \text{Br}(K)$ *if and only if* $[A_\wp] = [K_\wp] \in \text{Br}(K_\wp)$ *for all (finite and infinite) places* $\wp$ *of* K.

Proof. We have seen in the exercises that $[(L/K, \sigma, a)] = [K]$ if and only if $a \in N_{L/K}(L^*)$, so if and only if a is a global norm. On the other hand $A_\wp = (L_P/K_\wp, \sigma^k, a)$ for some k such that $\langle \sigma^k \rangle = \langle \sigma \rangle = \text{Gal}(L/K)$. So $[A_\wp] = [K_\wp] \in \text{Br}(K_\wp)$ if and only if $a \in N_{L_P/K_\wp}(L_P^*)$ is a local norm. So the Corollary follows from the Hasse Norm Theorem. □

Theorem 2.5.6. *(***Hasse-Brauer-Noether-Albert-Theorem***) Let* A *be a central simple* K*-algebra. Then* $[A] = [K] \in \text{Br}(K)$ *if and only if* $[A_\wp] = [K_\wp] \in \text{Br}(K_\wp)$ *for all (finite and infinite) places* $\wp$ *of* K.
So the group homomorphism inv *from Definition 2.5.3 is injective.*

Proof. $\Rightarrow$ is clear. So assume that $[A_\wp] = [K_\wp] \in \text{Br}(K_\wp)$ for all places $\wp$ of K but $[A] \neq [K] \in \text{Br}(K)$. Then the index m of A is $m > 1$. By Theorem 2.4.11 there is a finite Galois extension L of K that splits A, so $L \otimes_K A \cong L^{k \times k}$ for some k. Let p be a prime divisor of m and H a Sylow p-subgroup of $G = \text{Gal}(L/K)$. Choose some subnormal series

$$1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \ldots \trianglelefteq H_0 = H, \text{ such that } [H_j : H_{j-1}] = p$$

and let E_j be the fixed field of H_j for $j = 0, \ldots, n$. Then $E_n = L$, E_j/E_{j+1} is a cyclic extension and, since p does not divide $[E_0 : K]$ the index of $A_0 := E_0 \otimes_K A$ is not 1. Let $F := E_{n-1}$ and $B := F \otimes_K A$. Then L splits B, so B is similar to some cyclic algebra $B \sim C := (L/F, \sigma, b)$ for some $b \in F^*$. Now $C_\wp \sim F_\wp$ for all places $\wp$ of F by assumption. This is equivalent to the fact that $b \in N_{L_P/F_\wp}(L_P^*)$ for all places $\wp$. By the Hasse Norm Theorem this implies that b is a global norm and hence $C \sim F$ and so F splits A. Similarly one obtains that E_{n-2} splits A etc until E_0 splits A so in particular $m \mid [E_0 : K]$ which contradicts our assumption that p divides m but does not divide $[E_0 : K]$. □

Remark 2.5.7. *One may show that* $\sum_\wp \mathrm{inv}_\wp = 0$ *and that this is the only condition on the local Hasse invariants of a global central simple algebra, so the following sequence is exact*

$$1 \to \mathrm{Br}(K) \to \bigoplus_{\wp} \mathrm{Br}(K_\wp) \cong \bigoplus_{\wp \text{ finite}} \mathbb{Q}/\mathbb{Z} \oplus \bigoplus_{\wp \text{ real}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0$$

Theorem 2.5.8. *Let* A *be a central simple* K*-algebra and put* $m_\wp := \mathrm{inv}_\wp[A] = \mathrm{inv}([A_\wp])$ *for any (finite or infinite) place* $\wp$ *of* K*. Let* L *be a finite extension of* K*. Then* L *splits* A *if and only if for each place* P *of* L

$$m_\wp \text{ divides } [L_P : K_\wp]$$

where $\wp := P \cap K = P_{|K}$ *is the restriction of* P *to* K*.*

Proof. $[L \otimes_K A]$ is trivial if and only if $[L_P \otimes_{K_\wp} A_\wp]$ is trivial for all $\wp$. Moreover by Corollary 2.4.19 this is equivalent to $m_\wp \mid [L_P : K_\wp]$. □

Theorem 2.5.9. *Let* A *be a central simple* K*-algebra and put* $m_\wp := \mathrm{inv}_\wp[A] = \mathrm{inv}([A_\wp])$ *for any (finite or infinite) place* $\wp$ *of* K*. Then the order of* $[A] \in \mathrm{Br}(K)$ *is the least common multiple of all the local Schur indices* $m_\wp$*.*

Proof. Because the order of $[A_\wp] \in \mathrm{Br}(K_\wp)$ is exactly $m_\wp$. □

We aim to show that the order of $[A]$ in $\mathrm{Br}(K)$ is exactly the index of the underlying division algebra. For this we need a very deep theorem which we cannot prove here:

Theorem 2.5.10. *(***Grunwald-Wang Theorem***) Let* $\{\wp_1, \ldots, \wp_s\}$ *be a finite set of places of the global field* K *and let* $(m_{\wp_1}, \ldots, m_{\wp_s}) \in \mathbb{N}^s$ *be given so that* $m_\wp = 1$ *if* $\wp$ *is a complex place and* $m_\wp = 1$ *or* 2 *if* $\wp$ *is a real place. Let* $n \in \mathbb{N}$ *be divisible by all* $m_{\wp_i}$*. Then there is a cyclic extension* L/K *with*

$$[L : K] = n, \ [L_{P_i} : K_{\wp_i}] = m_{\wp_i} \text{ for all } i = 1, \ldots, s$$

where P_i *is some prime of* L *extending* $\wp_i$*.*

Theorem 2.5.11. *Let* A *be a central simple* K*-algebra and put* $m_\wp := \mathrm{inv}_\wp[A] = \mathrm{inv}([A_\wp])$ *for any (finite or infinite) place* $\wp$ *of* K*. Then the global Schur index of* A *is the order of* $[A] \in \mathrm{Br}(K)$*, i.e. the least common multiple of all the local Schur indices* $m_\wp$*.*

Proof. Let L be a cyclic extension of K as in the Grunwald-Wang theorem with $n := [L : K] = lcm(m_\wp)$. Then by Corollary 2.4.19 L_P splits $A_\wp$ for all places $\wp$ of K and hence L splits A. By Theorem 2.4.9 this implies that the index of A divides $[L : K] = n$. By Theorem 2.5.9 the number n is equal to the order of $[A]$ in $\mathrm{Br}(K)$. It holds in general, that the order of $[A]$ divides the index of A, so equality follows. □

Corollary 2.5.12. *Every central simple* K*-algebra* A *is a cyclic algebra, so there is a cyclic Galois extension* L *of* K *with* $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ *and some* $a \in K^*$ *such that* $A = (L/K, \sigma, a)$*.*

Proof. Choose L as in the last proof but with $n \in \mathbb{N}$ such that $n^2 = [A : K]$. Then n is a multiple of all local Schur indices and we may apply again the Grunwald-Wang theorem. □

2.5.1 Surjectivity of the reduced norm

Let K be a number field, $\wp$ a place of K and $K_\wp$ the completion of K at $\wp$.

Remark 2.5.13. *Let $D_\wp$ be a central $K_\wp$-division algebra. If $K_\wp \neq \mathbb{R}$ then the reduced norm $D_\wp \to K_\wp$ is surjective.*
The image of the reduced norm of $\left(\frac{-1,-1}{\mathbb{R}}\right) =: H$ is $\mathbb{R}_{\geq 0}$.

Proof. Assume that $\wp$ is a finite place (otherwise nothing to show). Let $R_\wp$ be the valuation ring in $K_\wp$. Then any element $a \in K_\wp^*$ has a unique expression as $a = u\pi^n$ with $n = v(a) \in \mathbb{Z}$ and $u \in R_\wp^*$. Let $L_\wp \leq D_\wp$ be a maximal unramified subfield of $D_\wp$. Then the reduced norm of $L_\wp^*$ contains $R_\wp^*$. Moreover the reduced norm of a prime element in $D_\wp$ is a prime element in $R_\wp$. So u and π^n are reduced norms and the surjectivity follows. □

Remark 2.5.14. $N(D^{n\times n}) = N(D)$.

Theorem 2.5.15. *(***Hasse-Schilling-Maass***) Let A be a central simple K-algebra and let $\alpha \in K^*$. Then α is a reduced norm of A if and only if $\sigma(\alpha) > 0$ for all real places σ of K that ramify in A ($[A \otimes_{K,\sigma} \mathbb{R}] = [H] \in \mathrm{Br}(\mathbb{R})$).*

Proof. Let S denote the set of real places of K that ramify in A and put $U(A) := \{\alpha \in K \mid \sigma(\alpha) > 0 \text{ for all } \sigma \in S\}$. We need to show that for any $\beta \in U(A)$ there is some $a \in A$ such that $N(a) = \beta$. Let $n^2 := [A : K]$. Then n is even if S is non empty. Let S' be a non empty finite set of finite primes of K that contains all finite primes of K that ramify in A.
Let $\beta \in U(A)$.
(a) For all $P \in S'$ the element β is a reduced norm of some element in the completion A_P, so we may find an irreducible polynomial

$$f_P(X) := X^n + a_{1,P}X^{n-1} + \ldots + a_{n-1,P}X + (-1)^n\beta \in K_P[X].$$

If S is non-empty then n is even and we put

$$f_P(X) := X^n + (-1)^n\beta \in K_P[X] \text{ for all } P \in S.$$

By the strong approximation theorem (Chinese remainder theorem) for any $\epsilon > 0$ there is some polynomial

$$f(X) := X^n + c_1X^{n-1} + \ldots + c_{n-1}X + (-1)^n\beta \in K[X]$$

such that

$$\begin{array}{lll} ||c_i - a_{i,P}||_P < \epsilon & 1 \leq i \leq n-1 & \text{for all } P \in S' \\ ||c_i||_P < \epsilon & 1 \leq i \leq n-1 & \text{for all } P \in S \end{array}$$

If ϵ is small, then f is irreducible in $K_P[X]$, since f_P is irreducible for all $P \in S' \neq \emptyset$. If $S \neq \emptyset$ then n is even and since $\sigma(\beta) > 0$ for all $\sigma \in S$ the polynomial $\sigma(f)$ has no real roots for sufficiently small ϵ. Let $L := K[X]/(f(X))$. Then all local degrees $[L_P : K_P]$ are multiples of the local Schur index since $[L_P : K_P] = n$ for $P \in S'$ and $L_P = \mathbb{C}$ for $P \in S$. So L is a splitting field of A and we may embed L as a maximal subfield of A. In particular there is some $a \in A$ such that $f(a) = 0$. This element has reduced norm β. □

2.6 Maximal orders in separable algebras.

The book by Max Deuring: Algebren (Springer Grundlehren) gives a very nice treatment of most of the results of the second part of this lecture.

Let K be a number field, $R = \mathbb{Z}_K$ the ring of integers in K and A a separable K-algebra. (Many things hold in the more general context that R is a Dedekind domain with field of fractions K).

If Λ is a maximal R-order in A, then the completion $\hat{\Lambda}_\wp$ is a maximal $\hat{R}_\wp$-order in $A_\wp$. Moreover

$$A_\wp = \bigoplus A_i,\ Z(A_i) = L_i,\ A_i \text{ simple }, \hat{\Lambda}_\wp = \bigoplus \Lambda_i$$

where Λ_i is a (up to conjugacy unique) maximal $\mathbb{Z}_{L_i}$-order in A_i.

Definition 2.6.1. *(a) Let Λ be an R-order in A. A* **prime ideal** *$\mathcal{P}$ of Λ is a proper non-zero two-sided ideal $\mathcal{P} \trianglelefteq \Lambda$ with $K\mathcal{P} = A$ such that for any pair S, T of two-sided Λ-ideals*

$$ST \subseteq \mathcal{P} \Rightarrow S \subseteq \mathcal{P} \text{ or } T \subseteq \mathcal{P}.$$

(b) Let $M \leq A$ be a full R-lattice in A. Then M is called a **normal ideal***, if $O_l(M)$ is a maximal order in A. An* **integral ideal** *is a normal ideal M such that $M \subseteq O_l(M)$. A* **maximal integral ideal** *is an integral ideal which is a maximal left ideal of its left order.*

Remark 2.6.2. *(a) Maximal 2-sided ideals are prime ideals.*
(b) Clearly $M \subseteq O_l(M)$ if and only if $M \cdot M \subseteq M$ which is equivalent to $M \subseteq O_r(M)$. In particular the notion of integrality does not depend on the choice of left or right order.

Theorem 2.6.3. *Let $\wp$ be some prime ideal of R and $\Lambda_\wp$ a maximal $R_\wp$-order in the separable K-algebra A. Then any left $\Lambda_\wp$-lattice L in A is free, i.e. there is some $y \in A$ such that $L = \Lambda_\wp y$.*

Proof. (a) Wlog we may assume that A is central simple: If $A = \bigoplus_i A_i$, then $\Lambda_\wp = \bigoplus \Lambda_i$ with maximal R_i-orders Λ_i in A_i. So $L = \bigoplus L_i$. If $L_i = \Lambda_i y_i$ then $L = \Lambda_\wp y$ with $y = \sum y_i \in A$.
(b) For the central simple case we pass to the completion of A at $\wp$. For the complete ring $\hat{\Lambda}_\wp$-lattices in the simple $\hat{A}_\wp$-module $V = \hat{A}_\wp e$ form a chain, so any $\hat{\Lambda}_\wp$-lattice is generated by any element that is not in the unique proper maximal sublattice. Since $\hat{A}_\wp = \bigoplus_e \hat{A}_\wp e$ the sum of the generators of $\hat{L}_\wp e$ is a generator for L. □

For a full R-lattice L in A we define

$$L^{-1} = \{x \in A \mid LxL \subseteq L\}.$$

Then L^{-1} is again a full R-lattice in A and $O_r(L^{-1}) \supseteq O_l(L), O_l(L^{-1}) \supseteq O_r(L)$.

Theorem 2.6.4. *Let Λ be a maximal order in the separable K-algebra A. Let L be a full left Λ-lattice in A. Then*

$$LL^{-1} = \Lambda,\ L^{-1}L = O_r(L),\ (L^{-1})^{-1} = L,\ O_l(L^{-1}) = O_r(L).$$

Proof. Since equality of lattices is a local property, it is enough to show the equalities for all localisations $L_\wp$ at prime ideals of R. But then $L_\wp$ is a principal $\Lambda_\wp$-ideal, so $L_\wp = \Lambda_\wp y_\wp$ for some $y_\wp \in A$, $O_r(L_\wp) = y_\wp^{-1}\Lambda_\wp y_\wp$, and $(L_\wp)^{-1} = y_\wp^{-1}\Lambda_\wp$, from which one sees all equalities. □

Theorem 2.6.5. *Let M be a full R-lattice in A. Then $O_l(M)$ is a maximal R-order if and only if $O_r(M)$ is a maximal R-order. So the notion of normality is independent from left and right.*

Proof. Being a maximal order is a local property, so we may pass to all localizations. But locally all left ideals of a maximal order are free, so locally the right order and the left order are conjugate and hence also the right order is a maximal order. □

2.6.1 The group of two-sided ideals.

We want to show that maximal R-orders Λ in skewfields are Dedekind domains. We could proceed as in the commutative case: Λ is Noetherian (since it is finite dimensional over R) and all completions of Λ are discrete valuation rings.

Theorem 2.6.6. *Let Λ be an R-order in A. Then the prime ideals of Λ are exactly the maximal ideals of Λ. If $\mathcal{P}$ is a prime ideal of Λ then $\wp := R \cap \mathcal{P}$ is a prime ideal of R and $\overline{\Lambda} := \Lambda/\mathcal{P}$ is a finite dimensional simple $R/\wp$-algebra.*

Proof. Clearly $\wp := R\cap\mathcal{P}$ is a prime ideal of R. Let $\overline{\Lambda} := \Lambda/\mathcal{P}$. Then $\overline{\Lambda}$ is a finite dimensional $R/\wp$-algebra and hence Artinian, so the Jacobson radical $J(\overline{\Lambda})$ is a nilpotent ideal. Since $\mathcal{P}$ is a prime ideal this implies that $J(\overline{\Lambda}) = 0$, so $\overline{\Lambda}$ is semi-simple. In fact it is simple since any product of non-zero ideals is again non-zero. But this means that $\mathcal{P}$ is a maximal ideal. □

Theorem 2.6.7. *Let Λ be a maximal R-order in the central simple K-algebra A. Then $\mathcal{P} \mapsto \wp := \mathcal{P} \cap R$ defines a bijection between the set of prime ideals $\mathcal{P}$ of Λ and those of R. Moreover $\mathcal{P}$ is the radical of the localisation $\Lambda_\wp$ and for each prime ideal $Q \neq \wp$ of R we have $\mathcal{P}_Q = \Lambda_Q$.*

Proof. Let $\mathcal{P}$ be a prime ideal of Λ and $\wp := \mathcal{P} \cap R$. The ideals of $\Lambda_\wp$ are all powers of the radical $J(\Lambda_\wp)$ (take the completion to obtain a matrix ring over a discrete valuation ring). Being a maximal ideal of Λ we obtain $\mathcal{P}_\wp = J(\Lambda_\wp)$. Moreover $\mathcal{P}_Q = \Lambda_Q$ for all other primes Q of R, since $(\wp\Lambda)_Q = \Lambda_Q$. So

$$\mathcal{P} = J(\Lambda_\wp) \cap \Lambda$$

is uniquely determined by $\wp$. One the other hand, given some prime ideal $\wp$ of R, the ideal $\mathcal{P}$ with $\mathcal{P}_\wp = J(\Lambda_\wp)$ and $\mathcal{P}_Q = \Lambda_Q$ for all $Q \neq \wp$ is a maximal 2-sided ideal with $\Lambda/\mathcal{P} \cong \Lambda_\wp/\mathcal{P}_\wp$. □

Theorem 2.6.8. *Let Λ be a maximal order in the central simple K-algebra A. Then the set of two-sided Λ-ideals $I(\Lambda)$ in A is the free abelian group on the prime ideals of Λ.*

Proof. Pass to the localizations to see that any two-sided Λ-ideal has a unique factorization as product of prime ideals. □

Corollary 2.6.9. *The theorem above holds more general for any maximal order Λ in a separable K-algebra.*

Proof. Maximal orders Λ in $\bigoplus A_i$ are direct sums $\Lambda = \bigoplus \Lambda_i$ for maximal $\mathrm{Int}_R(Z(A_i))$-orders Λ_i in the simple $Z(A_i)$-algebra A_i. Similarly all Λ-lattices decompose into a direct sum. □

Theorem 2.6.10. *Let K be a number field with ring of integers R, L/K a finite extension. Let Λ be a maximal order in some central simple L-algebra A, $S = \mathrm{Int}_R(L)$ the ring of integers in L. Given a prime ideal $\wp \trianglelefteq R$ let $\wp S = \wp_1^{e_1} \cdots \wp_d^{e_d}$ be the prime ideal factorization in S. Let $\mathcal{P}_i$ be the prime ideal of Λ that contains $\wp_i\Lambda$. Then $\wp_i\Lambda = \mathcal{P}_i^{m_i}$ where m_i is the Schur index of the $\wp_i$-adic completion of A. Moreover $\wp\Lambda = \prod_{i=1}^{d} \mathcal{P}_i^{e_i m_i}$. We have that $m_i = 1$ for almost all $\wp_i$ and the dual*

$$\Lambda^{\#} := \{a \in A \mid trace(a\Lambda) \subseteq S\} = \prod_{\wp_i} \mathcal{P}_i^{1-m_i}\Lambda$$

where the product runs through the prime ideals $\wp_i$ of S for which $m_i > 1$.

Proof. Exercises. □

Remark 2.6.11. *Let Λ be a maximal order in the central simple K-algebra A. Let $P(\Lambda)$ denote the set of two-sided Λ-ideals which are principal as left ideals, i.e.*

$$P(\Lambda) := \{\Lambda a \mid a \in A^*, \Lambda a \Lambda = \Lambda a\}.$$

Then $P(\Lambda) \leq I(\Lambda)$. The factor group is called the **ideal class group** *of Λ and its order is called the 2-sided classnumber of Λ, $H(\Lambda) := |I(\Lambda)/P(\Lambda)|$. The 2-sided classnumber of Λ is finite. More precisely*

$$H(\Lambda) \leq \prod_{\wp} m_{\wp}(A)h(R).$$

Here the product runs over all prime ideals $\wp$ of R that ramify in A and $m_\wp$ is the local Schur index at $\wp$.

2.6.2 The Brandt groupoid.

We now pass to one-sided ideals. If M, N are left ideals of the maximal order Λ, then it does not make sense to define the product MN. Let Λ_1 be a maximal order in A and M a left ideal of Λ_1. Then M is normal and hence also $\Lambda_2 := O_r(M)$ is a maximal order in A. We will indicate this are ${}_1M_2$, which means that $\Lambda_1\ {}_1M_2\Lambda_2 = {}_1M_2$. Given ideals ${}_1M_2$, ${}_2N_3$ we may multiply them as usual to obtain

$${}_1I_3 = {}_1M_2\ {}_2N_3 = \langle mn \mid m \in M, n \in N\rangle_R.$$

So the set of normal ideals in A forms a **groupoid** the so called Brandt groupoid.

Note that if $M = \Lambda_1 y$ is a principal left ideal, then $\Lambda_2 = y^{-1}\Lambda_1 y$ is conjugate to Λ_1.

Theorem 2.6.12. *Let Λ_1 and Λ_2 be maximal orders in A. Then there is a left Λ_1-ideal ${}_1M_2$ which has right order Λ_2. Any such ideal M defines a group isomorphism*

$$\varphi_{12} : I(\Lambda_1) \to I(\Lambda_2), I \mapsto M^{-1}IM$$

between the group of two-sided ideals of Λ_1 and Λ_2. The isomorphism φ_{12} is independent of the choice of M.

Proof. $M := \Lambda_1\Lambda_2$ is such an ideal with $O_l(M) = \Lambda_1$ and $O_r(M) = \Lambda_2$. That φ_{12} is a group isomorphism is clear, the inverse is $\varphi_{21} : I \mapsto MIM^{-1}$. Let ${}_1N_2$ be another $\Lambda_1 - \Lambda_2$-ideal and denote the resulting isomorphism by ψ_{12}. Then

$$\psi_{12}^{-1} \circ \varphi_{12}(I) = NM^{-1}IMN^{-1} = (MN^{-1})^{-1}(MN^{-1})I = I$$

for all $I \in I(\Lambda_1)$, since $I(\Lambda_1)$ is a commutative group and $(MN^{-1}) \in I(\Lambda_1)$. □

Definition 2.6.13. *(***classnumber and typenumber***) Let Λ be some maximal order in A. Two left Λ-ideals M and N are called* **isomorphic** *(or* **equivalent***) if there is some $a \in A$ such that $Ma = N$. The number of isomorphism classes of left Λ-ideals is called the* **classnumber** *$h(\Lambda)$.*
Two left Λ-ideals M and N are called **weakly equivalent***, if there is some two-sided Λ-ideal I and some $a \in A$ such that $IMa = N$.*
The number of conjugacy classes of maximal orders in A is called the **typenumber** *$t(A)$ of A.*

We will show below that $h(\Lambda)$ is finite for any R-order Λ in A.

Remark 2.6.14. *The group of twosided ideals $I(\Lambda)$ acts on the set of left Λ-ideals by left multiplication and also on the set of isomorphism classes of left Λ-ideals. Two left Λ-ideals M and N are weakly equivalent, if and only if they are in the same $I(\Lambda)$-orbit on the set of isomorphism classes of left Λ-ideals.*
The right orders of weakly equivalent left Λ-ideals are conjugate.

Theorem 2.6.15. *$t(A)$ is the number of weak equivalence classes of left Λ-ideal for any maximal order Λ.*

Proof. We have already seen that for any maximal order Γ in A there is some left Λ-ideal M such that $O_r(M) = \Gamma$. So all types of maximal orders occur as right orders of some fixed set of representatives of the weak equivalence classes of left Λ-ideals. Now let M and N be Λ-Γ bimodules, so left Λ-ideals with right order Γ. We need to show that M and N are weakly equivalent left Λ-ideals. Now $\Gamma = M^{-1}M = N^{-1}N$ and hence $M = M\Gamma = MN^{-1}N = IN$ for $I = MN^{-1} \in I(\Lambda)$. □

2.6.3 The finiteness of the class number.

Let M be a left Λ-ideal. Then M is equivalent to some integral ideal i.e. there is some $a \in A$ such that $Ma \leq \Lambda$. This is because M and Λ are finitely generated R-submodules of A and also full lattices. So they have compatible bases and we may take the denominators.
The theorem proven in this subsection (finiteness of the class number) is valid in a more general case that Λ is an order over some Dedekind domain. This is the Theorem by Jordan and Zassenhaus (see for instance Section 26 of Reiner's book Maximal orders).
Here we want to restrict to the case where K is a number field and $R = \mathbb{Z}_K$. In particular any R-order is a $\mathbb{Z}$-order and we may use Geometry of numbers to obtain explicit bounds on the norm of the integral ideals that represent all isomorphism classes of left Λ-ideals as in the commutative case. This exposition follows the book by Max Deuring (Algebren).
So assume that K is a number field.

Definition 2.6.16. *Let Λ be a maximal R-order in the separable K-algebra A. The* **norm** *of an integral left Λ-ideal M is $N(M) := |\Lambda/M|$. For an arbitary left Λ-ideal M we may always choose some invertible $a \in A$ such that $Ma \leq \Lambda$. Then $N(M) = N(Ma)N_{A/\mathbb{Q}}(a)^{-1}$ where $N_{A/\mathbb{Q}}$ is the regular norm over the rationals.*

Remark 2.6.17. *The norm of a two-sided prime ideal is a prime power.*
Let $\wp$ be a prime ideal of R, Γ and Λ be maximal R-orders in A and $\mathcal{P}_\Gamma$ and $\mathcal{P}_\Lambda$ the two-sided prime ideals of Γ resp. Λ that contain $\wp\Gamma$ resp. $\wp\Lambda$. Then $N(\mathcal{P}_\Gamma) = N(\mathcal{P}_\Lambda)$.
The norm of M is the product of the norms of all localisations $N(M) = \prod_{\wp \trianglelefteq R} |\Lambda_\wp/\Lambda_\wp M|$.
The norm is multiplicative, i.e. $N({}_1M_2\ {}_2L_3) = N(M)N(L)$.
The norm of a principal ideal Λa is $N(\Lambda a) = |N_{A/\mathbb{Q}}(a)|$ where $N_{A/\mathbb{Q}}(a)$ is the regular norm of a in the $\mathbb{Q}$-algebra A.

Theorem 2.6.18. *Let A be a separable K-algebra over the number field K. Then there is some $C = C(A) \in \mathbb{R}_{>0}$ so that for any maximal order Λ in A and any left Λ-ideal M', there is some integral left Λ-ideal $M = M'a$ equivalent to M' such that $N(M) < C$.*

Proof. We view A as a $\mathbb{Q}$-algebra and show that $M'' =: (M')^{-1}$ contains an element $a \in M''$ such that $N_{A/\mathbb{Q}}(a) < CN(M'')$. Then $a\Lambda \subseteq M''$ and so $M'a =: M \subseteq \Lambda$ has norm $N(M) < C$.
(a) We first assume that A is a division algebra. Then we can argue as in the case of number fields:
Let M be a left ideal of the maximal order Λ and choose some $\mathbb{Z}$-basis $B := (b_1, \ldots, b_n)$ of Λ. The regular norm of an element $\sum_{i=1}^n x_i b_i$ is a homogeneous polynomial of degree $n = \dim_{\mathbb{Q}}(A)$ in the variables x_i. Let

$$C := \max\{|N_{A/\mathbb{Q}}(\sum_{i=1}^n x_i b_i)| \mid |x_i| \leq 1 \text{ for all } i\}.$$

Embed A into Euclidean space $V = \mathbb{R}^n$ by letting B be an orthonormal basis. Then Λ is a lattice in V of volumne 1 and M is a lattice of volumne $N(M)$ and determinant $N(M)^2$. The point set

$$X := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| \leq N(M)^{1/n} \text{ for all } i\}$$

is a cube of volumne $2^n N(M)$. By Minkowski's lattice point theorem there is some non-zero $a \in M$ such that $a = \sum_{i=1}^n a_i b_i$ with $(a_1, \ldots, a_n) \in X$. Then $N_{A/\mathbb{Q}}(a) \leq N(M)C$.

(b) If A is a simple algebra, $A = D^{n\times n}$ for some division algebra D, then not every non-zero element in A is a unit, so it is not enough to find a non-zero element in the lattice M that lies in the cube X. If Γ is a maximal order in D then $\Lambda := \Gamma^{n\times n}$ is a maximal order in A. Let M be a left Λ-ideal and let $a = (a_{ij}) \in M$. Since Λ contains the matrix units e_{ij}, the ideal Γa contains all elements b of which the rows are linear combinations of the rows of a and M is determined by all these rows. Let M_i be the submodule consisting of thoses rows in M of which the first $(i-1)$ coefficients are 0 and let

$$m_i := \{x_i \mid (0,\dots,0,x_i,x_{i+1},\dots,x_n) \in M_i\} \leq \Lambda.$$

Then m_i is a left ideal in Λ and

$$N(M) = N(m_1)^n N(m_2)^n \cdots N(m_n)^n.$$

By part (a) of the proof there are elements $a_i \in m_i$ such that $N_{D/\mathbb{Q}}(a_i) \leq C_D N(m_i)$. Then a_i is the first coefficient of some row $(0,\dots,0,a_i,a_{i,i+1},\dots,a_{i,n})$ and the matrix

$$a := \begin{pmatrix} a_1 & a_{11} & \dots & a_{1n} \\ 0 & a_2 & \dots & a_{2n} \\ \vdots & \ddots & \dots & \vdots \\ 0 & \dots & 0 & a_n \end{pmatrix} \in M$$

has norm

$$N_{A/\mathbb{Q}}(a) = \prod_{i=1}^{n} N_{D/\mathbb{Q}}(a_i)^n \leq C_D^{n^2} N(m_1)^n \cdots N(m_n)^n = (C_D)^{n^2} N(M).$$

(c) In the semisimple case, $A = \bigoplus_i A_i$, with simple components A_i, we can apply the argument above to all components A_i to obtain constants C_i and then put $C := \prod_i C_i$. □

Corollary 2.6.19. *The classnumber of a finite dimensional separable $\mathbb{Q}$-algebra A is finite.*

Proof. It is enough to show that a given maximal order Λ in A has only finitely many isomorphism classes of left ideals in A. This follows from the theorem and the fact that $\Lambda/\lceil C\rceil\Lambda$ is a finite additive group and therefore has only finitely many subgroups. □

Example. Let $\Lambda := \langle 1, \zeta_3, i, i\zeta_3\rangle \leq \left(\frac{-1,-3}{\mathbb{Q}}\right)$. Then $N(a_1 + a_2\zeta_3 + a_3 i + a_4 i\zeta_3) = a_1^2 + a_1a_2 + a_2^2 + a_3^2 + a_3a_4 + a_4^2$ so $C = 6^2 = 36$. For $p \neq 3$, the maximal left Λ-ideals $I_p^{(1)},\dots,I_p^{(p+1)}$ containing $p\Lambda$ are of index p^2, since $\Lambda/p\Lambda \cong \mathbb{Z}_p^{2\times 2}/p\mathbb{Z}_p^{2\times 2} \cong \mathbb{F}_p^{2\times 2}$. For $p = 3$ the ring $\Lambda/p\Lambda \cong \mathbb{F}_9[x]/(x^2)$ and again, the maximal ideal I_3 has index $p^2 = 9$. So we need to show that the maximal ideals over $2, 3, 5$ and the product $I_{(2)}^{(j)} I_3$ $(j = 1, 2, 3)$ are principal ideals. Since I_3 is 2-sided, the product is principal if the two factors are principal. Now

$$I_2^{(1)} = \Lambda(1+i), I_2^{(2)} = \Lambda(1+i)\zeta_3, I_2^{(3)} = \Lambda(1+i)\zeta_3^2, I_3 = \Lambda(1-\zeta_3).$$

Also the six maximal ideals containing 5 are principal ideals, hence $h(\Lambda) = H(\Lambda) = 1$ and $t(A) = 1$.

2.6.4 The Eichler condition.

Definition 2.6.20. *Let K be a number field. A central simple K-algebra A is called a* **totally definite quaternion algebra**, *if for all infinite places σ of K the completion A_σ is isomorphic to the real division algebra $\mathbf{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.*
The algebra A satisfies the **Eichler condition** *if A is not a totally definite quaternion algebra.*

So if A is a totally definite quaternion algebra then $\dim_K(A) = 4$ and K is a totally real field and $A = \left(\frac{a,b}{K}\right)$ with $a, b \in K$, $\sigma(a) < 0$ and $\sigma(b) < 0$ for all infinite places of K.

The main result of this subsection is the following theorem due to Eichler:

Theorem 2.6.21. *(***Eichler***) Let A be a central simple K-algebra that satisfies the Eichler condition. Let L be a normal ideal in A. Then L is a principal left-ideal, $L = O_l(L)a$, if and only if the* **reduced norm** *of L*

$$Nr(L) := \langle N(\ell) \mid \ell \in L \rangle_{R-ideal} \trianglelefteq R = \mathbb{Z}_K$$

is a principal ideal $Nr(L) = R\alpha$ for some $\alpha \in U(A)$.

Recall that

$$U(A) = \{a \in K \mid \sigma(a) > 0 \text{ for all real places } \sigma \text{ that ramify in } A\}$$

So the determination of the ideal classes in A is reduced to a computation in the center, where we need to find a so called **ray class group**,

$$\mathrm{Cl}_A(R) := I(R)/\{aR \mid a \in U(A)\}.$$

This is a task in commutative algebraic number theory and can be solved with essentially the same methods as the computation of the class group for algebraic number fields. The non-Eichler case will be treated in the next subsection. Note that the reduced norm is always a map

$$Nr : \mathcal{L}(\Lambda)/\sim \to \mathrm{Cl}_A(R)$$

since principal left-ideals are mapped to 1.

This theorem has a long proof, see Section 34 in Reiners book. The main idea is based on the very strong approximation theorem and the fact that there is always one infinite place for which the norm form is indefinite. Since the proof does not reveal too much insight and we are too short in time (the proof would require at least one full 90-minutes lecture) I will omit the proof here.

2.6.5 Stable equivalence of ideals.

Let Λ be a maximal R-order in the central simple K-algebra A, (K a number field and $R = \mathbb{Z}_K$).

Definition 2.6.22. *Two left Λ-lattices (Λ-modules that are R-lattices) X, Y are called* **stably isomorphic**, *if there is some $r \in \mathbb{N}$ such that $X \oplus \Lambda^r \cong Y \oplus \Lambda^r$. Let $[X]$ denote the stable isomorphism class of X. Then*

$$\mathrm{Cl}(\Lambda) := \{[X] \mid X \textit{ is a left } \Lambda - \textit{ideal in } A\}$$

denotes the **additive class group** *of Λ.*

It is clear that $X \cong Y \Rightarrow [X] = [Y] \in \mathrm{Cl}(\Lambda)$ so the additive class of an ideal consists of full isomorphism classes.

Theorem 2.6.23. *For any two left Λ ideals M, M' in A, there is some left Λ ideal M'' in A such that $M \oplus M' \cong \Lambda \oplus M''$. Define $[M] + [M'] := [M''] \in \mathrm{Cl}(\Lambda)$. This makes the set $\mathrm{Cl}(\Lambda)$ into an abelian group with identity element $[\Lambda]$.*

Proof. By the Chinese Remainder Theorem we may replace M and M' by isomorphic left ideals so that $M, M' \leq \Lambda$ and Λ/M and Λ/M' are coprime. So $\mathrm{Ann}_R(\Lambda/M) + \mathrm{Ann}_R(\Lambda/M') = R$. Let

$$\varphi : M \oplus M' \to \Lambda, \varphi(m, m') := m + m'.$$

Then φ is surjective and the kernel $M'' := \ker(\varphi)$ is a left Λ-ideal in A (to see this, tensor the ses

$$0 \to M'' \to M \oplus M' \to \Lambda \to 0$$

with K). Now Λ is a projective left Λ-module and hence the ses is split, so $M \oplus M' \cong \Lambda \oplus M''$. It is trivial to show that addition is independent from the choice of representatives M, M' in the stable isomorphism classes and is associative and commutative and that $[\Lambda]$ is the identity element.
Let us show the existence of inverse elements:
Any left Λ ideal M is projective and hence a direct summand of some free Λ-module, so there is some Λ-module Y such that

$$M \oplus Y = \Lambda^r \text{ for some } r \in \mathbb{N}.$$

Tensoring with K yields Y as a submodule of A^{r-1} and hence Y is isomorphic to some submodule of Λ^{r-1} of full rank. Hence (exercise) there are left ideals $M_1, \ldots, M_{r-1}$ such that $Y = M_1 \oplus \ldots \oplus M_{r-1}$. Repeating the argument from above ($M_1 \oplus M_2 \cong M'' \oplus \Lambda$) we obtain $Y \cong \Lambda^{r-2} \oplus N$ for some left ideal $N \leq \Lambda$. So $M \oplus N \oplus \Lambda^{r-2} \cong \Lambda^r$ and hence $[M] + [N] = [\Lambda]$. □

Remark 2.6.24. *By Exercise Number 17, the additive class group $\mathrm{Cl}(R)$ is isomorphic to the usual ideal class group of R.*

Corollary 2.6.25. *Let Λ be a maximal R-order in the separable K-algebra A and let X be a left Λ-lattice such that $KX \cong A^r$. Then there is some left Λ-ideal J in A such that $X \cong \Lambda^{r-1} \oplus J$.*

Proof. Follows by applying Theorem 2.6.23 successively. □

Corollary 2.6.26. *Let Λ be a maximal R-order in the separable K-algebra A. Then any maximal order Γ in $A^{r \times r}$ is conjugate to*

$$\Gamma \sim \begin{pmatrix} \Lambda & \ldots & \Lambda & J^{-1} \\ \vdots & \vdots & \vdots & \vdots \\ \Lambda & \ldots & \Lambda & J^{-1} \\ J & \ldots & J & \Lambda' \end{pmatrix}$$

for some left Λ-ideal J and $\Lambda' := O_r(J)$.

Proof. Let $V = A^r$. This is an A-$A^{r\times r}$-bimodule. Since Λ and Γ are R-orders there is a Λ-Γ-lattice X in V. As a Λ-module, X is isomorphic to $\Lambda^{r-1} \oplus J$. So there is some $a \in (A^{r\times r})^*$ such that $Xa = \Lambda^{r-1} \oplus J$ and $a^{-1}\Gamma a = \mathrm{End}_\Lambda(Xa)$ is a desired. □

Note that for $r \geq 2$ it is enough to choose J from a system of representatives of stable isomorphism classes of left Λ-ideals.

Some notation: Let K be a number field and A a central simple K-algebra. Let

$$U(A) = \{a \in K \mid \sigma(a) > 0 \text{ for all real places } \sigma \text{ that ramify in } A\}$$

and $\mathrm{Cl}_A(R) := I(R)/\{aR \mid a \in U(A)\}$ denote the associated **ray class group**. Then $\sigma : \mathrm{Cl}_A(R) \to \mathrm{Cl}(R)$, $[I] \mapsto [I]$ is an epimorphism whose kernel is an elementary abelian 2-group (exercise or later). Let Λ be a maximal R-order in A. Then the reduced norm $Nr(L)$ of any left Λ ideal L in A is

$$Nr(L) := \langle N(\ell) \mid \ell \in L\rangle_{R-ideal} \trianglelefteq R = \mathbb{Z}_K$$

The aim of the rest of this subsection is to prove the following theorem by Swan:

Theorem 2.6.27. *Let K be an algebraic number field. Then the reduced norm defines a group isomorphism*

$$\nu : \mathrm{Cl}(\Lambda) \to \mathrm{Cl}_A(R), \nu([L]) := [Nr(L)]$$

between the additive class group of Λ and the multiplicative ray class group of R.

For the proof we need to deal with matrix rings over A. So let $B := A^{r\times r} = \mathrm{End}_A(A^r)$. Then B and A have the same ramified prime ideals and hence $U(A) = U(B) \leq K^*$ and therefore $\mathrm{Cl}_A(R) = \mathrm{Cl}_B(R)$. If Λ is a maximal order in A, then $\Gamma := \Lambda^{r\times r} = \mathrm{End}_\Lambda(\Lambda^r)$ is a maximal order in B.

Lemma 2.6.28. *To each Λ-lattice $X \leq A^r$ there corresponds a Γ-lattice*

$$\varphi(X) := \mathrm{Hom}_\Lambda(\Lambda^r, X) \leq B.$$

If $X = J_1 \oplus \ldots \oplus J_r$ for left Λ ideals $J_i \leq A$, then $Nr(\varphi(X)) = \prod_{i=1}^r Nr(J_i)$.

Proof. We first remark that

$$\varphi : \Lambda - mod \to \Gamma - mod,\ X \mapsto \mathrm{Hom}_\Lambda(\Lambda^r, X)$$

is an equivalence of categories, since Λ^r is a progenerator for $\Lambda - mod$ with endomorphism ring Γ. Wlog we may assume that $X \leq \Lambda^r$ and all ideals J_i are contained in Λ. Then $\varphi(X) \cong X \oplus \ldots \oplus X$ is a left-ideal contained in Γ and for the regular norm

$$N_{B/K}(\varphi(X)) = \mathrm{ord}_R(\Gamma/\varphi(X)) = (\mathrm{ord}_R(\Lambda^r/X))^r = (\prod_{i=1}^r \mathrm{ord}_R(\Lambda/J_i))^r = (\prod_{i=1}^r N_{A/K}(J_i))^r$$

where $\mathrm{ord}_R(M) = \prod_{j=1}^s \wp_j$, if $M = M_0 > M_1 > \ldots > M_s = 0$ with R-composition factors $M_{j-1}/M_j \cong R/\wp_j$. If $[A : K] = n^2$ then $[B : K] = (rn)^2$ and $N_{A/K} = Nr^n$, $N_{B/K} = Nr^{rn}$ from which we obtain the formula for the reduced norms. □

Corollary 2.6.29. *Let $X = \bigoplus_{i=1}^{r} J_i$, $X' = \bigoplus_{i=1}^{r} J_i'$. Then*

(i) $X \cong X'$ as Λ-modules, if and only if $\varphi(X) \cong \varphi(X')$ as Γ-modules.

(ii) If $X \cong X'$ then $\prod_{i=1}^{r}[Nr(J_i)] = \prod_{i=1}^{r}[Nr(J_i')] \in \mathrm{Cl}_A(R)$.

(iii) If A satisfies the Eichler condition or $r \geq 2$, then $X \cong X'$ if and only if $\prod_{i=1}^{r}[Nr(J_i)] = \prod_{i=1}^{r}[Nr(J_i')] \in \mathrm{Cl}_A(R)$.

Proof. (i) follows from the fact that φ is a Morita equivalence.
(ii) is clear.
(iii) is Eichler's theorem 2.6.21 from the previous section, where one has to note that $A^{r\times r}$ always satisfies the Eichler condition, if $r \geq 2$. □

In particular if A satisfies the Eichler condition over R, then two left Λ ideals M, M' are isomorphic if and only if they are stably isomorphic. In general we always have that $A^{2\times 2}$ satisfies the Eichler condition. This allows us to conclude that two left Λ ideals M and M' are stably isomorphic if and only if $\Lambda \oplus M \cong \Lambda \oplus M'$.

We now conclude the proof of Theorem 2.6.27: Proof. The proof of the Lemma above shows that ν is well defined. If $J \oplus J' \cong \Lambda \oplus J''$ then $\nu(J)\nu(J') = \nu(J'')$, so ν is a group homomorphism. If $\nu(J) = \nu(\Lambda)$, then by the above $J \oplus \Lambda \cong \Lambda \oplus \Lambda$ and hence J is stably isomorphic to Λ, $[J] = 1$. So ν is injective.
To show the surjectivity of ν we need to find a preimage for all classes of non-zero prime ideals $\wp$ in R. Given such a prime ideal $\wp$, there is a maximal left Λ-ideal P, such that $\wp\Lambda < P < \Lambda$. But then the reduced norm $Nr(P) = \wp$. □

2.6.6 Algorithmic determination of classes and types

This section deals with totally definite quaternion algebras over totally real number fields and is taken from my paper "Finite quaternionic matrix groups", in which I classified all maximal finite sugroups of $\mathrm{GL}_n(D)$ for definite quaternion algebras such that $[D : \mathbb{Q}]n \leq 40$. My main tools to deal with definite quaternion algebras are lattices. I had programs to list short vectors in an integral lattice and to compute isomteries of lattices and their automorphism group (Plesken/Souvignier-algorithm).

So let $\mathcal{D}$ be a totally definite quaternion algebra with center K, a totally real number field, $[K : \mathbb{Q}] = d$. Then we may find one maximal order Λ using the radical idealiser process to obtain a hereditary order and then enlarging this order by adding suitable integral elements. Then we can find enough classes of Λ left ideals, by listing integral ideals of small norm. To check completeness we use the well known mass formulas developed by M. Eichler.

Theorem 2.6.30. *(Eichler's Massformula, without proof) Let h be the class number of K, $K = Z(\mathcal{D})$, $[K : \mathbb{Q}] = d$, $R = \mathbb{Z}_K$ $\mathcal{D}$ a totally definite quaternion algebra. Let D the discriminant of $\mathcal{D}$ over K and Λ any maximal order in $\mathcal{D}$. Let $(I_i)_{1\leq i\leq s}$ be a system of representatives of left ideal classes of Λ, $\Lambda_i := \{x \in \mathcal{D} \mid I_i x \subseteq I_i\}$ the right order of I_i and*

$\omega_i := [\Lambda_i^* : R^*]$ the index of the unit group of R in the unit group of Λ_i. Then one has:

$$\sum_{i=1}^{s} \omega_i^{-1} = 2^{1-d} \cdot |\zeta_K(-1)| \cdot h \cdot \prod_{\wp | D} (N_{K/\mathbb{Q}}(\wp) - 1)$$

where the product is taken over all primes $\wp$ of R dividing the discriminant D of $\mathcal{D}$.

A proof is for instance given in Vignéras' lecture notes.

If Λ_i and Λ_j are conjugate in $\mathcal{D}$, one may choose a new representative for the class of I_j to achieve that $\Lambda_i = \Lambda_j$. Then $I_i^{-1} I_j$ is a 2-sided Λ_i-ideal. Moreover the Λ-left ideals I_i and I_j are equivalent, if and only if $I_i^{-1} I_j$ is principal.

So if one reorders the Λ_i such that the first t orders $\Lambda_1, \ldots, \Lambda_t$ form a system of representatives of conjugacy classes of maximal orders in $\mathcal{D}$ and H_i the number of isomorphism classes of 2-sided ideals of Λ_i $(1 \leq i \leq t)$, then

$$\sum_{i=1}^{s} \omega_i^{-1} = \sum_{i=1}^{t} \omega_i^{-1} H_i.$$

Definition 2.6.31. *Let $\Lambda_1, \ldots, \Lambda_t$ form a system of representatives of conjugacy classes of maximal orders in $\mathcal{D}$. Let $^- : \mathcal{D} \to \mathcal{D}$ denote the quaternionic conjugation, $\overline{x} := \mathrm{trace}_{red}(x) - x$, where trace_{red} is the reduced trace. Then $\mathrm{trace}_{red}(\Lambda_i) \subseteq R$ and hence $\overline{\Lambda_i} = \Lambda_i$ for all i.*

(a) $\omega_i := [\Lambda_i^* : R^*]$ is the index of the unit groups. (we will see below that ω_i is finite.

(b) $\omega_i^1 := \frac{1}{2} |\{x \in \Lambda_i \mid x\overline{x} = 1\}|$ denotes the index of ± 1 in the group of units in Λ_i of norm 1.

(c) Let $N : \mathcal{D} \to K$, $N(x) := x\overline{x}$ and $\omega_i^{ns} := N(\Lambda_i^*)/(R^*)^2$. Then $\omega_i = \omega_i^1 \cdot \omega_i^{ns}$.

The algorithmic problems in evaluating these formulas are:
a) determine the ideals I_j.
b) decide whether two maximal orders are conjugate in $\mathcal{D}$.
c) determine the length of the orbit of Λ under the Galois group $Gal(K/\mathbb{Q})$.
d) determine $\omega_i^{-1} H_i$.

Problem a) is the major difficulty here. There is of course the well known geometric approach to this question using the Minkowski bound on the norm of a representative of the ideal classes. From the arithmetic point of view one may apply two different strategies to find the ideals I_j:
There is a coarser equivalence relation than conjugacy namely the stable isomorphism cf. Reiner (35.5). The theorem of Eichler (see Reiner (34.9)) says that the reduced norm is an isomorphism of the group of stable isomorphism classes of Λ-left ideals onto the narrow class group of the center K. This gives estimates for the norms of the ideals I_j.
A second arithmetic strategy is to look for (commutative, non full) suborders $\mathcal{O}$ of $\mathcal{D}$. The number of the maximal orders Λ_i containing $\mathcal{O}$ as a pure submodule can be calculated using the formula (5.12) from Vignéras.

Theorem 2.6.32. *Let Λ we a maximal order in $\mathcal{D}$ and $I_1, \ldots, I_s$ represent the isomorphism classes of left Λ-ideals in $\mathcal{D}$. Let $\Lambda_i := O_r(I_i)$ denote the right order of I_i. Let $B = \mathbb{Z}_L$ with $[L : K] = 2$, L a maximal subfield of $\mathcal{D}$ and let*

$$m_i(B) := |\{\varphi : B \hookrightarrow \Lambda_i\}/\Lambda_i^*|.$$

For a prime ideal $\wp \trianglelefteq \mathbb{Z}_K$ that divides the discriminant D of $\mathcal{D}$ let $\left(\frac{B}{\wp}\right) = -1$ if $\wp$ is inert in $\mathbb{Z}_L/\mathbb{Z}_K$ and $\left(\frac{B}{\wp}\right) = 0$ if $\wp$ is ramified in $\mathbb{Z}_L/\mathbb{Z}_K$. Then

$$\sum_{i=1}^{s} m_i(B) = h(B) \prod_{\wp | D} (1 - \left(\frac{B}{\wp}\right)$$

where $h(B)$ is the class number of B.

Examples:

$\mathcal{D} = \mathcal{Q}_{\infty,2}$ Here $K = \mathbb{Q}$ and there is a unique maximal order Λ up to conjugacy in $\mathcal{D}$:

$$\Lambda = \langle 1, i, j, \frac{1 + i + j + ij}{2} \mid i^2 = j^2 = -1, ij = -ji = k \rangle.$$

Λ is euclidean and the unit group is $\Lambda^* = \mathrm{SL}_2(3)$ hence $\omega = \frac{24}{2} = 12$. Evaluating the mass formula gives us $\zeta_{\mathbb{Q}}(-1) = \zeta(-1) = \frac{1}{12}$.

$\mathcal{D} = \mathcal{Q}_{\infty,11}$ Now the mass formula is

$$\frac{1}{12}(11 - 1) = \frac{5}{6} = \frac{1}{2} + \frac{1}{3}$$

We claim that there are maximal orders Λ_1 and Λ_2 with $\Lambda_1^* \cong C_4$ and $\Lambda_2^* \cong C_6$. Then these orders are not isomorphic and hence not conjugate and provide a system of representatives of conjugacy classes of maximal orders in $\mathcal{D}$. The Λ_1-left ideals are represented by Λ_1 and $\Lambda_1\Lambda_2$.
The first observation is that the imaginary quadratic number fields $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{-3}]$ both are maximal subfields of $\mathcal{D}$ (compare local invariants, in both fields 11 is inert). So there is a maximal order Λ_1 containing an element i of order 4 and some maximal order Λ_2 containing an element w of order 6. Since i and w both generate maximal subfields of $\mathcal{D}$, the centralizer

$$C_1 := C_{\Lambda_1^*}(i) = \mathbb{Z}[i]^* = \langle i \rangle \text{ and } C_2 := C_{\Lambda_2^*}(w) = \mathbb{Z}[w]^* = \langle w \rangle.$$

If $\Lambda_1^* \neq C_1$ then there would be an additional element $a \in \Lambda_1^*$ such that $\langle i, a \rangle_{\mathbb{Q}-algebra} = \mathcal{D}$. The group $G := \langle i, a \rangle$ is a finite subgroup of $\mathcal{D}^* \leq \mathrm{GL}_4(\mathbb{Q})$ and its $\mathbb{Z}$-span is some order Λ in $\mathcal{D}$. But the discriminant of Λ is a divisor of $|G|^4$. Since $disc(\Lambda_1) = 11^2$, we hence obtain that $11 \mid |G|$ which is a contradiction since $\varphi(11) = 10 > 4$. Similarly $\Lambda_2^* = \langle w \rangle$.

$\mathcal{D} = \mathcal{Q}_{\sqrt{3},\infty,\infty}$ Here $\mathcal{D} = \mathbb{Q}[\sqrt{3}] \otimes \mathcal{Q}_{\infty,2} == \mathbb{Q}[\sqrt{3}] \otimes \mathcal{Q}_{\infty,3}$ and one obtains maximal orders Λ_1 and Λ_2 with

$$G_1 := \mathrm{SL}_2(3) \leq \Lambda_1^* \text{ and } G_2 := C_{12}.C_2 \leq \Lambda_2^*.$$

One may also show that these groups of order 24 are maximal finite subgroups of Λ_1^* and Λ_2^*. But the mass formula says that

$$[\Lambda_1^* : \mathbb{Z}[\sqrt{3}]^*]^{-1} + [\Lambda_2^* : \mathbb{Z}[\sqrt{3}]^*]^{-1} = \frac{1}{12}.$$

What is wrong here? The answer is that $\Lambda_i^* \neq \mathbb{Z}[\sqrt{3}]^* \times G$ for some (finite) sugroup G, but both unit groups are non-split extensions. For $i = 1$ and 2 there are elements $g_i \in N_{\Lambda_i^*}(G_i)$ such that $g_i^2 = 2 + \sqrt{3} = u$, the fundamental unit in $\mathbb{Z}[\sqrt{3}]$. Note that u is a totally positive element, so may be a norm of some element in Λ_i, but u is not a square in $\mathbb{Z}[\sqrt{3}]^*$.

$\mathcal{D} := \mathcal{Q}_{\sqrt{3}+\sqrt{5},\infty}$ Then the narrow class group of $K = \mathbb{Q}[\sqrt{3} + \sqrt{5}]$ has order 2 and is generated by a prime ideal dividing 11. So there are 2 stable isomorphism classes of Λ-ideals one containing the ideal classes of I_1, I_2, and I_3, the other one the one of I_4. The second strategy applied to $\mathcal{O} = \mathbb{Z}[\zeta_5, \sqrt{3}]$ gives that there are 2 orders Λ_i containing a fifth root of unity, because the class number of $\mathcal{O}$ is 2 (and again a prime ideal dividing 11 generates the class group).

The problems b), c), and d) can be dealt with using the normform of $\mathcal{D}$:

Let $\mathcal{D}$ be a definite quaternion algebra over K and N be its reduced norm which is a quadratic form with associated bilinear form $\langle x, y\rangle = tr(x\overline{y})$ where tr is the reduced trace and $^-$ the canonical involution of $\mathcal{D}$. The special orthogonal group

$$SO(\mathcal{D}, N) := \{\varphi : \mathcal{D} \to \mathcal{D} \mid N(\varphi(x)) = N(x) \text{ for all } x \in \mathcal{D}, det(\varphi) = 1\}$$

is the group of all proper isometries of $\mathcal{D}$ with respect to the quadratic form N.

Theorem 2.6.33. *With the notation above one has*

$$SO(\mathcal{D}, N) = \{x \mapsto a_1 x a_2^{-1} \mid a_i \in \mathcal{D}^*, N(a_1) = N(a_2)\}$$

is induced by left multiplication with elements of $\mathcal{D}$ of norm 1 and conjugation with elements of $\mathcal{D}^*$.

Proof. Clearly the mapping $x \mapsto a_1 x a_2^{-1}$ with $a_i \in \mathcal{D}^*$ and $N(a_1) = N(a_2)$ is a proper isometry of the K-vector space $(\mathcal{D}, N)$.

To see the converse inclusion let $\mathcal{D} = \langle 1, i, j, ij = k = -ji\rangle_K$ with $i^2 = a$ and $j^2 = b$ and $\varphi : \mathcal{D} \to \mathcal{D}$ be an isometry of determinant 1 with respect to N. Then $N(\varphi(1)) = 1$ and after left multiplication by $\varphi(1)^{-1}$ we may assume that $\varphi(1) = 1$. Let $b_2 := \varphi(i)$, $b_3 := \varphi(j)$, and $b_4 := \varphi(k)$. Then $tr(b_i 1) = 0$ and hence $\overline{b_i} = -b_i$ for all $i = 2, 3, 4$, and $b_2^2 = a$, $b_3^2 = b$, $b_4^2 = -ab$. Moreover $tr(b_i b_j^*) = 0 = -tr(b_i b_j)$ and hence $b_i b_j = -b_j b_i$ for all $2 \leq i \neq j \leq 4$. Thus $(b_2 b_3) b_4 = b_4 (b_2 b_3)$ and therefore $b_4 \in K b_2 b_3$ is an element of trace 0 in the field generated by $b_2 b_3$. Since $b_4^2 = (b_2 b_3)^2$, this implies that $b_4 = \pm b_2 b_3$. If $b_4 = b_2 b_3$, then φ is an K-algebra automorphism of $\mathcal{D}$ and hence induced by conjugation with an element of $\mathcal{D}^*$ and we are done. In this case φ is of determinant 1. Hence if $b_4 = -b_2 b_3$, the mapping φ has determinant -1, which is a contradiction. □

Corollary 2.6.34. *Let Λ_i $(i = 1, 2)$ be two orders in $\mathcal{D}$. Then Λ_1 is conjugate to Λ_2 if and only if the lattices (Λ_1, N) and (Λ_2, N) are properly isometric.*

Proof. Clearly if the two orders are conjugate the lattices are properly isometric, so we show the converse: let $\varphi : \Lambda_1 \to \Lambda_2$ be a proper isometry with respect to N. By the Proposition there are elements $a_1, a_2 \in \mathcal{D}^*$ with $N(a_1) = N(a_2)$ such that $a_1\Lambda_1 a_2^{-1} = \Lambda_2$. Since $1 \in \Lambda_1$ this implies that $a_1 a_2^{-1}$ is an element of norm 1 in Λ_2 and hence $\Lambda_2 = a_1 a_2^{-1} a_2 \Lambda_1 a_2^{-1} = a_2 \Lambda_1 a_2^{-1}$ is conjugate to Λ_1. □

Since $^-$ is the identity on the subspace K and the negative identity on the 3-dimensional subspace $1^\perp$ consisting of the elements of $\mathcal{D}$ with trace 0, one easily sees that $^-$ is an improper isometry (of determinant -1) of $(\mathcal{D}, N)$. Thus, if one of the orders Λ_1 or Λ_2 is stable under $^-$, one may omit the word "properly" in the Corollary above. Note that this holds particularly for maximal orders.

Corollary 2.6.35. *Let Λ be an order in $\mathcal{D}$. The group of proper isometries of the lattice (Λ, N) is induced by the transformations of the form $b \mapsto axbx^{-1}$, where $a \in \Lambda$ is an element of norm 1 and $x \in N_{\mathcal{D}^*}(\Lambda)$ normalizes Λ.*

Normalizer and 2-sided ideals.

Remark 2.6.36. *Let $a \in N_{\mathcal{D}^*}(\Lambda)$. Then $a\Lambda a^{-1} = \Lambda$ and hence Λa is a principal 2-sided ideal. Two elements $a, b \in N_{\mathcal{D}^*}(\Lambda)$ induce the same automorphism by conjugation, if and only if $ab^{-1} = c \in K^*$. This means that the quotient $(\Lambda a)(\Lambda b)^{-1} = \Lambda c \in I(\Lambda)$ is a central principal ideal.*

Remark 2.6.37. *Assume that R is a principal ideal domain and let $\wp_1, \ldots, \wp_s$ be the prime ideals of R that ramify in Λ and let $\kappa : N_{\mathcal{D}^*}(\Lambda_i) \to \mathrm{Aut}(\Lambda_i), a \mapsto (x \mapsto axa^{-1})$. Then $|\kappa(N_{\mathcal{D}^*}(\Lambda_i))| = \omega_i 2^s H_i^{-1}$. Therefore the order of the isometry group*

$$|\,\mathrm{Aut}(\Lambda_i, N)| = \underbrace{\omega_i^1}_{left\ mult.} \underbrace{\omega_i 2^s H_i^{-1}}_{\kappa(normalizer)} \cdot \underbrace{2}_{-1} \cdot \underbrace{2}_{quat.conj.} .$$

where s is the number of finite primes of K that ramify in $\mathcal{D}$. Now $2\omega_i^1$ is simply the number of shortest vectors of the lattice (Λ_i, N) and can easily be calculated. Hence $\omega_i^{-1} H_i = |Aut(\Lambda_i, N)|^{-1} 2^{s+2} \omega_i^1$ can be obtained using automorphism groups and short vectors of lattices to evaluate the mass formula.

If the quaternion algebra $\mathcal{D}$ has the additional property that if a prime ideal $\wp \trianglelefteq R$ ramifies in $\mathcal{D}$ then all prime ideals that contain $\wp \cap \mathbb{Z}$ also ramify in $\mathcal{D}$, then the Galois group $Gal(K/\mathbb{Q})$ acts on $\mathcal{D}$ (note that this is the case for endomorphism rings of modules of finite groups, they have **uniformily distributed invariants**):

Choose a K-basis $(1 =: b_1, b_2, b_3, b_4)$ of $\mathcal{D}$. An element $\sigma \in Gal(K/\mathbb{Q})$ defines an automorphism σ of the $\mathbb{Q}$-algebra $\mathcal{D}$ by $\sigma(\sum a_i b_i) := \sum \sigma(a_i) b_i$. By the Theorem of Skolem and Noether the class $\sigma Inn(\mathcal{D})$ of the automorphism σ does not depend on the chosen basis. Therefore one gets a well defined action of $Gal(K/\mathbb{Q})$ on the set of conjugacy classes of maximal orders in $\mathcal{D}$. This action preserves ω_i and H_i.

If n_i denotes the length of the orbits of the class of $\mathcal{M}_i$ under $Gal(K/\mathbb{Q})$ one gets the following table:

d	$\mathcal{D}$	$\sum n_i(\omega_i^1 \cdot \omega_i^{ns})^{-1} \cdot H_i$
1	$\mathcal{Q}_{\infty,2}$	12^{-1}
	$\mathcal{Q}_{\infty,3}$	6^{-1}
	$\mathcal{Q}_{\infty,5}$	3^{-1}
	$\mathcal{Q}_{\infty,2,3,5}$	$3^{-1}+3^{-1}$
	$\mathcal{Q}_{\infty,7}$	2^{-1}
	$\mathcal{Q}_{\infty,11}$	$2^{-1}+3^{-1}$
	$\mathcal{Q}_{\infty,13}$	1
	$\mathcal{Q}_{\infty,17}$	$1+3^{-1}$
	$\mathcal{Q}_{\infty,19}$	$1+2^{-1}$
2	$\mathcal{Q}_{\sqrt{2},\infty}$	24^{-1}
	$\mathcal{Q}_{\sqrt{2},\infty,2,3}$	1
	$\mathcal{Q}_{\sqrt{2},\infty,2,5}$	3^{-1}
	$\mathcal{Q}_{\sqrt{3},\infty}$	$(12\cdot 2)^{-1}+(12\cdot 2)^{-1}$
	$\mathcal{Q}_{\sqrt{5},\infty}$	60^{-1}
	$\mathcal{Q}_{\sqrt{5},\infty,2,3}$	$5^{-1}\cdot 2$
	$\mathcal{Q}_{\sqrt{5},\infty,2,5}$	5^{-1}
	$\mathcal{Q}_{\sqrt{5},\infty,5,3}$	$5^{-1}+3^{-1}$
	$\mathcal{Q}_{\sqrt{6},\infty}$	$(12\cdot 2)^{-1}+(6\cdot 2)^{-1}+(4\cdot 2)^{-1}$
	$\mathcal{Q}_{\sqrt{7},\infty}$	$(4\cdot 2)^{-1}+(3\cdot 2)^{-1}+(12\cdot 2)^{-1}$
	$\mathcal{Q}_{\sqrt{10},\infty}$	$3^{-1}+2^{-1}+12^{-1}+4^{-1}$
	$\mathcal{Q}_{\sqrt{11},\infty}$	$12^{-1}+2^{-1}$
	$\mathcal{Q}_{\sqrt{13},\infty}$	12^{-1}
	$\mathcal{Q}_{\sqrt{15},\infty}$	$3^{-1}+(1\cdot 2)^{-1}+(2\cdot 2)^{-1}+6^{-1}+(3\cdot 2)^{-1}+2^{-1}+12^{-1}+(2\cdot 2)^{-1}$
	$\mathcal{Q}_{\sqrt{17},\infty}$	6^{-1}
	$\mathcal{Q}_{\sqrt{21},\infty}$	$12^{-1}+6^{-1}$
	$\mathcal{Q}_{\sqrt{33},\infty}$	$6^{-1}+3^{-1}$
3	$\mathcal{Q}_{\theta_7,\infty,7}$	14^{-1}
	$\mathcal{Q}_{\theta_7,\infty,2}$	12^{-1}
	$\mathcal{Q}_{\theta_7,\infty,3}$	$6^{-1}+7^{-1}$
	$\mathcal{Q}_{\theta_9,\infty,3}$	18^{-1}
	$\mathcal{Q}_{\theta_9,\infty,2}$	$12^{-1}+9^{-1}$
	$\mathcal{Q}_{\omega_{13},\infty,13}$	1
	$\mathcal{Q}_{\omega_{19},\infty,19}$	$2^{-1}+1+3\cdot 1$

d	$\mathcal{D}$	$\sum n_i(\omega_i^1 \cdot \omega_i^{ns})^{-1} \cdot H_i$
4	$\mathcal{Q}_{\theta_{15},\infty}$	$(30\cdot 2)^{-1} + 60^{-1}$
	$\mathcal{Q}_{\theta_{16},\infty}$	$16^{-1} + 24^{-1}$
	$\mathcal{Q}_{\theta_{20},\infty}$	$(20\cdot 2)^{-1} + (12\cdot 2)^{-1} + 60^{-1}$
	$\mathcal{Q}_{\theta_{24},\infty}$	$(24\cdot 2)^{-1} + (8\cdot 2)^{-1} + 24^{-1}$
	$\mathcal{Q}_{\eta_{17},\infty}$	$6^{-1} + 2\cdot 12^{-1}$
	$\mathcal{Q}_{\sqrt{2}+\sqrt{5},\infty}$	$24^{-1} + 60^{-1}$
	$\mathcal{Q}_{\sqrt{2}+\sqrt{5},\infty,2,5}$	$5^{-1} + 2\cdot 1\cdot 2$
	$\mathcal{Q}_{\eta_{40},\infty}$	$(10\cdot 2)^{-1} + 60^{-1} + 5^{-1} + (2\cdot 2)^{-1} + (12\cdot 2)^{-1} + (4\cdot 2)^{-1}$
	$\mathcal{Q}_{\sqrt{3}+\sqrt{5},\infty}$	$60^{-1} + (12\cdot 2)^{-1} + (12\cdot 2)^{-1} + (5\cdot 2)^{-1}$
	$\mathcal{Q}_{\eta_{48},\infty}$	$(6\cdot 2)^{-1} + (2\cdot 2)^{-1} + 2\cdot 3^{-1} + 24^{-1}$
		$+(8\cdot 2)^{-1} + 2\cdot(1\cdot 2)^{-1} + (4\cdot 2)^{-1} + (1\cdot 2)^{-1} + (8\cdot 2)^{-1} + (2\cdot 2)^{-1}$
5	$\mathcal{Q}_{\theta_{11},\infty,11}$	$22^{-1} + 3^{-1}$
	$\mathcal{Q}_{\theta_{11},\infty,2}$	$12^{-1} + 1^{-1} + 11^{-1}$
	$\mathcal{Q}_{\theta_{11},\infty,3}$	$6^{-1} + 1^{-1}\cdot 2 + 5\cdot 1^{-1} + 1^{-1}\cdot 2$
	$\mathcal{Q}_{\sigma_{25},\infty,5}$	$3^{-1} + 5\cdot 3^{-1}\cdot 2 + 5\cdot 1^{-1}\cdot 2 + 5\cdot 1^{-1} + 5\cdot 1^{-1}$

In the first column the degree $d := [K : \mathbb{Q}]$ is given, in the second one the name of the quaternion algebra $\mathcal{D}$ by giving the rational places that ramify in $\mathcal{D}$. The third column contains the relevant dimensions n and in the last column, the mass formula of $\mathcal{D}$ is expanded. Here the sum is taken over a system of representatives of the orbits of $Gal(K/\mathbb{Q})$ on the conjugacy classes of maximal orders in $\mathcal{D}$.

For the algebraic numbers the following notation is used:

Notation. As usual ζ_m denotes a primitive m-th root of unity in $\mathbb{C}$ and $\sqrt{m}$ a square root of m. Moreover $\theta_m := \zeta_m + \zeta_m^{-1}$ denotes a generator of the maximal totally real subfield of the m-th cyclotomic field. ω_m (resp. η_m, σ_m) denote generators of a subfield K of $\mathbb{Q}[\zeta_m]$ with $Gal(K/\mathbb{Q}) \cong C_3$ (resp. C_4, C_5).

$\mathcal{Q}_{\infty,2} = \langle 1, i, j, \omega = \frac{1+i+j+ij}{2} \rangle_{\mathbb{Q}}$, where $i^2 = j^2 = (ij)^2 = -1$, and the maximal order is
$\langle 1, , i, j, \omega \rangle_{\mathbb{Z}}$,

$\mathcal{Q}_{\infty,3} = \langle 1, \omega, i, \omega i \rangle_{\mathbb{Q}} \cong \mathbb{Q}[\omega] \oplus \mathbb{Q}[\omega]i$, where $\omega^2 + \omega + 1 = 0$, $i^2 = -1$, $\omega^i = \omega^{-1}$ and the maximal order is
$\langle 1, \omega, i, \omega i \rangle_{\mathbb{Z}}$,

$\mathcal{Q}_{\infty,5} = \langle 1, i, j, ij \rangle_{\mathbb{Q}}$, where $i^2 = -2,\ j^2 = -5,\ (ij)^2 = -10$, and the maximal order is
$\langle 1, \omega := \frac{2+i-ij}{4}, \rho := \frac{1+i+j}{2}, ij \rangle_{\mathbb{Z}}$
$\mathcal{Q}_{\infty,7} = \langle 1, \rho, i, \rho i \rangle_{\mathbb{Q}} \cong \mathbb{Q}[\rho] \oplus \mathbb{Q}[\rho]i$, where $\rho^2 - \rho + 2 = 0$, $i^2 = -1$, $(i\rho)^2 = -2$ and the maximal order is
$\langle 1, \rho, i, \rho i \rangle_{\mathbb{Z}}$,

$\mathcal{Q}_{\infty,11} = \langle 1, \rho, i, \rho i \rangle_{\mathbb{Q}} \cong \mathbb{Q}[\rho] \oplus \mathbb{Q}[\rho]i$, where $\rho^2 + \rho + 3 = 0$, $i^2 = -1$, $(i\rho)^2 = -3$ and representatives for the two conjugacy classes of maximal orders are
$\mathcal{O}_1 := \langle 1, \rho, i, \rho i \rangle_{\mathbb{Z}}$ (with unit group C_4) and
$\mathcal{O}_2 := \langle 1, \rho + i, 2i, \frac{1+\rho i}{2} \rangle_{\mathbb{Z}}$ (with unit group C_6).

$\mathcal{Q}_{\sqrt{2},\infty,\infty} = \langle 1, \zeta_8, \alpha, \zeta_8\alpha \rangle_{\mathbb{Q}[\sqrt{2}]} \cong \mathbb{Q}[\zeta_8] \oplus \mathbb{Q}[\zeta_8]\alpha$, where $\zeta_8^2 - \sqrt{2}\zeta_8 + 1 = 0$, $\alpha^2 = -1$, and $\alpha^{-1}\zeta_8\alpha = \zeta_8^{-1}$ and the maximal order is
$\langle 1, \zeta_8, \frac{1+\alpha}{\sqrt{2}}, \zeta_8\frac{1+\alpha}{\sqrt{2}} \rangle_{\mathbb{Z}[\sqrt{2}]}$.

$\mathcal{Q}_{\sqrt{3},\infty,\infty} = \langle 1, \zeta_{12}, \alpha, \zeta_{12}\alpha \rangle_{\mathbb{Q}[\sqrt{3}]} \cong \mathbb{Q}[\zeta_{12}] \oplus \mathbb{Q}[\zeta_{12}]\alpha$, where $\zeta_{12}^2 - \sqrt{3}\zeta_{12} + 1 = 0$, $\alpha^2 = -1$, and $\alpha^{-1}\zeta_{12}\alpha = \zeta_{12}^{-1}$ and representatives for the two conjugacy classes of maximal orders are
$\mathcal{O}_1 := \langle 1, \zeta_{12}, \alpha, \zeta_{12}\alpha \rangle_{\mathbb{Z}[\sqrt{3}]}$ (where the torsion subgroup of the unit group is $C_{12}.C_2$) and
$\mathcal{O}_2 := \langle 1, \frac{(1+i)(1+\sqrt{3})}{2}, \frac{(1+j)(1+\sqrt{3})}{2}, \frac{1+i+j+ij}{2} \rangle_{\mathbb{Z}[\sqrt{3}]}$, where $i := \zeta_{12}^3$ and $j := \alpha$ (where the torsion subgroup of the unit group is $SL_2(3)$).

$\mathcal{Q}_{\sqrt{5},\infty,\infty} = \langle 1, \zeta_5, \alpha, \zeta_5\alpha \rangle_{\mathbb{Q}[\sqrt{5}]} \cong \mathbb{Q}[\zeta_5] \oplus \mathbb{Q}[\zeta_5]\alpha$, where with $b_5 := \frac{-1+\sqrt{5}}{2}$ it holds that $\zeta_5^2 - b_5\zeta_5 + 1 = 0$, $\alpha^2 = -1$, and $\alpha^{-1}\zeta_5\alpha = \zeta_5^{-1}$ and the maximal order is
$\langle 1, \frac{(1-\zeta_5)(1+\alpha b_5)}{\sqrt{5}}, \alpha, \zeta_5\alpha \rangle_{\mathbb{Z}[b_5]}$.

$\mathcal{Q}_{\sqrt{5},\infty,\infty,2,\sqrt{5}} = \langle 1, \zeta_5, \alpha, \zeta_5\alpha \rangle_{\mathbb{Q}[\sqrt{5}]} \cong \mathbb{Q}[\zeta_5] \oplus \mathbb{Q}[\zeta_5]\alpha$, where with $b_5 := \frac{-1+\sqrt{5}}{2}$ it holds that $\zeta_5^2 - b_5\zeta_5 + 1 = 0$, $\alpha^2 = -2$, and $\alpha^{-1}\zeta_5\alpha = \zeta_5^{-1}$ and the maximal order is
$\langle 1, \zeta_5, \alpha, \zeta_5\alpha \rangle_{\mathbb{Z}[b_5]}$.

$\mathcal{Q}_{\sqrt{5},\infty,\infty,3,\sqrt{5}} = \langle 1, \zeta_5, \alpha, \zeta_5\alpha \rangle_{\mathbb{Q}[\sqrt{5}]} \cong \mathbb{Q}[\zeta_5] \oplus \mathbb{Q}[\zeta_5]\alpha$, where with $b_5 := \frac{-1+\sqrt{5}}{2}$ it holds that $\zeta_5^2 - b_5\zeta_5 + 1 = 0$, $\alpha^2 = -3$, and $\alpha^{-1}\zeta_5\alpha = \zeta_5^{-1}$ and representatives for the two conjugacy classes of maximal orders are
$\mathcal{O}_1 := \langle 1, \zeta_5, \alpha, \zeta_5\alpha \rangle_{\mathbb{Z}[b_5]}$ (where the torsion subgroup of the unit group is $\cong C_{10}$) and
$\mathcal{O}_2 := \langle 1, \frac{1+\alpha}{2}, 2\zeta_5, \zeta_5(1+\alpha) rangle_{\mathbb{Z}[b_5]}$ (where the torsion subgroup of the unit group is $\cong C_6$).

$\mathcal{Q}_{\sqrt{6},\infty,\infty} = \langle 1, i, j, \omega := \frac{1+i+j+ij}{2} \rangle_{\mathbb{Q}[\sqrt{6}]}$, where $i^2 = j^2 = (ij)^2 = -1$ and representatives for the three conjugacy classes of maximal orders are

$\mathcal{O}_1 := \langle 1, \frac{2+\sqrt{6}}{2}(1+i), \frac{2+\sqrt{6}}{2}(1+j), \frac{1+i+j+ij}{2}\alpha \rangle_{\mathbb{Z}[\sqrt{6}]}$ (where the torsion subgroup of the unit group is $SL_2(3)$),

$\mathcal{O}_2 := \langle 1, \frac{3+\sqrt{6}}{3}(1+\omega) =: a, \frac{2+\sqrt{6}}{2}(j-i) =: b, ab \rangle_{\mathbb{Z}[\sqrt{6}]}$, where $\omega^b = \omega^{-1}$ (where the torsion subgroup of the unit group is $\tilde{S}_3$). and

$\mathcal{O}_3 := \langle 1, \frac{2+\sqrt{6}}{2}(1+i) =: a, \frac{j+ij+\sqrt{6}}{2} =: b, ab \rangle_{\mathbb{Z}[\sqrt{6}]}$ (where the torsion subgroup of the unit group is Q_8).

$\mathcal{Q}_{\sqrt{7},\infty,\infty} = \langle 1, i, j, ij \rangle_{\mathbb{Q}[\sqrt{7}]}$, where $i^2 = j^2 = (ij)^2 = -1$ and representatives for the three conjugacy classes of maximal orders are

$\mathcal{O}_1 := \langle 1, i, \frac{j+\sqrt{7}i}{2}, \frac{ij+\sqrt{7}}{2} \rangle_{\mathbb{Z}[\sqrt{7}]}$ (where the torsion subgroup of the unit group is Q_8),

$\mathcal{O}_2 := \langle 1, \frac{j+\sqrt{7}i}{2}, i + \frac{ij+\sqrt{7}}{2}, \frac{2+\sqrt{7}}{3}(1 + (1-\sqrt{7})i - \frac{j+\sqrt{7}i}{2} - \frac{ij+\sqrt{7}}{2}) \rangle_{\mathbb{Z}[\sqrt{7}]}$ (where the torsion subgroup of the unit group is C_3),

$\mathcal{O}_3 := \langle 1, \frac{3+\sqrt{7}}{2}(1+i), \frac{3+\sqrt{7}}{2}(1+j), \frac{1+i+j+ij}{2} \rangle_{\mathbb{Z}[\sqrt{7}]}$ (where the torsion subgroup of the unit group is $SL_2(3)$),

$\mathcal{Q}_{\sqrt{13},\infty,\infty} = \langle 1, i, j, \omega := \frac{1+i+j+ij}{2} \rangle_{\mathbb{Q}[\sqrt{13}]}$, where $i^2 = j^2 = (ij)^2 = -1$ and the maximal order is

$\langle 1, i, \frac{i+j+z+zi}{2}, \frac{1+i+j+ij}{2} \rangle_{\mathbb{Z}[z]}$, where $z = \frac{3+\sqrt{13}}{2}$.

$\mathcal{Q}_{\sqrt{21},\infty,\infty} = \langle 1, \omega, i, \omega i \rangle_{\mathbb{Q}[\sqrt{21}]}$, where $\omega^2+\omega+1 = 0$, $i^2 = -1$, $\omega^i = \omega^{-1}$ and representatives for the two conjugacy classes of maximal orders are

$\mathcal{O}_1 := \langle 1, \frac{(1-\omega)(1+z)}{3}, i, \frac{(1-\omega)(1+z)}{3}i \rangle_{\mathbb{Z}[z]}$, where $z = \frac{1+\sqrt{21}}{2}$,

and $\mathcal{O}_2 := \langle 1, \omega, \frac{1+2\omega+i+z\omega}{3} =: j, \frac{\omega+\omega j+z+zj}{2} \rangle_{\mathbb{Z}[z]}$.

2.7 Automorphisms of algebras

2.7.1 Skew Laurent series

Let F be a field, D some F-division algebra, $\sigma : D \to D$ some F-algebra automorphism.

Definition 2.7.1. *$D((x,\sigma)) := \{\sum_{i\geq n} x^i d_i \mid n \in \mathbb{Z}, d_i \in D\}$ is called the* **skew Laurent series ring** *defined by σ. $D((x,\sigma))$ is an (associative and distributive) F-algebra with $dx = xd^\sigma$ for all $d \in D$.*

Remark 2.7.2.

- *$(\sum_{i\geq n} x^i d_i)(\sum_{j\geq m} x^j d'_j) = \sum_{k\geq n+m} x^k d''_k$ where $d''_k = \sum_{i+j=k} d_i^{\sigma^j} d'_j \in D$ is a finite sum, so multiplication is well defined.*
- *$D \cong 1 \cdot D \cong x^0 \cdot D \hookrightarrow D((x,\sigma))$ is some F-subalgebra.*
- *$(1-x)(1+x+x^2+\ldots) = 1$*
- *$v : D((x,\sigma)) \to \mathbb{Z} \cup \{\infty\}$, $v(\sum_{i\geq n} x^i d_i) := n$ if $d_n \neq 0$ is a discrete valuation on $D((x,\sigma))$.*
- *$V := \{z \in D((x,\sigma)) \mid v(z) \geq 0\}$ is an F-subalgebra of $D((x,\sigma))$ with maximal ideal $M := \{z \in D((x,\sigma)) \mid v(z) \geq 1\}$ and residue skew field $V/M \cong D$.*
- *For any $w \in M$ the series $1 + w + w^2 + \ldots \in V$ is well defined and $(1-w)(1+w+w^2+\ldots) = 1$, so $(1-w) \in V^*$.*

Theorem 2.7.3. *$D((x,\sigma))$ is a skew field and V is a valuation ring.*

Proof. We need to show that any non-zero element of D is invertible. Let $0 \neq z = (\sum_{i\geq n} x^i d_i) \in D((x,\sigma))$ with $d_n \neq 0$. Then $z = x^n d_n (1-w)$ where $w = -\sum_{j\geq 1} x^j d'_j \in M$. Therefore $z^{-1} = (1-w)^{-1} d_n^{-1} x^{-n} \in D((x,\sigma))$. □

Remark 2.7.4. *Let $\mathrm{Fix}_\sigma(D) = \{a \in D \mid a^\sigma = a\}$. Then*

$$Z(D((x,\sigma))) = \{\sum_{i\geq n} x^i d_i \mid d_i \in \mathrm{Fix}_\sigma(D) \text{ and } d_i d d_i^{-1} = d^{\sigma^i} \text{ for all } d \in D\}.$$

If the restriction of σ to the center $K = Z(D)$ has infinite order, then $Z(D((x,\sigma))) \cong \mathrm{Fix}_\sigma(K)$.

Proof. (a) $z := \sum_{i\geq n} x^i d_i \in Z(D((x,\sigma)))$ if and only if all monomials $x^i d_i$ commute with all monomials in $D((x,\sigma))$ (Exercise).
(b) $(x^i d_i)(x^j d') = x^{i+j} d_i^{(\sigma^j)} d'$ and $(x^j d')(x^i d_i) = x^{i+j} (d')^{(\sigma^i)} d_i$. So if z is central, then for all i, j and all $d' \in D$ we obtain

$$d_i^{(\sigma^j)} d' = (d')^{(\sigma^i)} d_i$$

Putting $d' = 1$ yields that $d_i^\sigma = d_i$ for all i and then $d_i d' d_i^{-1} = (d')^{(\sigma^i)}$ for all i and all $d' \in D$. □

2.7.2 Automorphism groups of algebras

Let F be a field, A some F-algebra, so $F \hookrightarrow Z(A) \subseteq A$.

Definition 2.7.5.

- $\mathrm{Aut}(A) := \{\sigma : A \to A \mid \sigma \textit{ is a ring automorphism }\}$.
- $\mathrm{Aut}_F(A) := \{\sigma : A \to A \mid \sigma \textit{ is an } F\textit{-algebra automorphism }\}$. *Then* $\mathrm{Aut}_F(A) \leq \mathrm{Aut}(A)$ *more precisely* $\mathrm{Aut}_F(A) = \{\sigma \in \mathrm{Aut}(A) \mid \sigma(F) = F \textit{ and } \sigma_{|F} = \mathrm{id}\}$.
- $\mathrm{Inn}(A^*) := \{\mathrm{Inn}_a : A \to A, x \mapsto a^{-1}xa \mid a \in A^*\} \trianglelefteq \mathrm{Aut}(A)$.
- $\mathrm{Out}(A) := \mathrm{Aut}(A)/\mathrm{Inn}(A^*)$.
- $\mathrm{Aut}(F, A) := \{\sigma \in \mathrm{Aut}(F) \mid \sigma \textit{ has a extension to some } \tilde{\sigma} \in \mathrm{Aut}(A)$.

Remark 2.7.6.

- *There is an exact sequence of groups*

$$1 \to Z(A)^* \to A^* \to \mathrm{Aut}(A) \to \mathrm{Out}(A) \to 1.$$

- *All ring automorphisms of A fix the center $Z(A)$ as a set, so there is a restriction map* $_{|Z(A)} : \mathrm{Aut}(A) \to \mathrm{Aut}(Z(A)), \sigma \mapsto \sigma_{|Z(A)}$.
- $\mathrm{Aut}(A)$ *acts on* $A^*/Z(A)^* \cong \mathrm{Inn}(A^*) \trianglelefteq \mathrm{Aut}(A)$ *by application* $(aZ(A)^*, \sigma) \mapsto a^\sigma Z(A^*)$ *respectively by the usual conjugation* $(\mathrm{Inn}_a, \sigma) \mapsto \sigma^{-1}\,\mathrm{Inn}_a\,\sigma$. *The mapping* $\mathrm{Inn} : A^*/Z(A)^* \to \mathrm{Inn}(A^*)$ *is an equivalence of* $\mathrm{Aut}(A)$*-groups.*

Example. Let $F \leq K \leq L$, $\mathrm{Gal}(L/F)$ abelian, $\mathrm{Gal}(L/K) = \langle\varphi\rangle$ cyclic, $[L : K] = n$. For $a \in K^*$ we consider the cyclic algebra $A = (L/K, \varphi, a) = \bigoplus u^i L$ with $\ell u = u\ell^\varphi$ and $u^n = a$. Then a Galois automorphism $\sigma \in \mathrm{Gal}(K/F)$ can be extended to some automorphism of A if and only if there is some $\lambda \in L^*$ such that $\frac{a^\sigma}{a} = N_{L/K}(\lambda)$. In particular if $a \in F$, then $\mathrm{Gal}(K/F) \leq \mathrm{Aut}(K, A)$.

Proof. We first note that by Galois theory any $\sigma \in \mathrm{Gal}(K/F)$ can be extended to some $\sigma \in \mathrm{Gal}(L/F)$. $\Leftarrow$: Let $\sigma \in \mathrm{Gal}(L/F)$ and define $\tilde{\sigma} \in \mathrm{Aut}(A)$ by $\tilde{\sigma} : u \mapsto u\lambda$ and $\ell \mapsto \ell^\sigma$. To show that this defines a ring automorphism we need to check the relations:

$$(u^{\tilde{\sigma}})^n = (u\lambda)^n = u^n N_{L/K}(\lambda) = aN_{L/K}(\lambda) = a^\sigma = (u^n)^{\tilde{\sigma}}$$

$$(\ell u)^{\tilde{\sigma}} = \ell^{\tilde{\sigma}} u^{\tilde{\sigma}} = \ell^\sigma u\lambda = u\lambda\ell^{\sigma\varphi} = (u\ell^\varphi)^{\tilde{\sigma}}.$$

$\Rightarrow$: Now let $\tilde{\sigma} \in \mathrm{Aut}(A)$ such that $\tilde{\sigma}_{|K} = \sigma$. Let $\sigma_1 \in \mathrm{Gal}(L/K)$ be an extension of σ. Then $L = \sigma_1(L)$ and $\tilde{\sigma}(L)$ are K-isomorphic subalgebras of A, so by Skolem/Noether, they are conjugate and we may assume wlog that $\tilde{\sigma}(L) = L$. Let $\lambda := u^{\tilde{\sigma}}u^{-1}$. Then $\lambda \in L = C_A(L)$ and $(u^n)^\sigma u^{-n} = a^\sigma/a = N_{L/K}(\lambda)$. □

2.7.3 The algebra ${}_\sigma A$

Definition 2.7.7. *Let A be some F-algebra and $\sigma \in \mathrm{Aut}(F)$. Then ${}_\sigma A$ is the F-algebra whose underlying ring is A and the embedding of F into $Z(A)$ is given by $f \mapsto f^\sigma 1_A$.*

Theorem 2.7.8. *$\sigma \in \mathrm{Aut}(F, A)$ if and only if ${}_\sigma A \cong A$ as F-algebra.*

Proof. First note that the identity map $\mathrm{id} : {}_\sigma A \to A, a \mapsto a$ restricts to $\mathrm{id}_{|F} = \sigma$. Note that the identity is an F-algebra isomorphism, if and only if $\sigma = \mathrm{id}$.
If $\varphi : A \to {}_\sigma A$ is an F-algebra isomorphism, then $\varphi\mathrm{id} : A \to {}_\sigma A \to A$ is a ring automorphism of A with $(\varphi\mathrm{id})_{|F} = \mathrm{id}_{|F} = \sigma$.
On the other hand assume that there is some $\tilde{\sigma} \in \mathrm{Aut}(A)$ such that $\tilde{\sigma}_{|F} = \sigma$. Then $\tilde{\sigma} : A \to {}_\sigma A$ is an F-algebra isomorphism. □

2.7.4 The finite dimensional and central simple case.

Let $K = Z(A)$ be a field and A a finite dimensional central simple K-algebra. Then by the theorem of Skolem and Noether $\mathrm{Aut}_K(A) = \mathrm{Inn}(A^*)$. Therefore

$$\mathrm{Out}(A) = \mathrm{Aut}(A)/\mathrm{Inn}(A^*) = \mathrm{Aut}(A)/\mathrm{Aut}_K(A) \cong \mathrm{Aut}(K, A)$$

Corollary 2.7.9. $\mathrm{Out}(A) \cong \mathrm{Aut}(K, A)$ *only depends on the class of A in the Brauer group of K.*

Proof. Write $A = M_n(D)(= D^{n\times n})$ for some central K-division algebra D. Then D is uniquely determined since $D \cong \mathrm{End}_A(V)$ for the simple A-module V. Let $\sigma \in \mathrm{Aut}(K)$. Then

$$\sigma \in \mathrm{Aut}(K, A) \Leftrightarrow {}_\sigma M_n(D) = M_n({}_\sigma D) \cong_K M_n(D) \Leftrightarrow {}_\sigma D \cong_K D \Leftrightarrow \sigma \in \mathrm{Aut}(K, D).$$

□

2.7.5 Generalized cyclic algebras.

Let $K = Z(A)$ be a field and A a finite dimensional central simple K-algebra.

Lemma 2.7.10. *Let $\sigma \in \mathrm{Aut}(A)$, $\mathrm{ord}(\sigma_{|K}) = n < \infty$. Then there is some $\alpha \in A^*$ with $\mathrm{Inn}_\alpha = \sigma^n$ such that $\alpha^\sigma = \alpha$.*

Proof. Let $\beta \in A^*$ such that $\mathrm{Inn}_\beta = \sigma^n$ (such β exists by the Theorem of Skolem and Noether). Then Inn_β and σ commute in $\mathrm{Aut}(A)$ so $\beta K^* = \beta^\sigma K^*$ (see Remark 2.7.6) and $b := \beta^{1-\sigma} \in K^*$. Let $F := \mathrm{Fix}_\sigma(K)$. Then K/F is cyclic and $N_{K/F}(b) = 1$. The Theorem 90 by Hilbert implies the existence of some $a \in K^*$ such that $b = \frac{a^\sigma}{a}$. Put $\alpha := \beta a$. □

Definition 2.7.11. *In the situation of the lemma put*

$$B := (A, \sigma, \alpha) := \bigoplus_{i=0}^{n-1} u^i A \text{ with } u^n = \alpha, au = ua^\sigma$$

Then (A, σ, α) is an F-algebra, where $F = \mathrm{Fix}_\sigma(K)$.

Theorem 2.7.12. *Let B be as in Definition 2.7.11 and $F := \mathrm{Fix}_\sigma(K)$. Then B is a central simple F-algebra, $\dim_F(B) = n^2 \dim_K(A)$, $C_B(K) = A$.*

Proof. The proof is similar as for crossed product algebras. Of course B is a ring, $F \subseteq K \subseteq A \cong u^0 A \subseteq B$, and

$$\dim_F(B) = \dim_K(B)\dim_F(K) = \dim_K(A)\dim_A(B)\dim_F(K) = m^2 \cdot n \cdot n = (mn)^2.$$

To show that B is a simple algebra we proceed as for crossed products. Assume that $0 \neq X \trianglelefteq B$ is a twosided ideal of B and choose $0 \neq x = \sum_{i=0}^{r} u^i a_i \in X$ such that r is minimal. Then $a_0 \neq 0$ (otherwise multiplication by u^{-1} yields a smaller r).
If $r = 0$, then $0 \neq x = a_0 \in A$ and hence $0 \neq x \in A \cap X \trianglelefteq A$, so $A \cap X = A$ because A is simple. But then $X = B$.
If $r > 0$ then choose $b \in K^* \setminus F$ such that $b \neq b^{(\sigma^r)}$. Then $x - bxb^{(\sigma^r)^{-1}} = \sum_{i=0}^{r} u^i a_i' \in X$ with

$$a_0' = a_0(1 - b/(b^{\sigma^r})) \neq 0,\ a_r' = a_r - b^{(\sigma^r)} a_r b^{(\sigma^r)^{-1}} = 0$$

contradicting the minimality of r. □

Corollary 2.7.13. *Let $\sigma \in \mathrm{Aut}(K)$, $F := \mathrm{Fix}_\sigma(K)$, $[K : F] = n < \infty$. Then $\sigma \in \mathrm{Aut}(K, A)$ if and only if there is some central simple F-algebra B containing K as a subfield such that $C_B(K) \cong A$.*

Proof. $\Leftarrow$: from the construction in the theorem above.
$\Rightarrow$: The theorem of Skolem and Noether gives the existence of some $u \in B^*$ such that $(\mathrm{Inn}_u)_{|K} = \sigma$. In particular $u^{-1}Ku = K$ and therefore $u^{-1}Au = A$ so the restriction of Inn_u to A is an automorphism of A that extends σ. □

Examples:
1) Let A, σ, α be as in Lemma 2.7.10, then $(M_n(A), (\sigma)_{ij}, \mathrm{diag}(\alpha, \ldots, \alpha)) \cong_F M_n((A, \sigma, \alpha))$.
2) Let A_0 be a central simple F-algebra and K/F cyclic, $\mathrm{Gal}(K/F) = \langle \sigma_0 \rangle$ of order n. Let $A := A_0 \otimes_F K$, $\sigma := \mathrm{id} \otimes \sigma_0 \in \mathrm{Aut}_F(A)$. Then any α as in Lemma 2.7.10 satisfies $\alpha \in F^*$ and for any $\alpha \in F^*$ we obtain $(A, \sigma, \alpha) \cong A_0 \otimes_F (K/F, \sigma_0, \alpha)$.
To see this note that both tensor factors naturally imbed into the generalized cyclic algebra. The images commute, so we obtain a homomorphism of the tensor product, which is injective, since the tensor product is simple and hence an isomorphism by comparing dimensions.

2.7.6 Restriction

Remark 2.7.14. *Let B be as in Theorem 2.7.12. Then $B \otimes_F K \cong M_n(A)$.*

Proof. B is a free right A-module of rank n and the left multiplication

$$\lambda : B \to \mathrm{End}_A(B) = M_n(A), b \mapsto \lambda(b) : x \mapsto bx$$

is an F-algebra monomorphism. Also $K = Z(M_n(A)) \leq M_n(A)$ so we obtain an embedding of the central simple K-algebra $\lambda \otimes \mathrm{diag} : B \otimes_F K \to M_n(A)$. This is an isomorphism by comparing dimensions. □

Theorem 2.7.15. *Let $\sigma \in \mathrm{Aut}(K)$, $\mathrm{ord}(\sigma) = n$, $F := \mathrm{Fix}_\sigma(K)$, A/K central simple, $[A : K] = m^2 < \infty$. Then $\sigma \in \mathrm{Aut}(K, A)$ if and only if $[A] \in Im(res : \mathrm{Br}(F) \to \mathrm{Br}(K))$.*

Proof. $\Rightarrow$: Is the remark above.
$\Leftarrow$: Let B be some central simple F-algebra such that $B \otimes_F K \cong M_r(A)$. The $\mathrm{id} \otimes \sigma \in \mathrm{Aut}(M_r(A))$, so $\sigma \in \mathrm{Aut}(K, M_r(A)) = \mathrm{Aut}(K, A)$. □

Examples:
1) If K is a local field, then the restriction map $\mathrm{Br}(F) \to \mathrm{Br}(K)$ is surjective, since this is just multiplication by $n := [K : F]$ from $\mathbb{Q}/\mathbb{Z}$ to $\mathbb{Q}/\mathbb{Z}$. In particular $\mathrm{Aut}(K, A) = \mathrm{Aut}(K)$.
2) If K is a global field, $\wp$ a place of F and $\wp'$ a place of K that lies over $\wp$, then the degree $n_\wp := [K_{\wp'} : F_\wp]$ of the completions does not depend on the choice of $\wp'$ since K/F is Galois. Let A_0 be some central simple F-algebra. Then the local invariants for $A_0 \otimes_F K$ are

$$\mathrm{inv}_{\wp'}(A_0 \otimes_F K) = \mathrm{inv}_\wp(A_0) n_\wp$$

so these are constant on the places $\wp'$ that lie over some fixed place $\wp$ of K. Since we may always find some further place that is not decomposed in K/F (to insure that the sum of the local invariants of A_0 is 0) we obtain

Remark 2.7.16. *For any central simple K-algebra A:*

$\sigma \in \mathrm{Aut}(K, A) \Leftrightarrow [A] \in Im(\mathrm{res} : \mathrm{Br}(F) \to \mathrm{Br}(K)) \Leftrightarrow \mathrm{inv}_{\sigma(\wp)}(A) = \mathrm{inv}_\wp(A)$ *for all places $\wp$ of K.*

2.8 The Brauer group of $\mathbb{Q}((t))$.

2.8.1 Discrete valuated skew fields.

Let $(\mathcal{D}, v)$ be some complete discrete valuated skew field, $F := Z(\mathcal{D})$, $V := \{x \in \mathcal{D} \mid v(x) \geq 0\}$ the valuation ring with maximal ideal $M := \{x \in \mathcal{D} \mid v(x) > 0\}$. Then $D := V/M$ is a skew field with

$$\overline{F} = V \cap F/M \cap F \leq Z(D) \leq D = V/M.$$

Any $d \in \mathcal{D}^*$ induces an automorphism of V that fixes M, because $v(dxd^{-1}) = v(x)$ for all $x \in \mathcal{D}$. So $\mathrm{Inn}_d : V \to V, M \to M$ defines $\overline{\mathrm{Inn}_d} \in \mathrm{Aut}(D), \overline{x} \mapsto \overline{d^{-1}xd}$. For any $u \in V^*$ we obtain $\overline{\mathrm{Inn}_u} = \mathrm{Inn}_{\overline{u}} \in \mathrm{Inn}(D)$. We assume wlog that $v : \mathcal{D}^* \to \mathbb{Z}$ is surjective.

Remark 2.8.1. *There is a group homomorphism $\theta : \mathbb{Z} = v(\mathcal{D}^*) \to \mathrm{Gal}(Z(D)/\overline{F}), \gamma \mapsto (\overline{\mathrm{Inn}_d})_{|Z(D)}$ where $d \in \mathcal{D}^*$ is any element with $v(d) = \gamma$.*

Lemma 2.8.2. *Let $L \leq \mathcal{D}$ be a subfield. Then $\overline{L} \cap Z(D) \subset \mathrm{Fix}(\theta(v(L^*)))$.*

2.8.2 Skew Laurent series II

We apply this to the following situation: D/K is a central division algebra, $[D : K] = m^2 < \infty$, $\sigma \in \mathrm{Aut}(D)$, $\mathrm{ord}(\sigma_{|K}) = n < \infty$, $F = \mathrm{Fix}_\sigma(K)$. In this situation we know that there is some $\alpha \in D^*$ such that $\sigma(\alpha) = \alpha$ and $\mathrm{Inn}_\alpha = \sigma^n$ (Lemma 2.7.10).

Moreover

$$\mathcal{D} := D((x,\sigma)) := \{\sum_{i\geq n} x^i d_i \mid n \in \mathbb{Z}, d_i \in D\}$$

is a discrete valuated division algebra with valuation ring $V = \{\sum_{i\geq 0} x^i d_i \mid d_i \in D\}$ and maximal ideal $M = \{\sum_{i\geq 1} x^i d_i \mid d_i \in D\}$ and $V/M \cong D$.

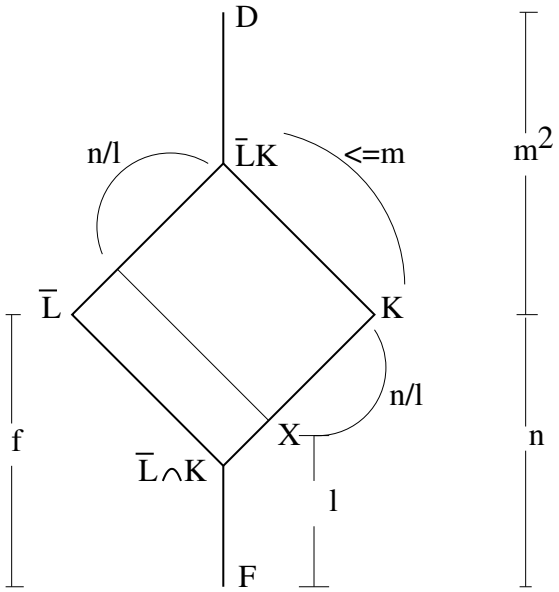
Remark 2.8.3. *A monomial $z = x^k a \in \mathcal{D}$ is in the center of $\mathcal{D}$ if and only if $k = ni$ and $a = \alpha^i c$ for some $i \in \mathbb{Z}$ and $c \in F$. So*

$$Z(\mathcal{D}) = F((t)) =: Z \text{ with } t := x^n\alpha^{-1}.$$

Moreover $\mathcal{D} = \bigoplus_{i=0}^{n-1} x^i D((t)) = (D((t)), \sigma_t, \alpha t)$ with $x^n = t\alpha = \alpha t$, $(\mathrm{Inn}_x)_{|D((t))} = \sigma_t$ and $d^{\sigma_t} = d^\sigma$ for all $d \in D$ and $t^{\sigma_t} = t$. By Theorem 2.7.12 $\mathrm{ind}(\mathcal{D}) = nm$.

The map $\theta : \mathbb{Z} \to \mathrm{Gal}(K/F)$ maps any $\gamma \in \mathbb{Z}$ to $\theta(\gamma) = (\overline{\mathrm{Inn}_{x^\gamma}})_{|K} = \sigma^\gamma$.

Subfields



Lemma 2.8.4. *Let L be some maximal subfield of $\mathcal{D}$, so $[L : Z] = mn$. Then $\overline{L}K \leq D$ is some maximal subfield of D.*

Proof. Let $Z = F((t)) = Z(\mathcal{D})$, $e := [v(L^*) : v(Z^*)] = [\ell\mathbb{Z} : n\mathbb{Z}] = \frac{n}{\ell}$, $f := [\overline{L} : F]$. Then $ef = [L : Z] = nm$ so $m = \frac{f}{\ell}$. Let $X := \mathrm{Fix}_K(\sigma^\ell)$. Then $\overline{L} \cap K \leq X$ and $[X : F] = \ell$, $[K : X] = \frac{n}{\ell}$. Moreover

$$\frac{f}{\ell} = m \geq [\overline{L}K : K] = [\overline{L} : \overline{L} \cap K] \text{ and } [\overline{L} : \overline{L} \cap K][\overline{L} \cap K : F] = f$$

Since $[\overline{L} \cap K : F] \leq [X : F] = \ell$ we obtain equality everywhere. □

Theorem 2.8.5. *Assume that $char(F) = 0$. If $D((x,\sigma)) =: \mathcal{D}$ is a crossed product algebra (i.e. there is some maximal subfield that is Galois over $F((t)) = Z(\mathcal{D})$), then there is some maximal subfield $M \leq D$ such that M/F is Galois.*

Proof. Let $L \leq \mathcal{D}$ be a maximal subfield such that $L/Z(\mathcal{D})$ is Galois. Put $M := \overline{L}K = \overline{L}Z(D) \leq D$. Then M is a subfield of D. By Lemma 2.8.4 it is a maximal subfield. To show that M/F is Galois it is enough to show that M/F is normal. But L/Z is normal, so by Hensels Lemma also $\overline{L}/\overline{Z}$ is normal. So $\overline{L}/F$ is normal, K/F is cyclic and hence normal and so is the compositum M. □

2.8.3 Non-crossed products over $\mathbb{Q}((t))$

We know come to the main result of this section, the construction of a division algebra $\mathcal{D}$ with center $\mathbb{Q}((t))$ that is not a crossed product algebra. To this aim we use the previous theorem and try to construct a division algebra D with $Z(D) = K$ a number field such that D does not contain a maximal subfield M that is Galois over $\mathbb{Q}$.

(0) Choose some prime $\ell > 2$.

(1) Choose some other prime p such that $p \equiv_\ell 1$ but $p \not\equiv_{\ell^2} 1$.

(2) Construct some cyclic extension $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] = \ell$ and p is totally ramified in K (for instance the subfield of degree ℓ of the p-th cyclotomic number field). Put $\langle\sigma\rangle := \mathrm{Gal}(K/\mathbb{Q})$.

(3) Choose some prime $\ell \neq q \not\equiv_\ell 1$ that is inert in $K/\mathbb{Q}$.

(4) Choose some cyclic division algebra D/K with center K such that

$$\mathrm{inv}_q(D) \neq 0 \text{ and } \mathrm{inv}_{\sigma(\wp)}(D) = \mathrm{inv}_\wp(D) \text{ for all places } \wp \text{ of } K.$$

Under these assumptions there is some $\tilde{\sigma} \in \mathrm{Aut}(D)$ such that $\tilde{\sigma}_{|K} = \sigma$.

(5) Put $\mathcal{D} := D((x,\tilde{\sigma}))$. Then $Z(\mathcal{D}) = \mathbb{Q}((t))$ with $t = x^n\alpha^{-1}$.

Theorem 2.8.6. *$\mathcal{D}$ is not a crossed product algebra.*

Proof. We use Theorem 2.8.5. If $\mathcal{D}$ is a crossed product algebra, then the algebra D with $Z(D) = K$ contains some maximal subfield M such that $M/\mathbb{Q}$ is a Galois extension. Then $[M : \mathbb{Q}] = \ell^2$ and we have two possible situations:
1) $\mathrm{Gal}(M/\mathbb{Q})$ is cyclic. Then K is the unique proper subfield of M and since p is totally ramified in $K/\mathbb{Q}$ it is also totally (and tamely) ramified in $M/\mathbb{Q}$. So the completion is $M_p = \mathbb{Q}_p(\sqrt[\ell^2]{\pi})$ for some prime element π in $\mathbb{Q}_p$. But M_p is only normal over $\mathbb{Q}_p$ if $\mathbb{Q}_p$ contains the ℓ^2-th roots of unity. This contradicts our assumption (1) that $p \not\equiv_{\ell^2} 1$.
2) $\mathrm{Gal}(M/\mathbb{Q}) \cong C_\ell \times C_\ell$. Then we consider the completion at the prime q. By assumption q is inert in K, so K_q is the unique unramified extension of degree ℓ of $\mathbb{Q}_q$. Since M is a maximal subfield (and hence a splitting field) of D and $\mathrm{inv}_q(D) \neq 0$, the completion M_q is

a field and hence $M_q = K_q N_q$ is the compositum of K_q with any other subfield N_q of index ℓ over $\mathbb{Q}_q$. Since $N_q \neq K_q$ the extension $N_q/\mathbb{Q}_q$ is again totally (and tamely) ramified and now of degree ℓ. Being Galois implies that $\mathbb{Q}_q$ contains the ℓth roots of unity, so $q \equiv_\ell 1$ a contradiction to assumption (3). □

Example Choose $\ell = 3$, $p = 7$, $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Then $q = 2$ works and we may define D a division algebra with center K and local invariants

$$\mathrm{inv}_2(D) = \frac{1}{3},\ \mathrm{inv}_5(D) = \frac{2}{3}$$

2.8.4 An example where exponent ≠ index

Let $\sigma \in \mathrm{Aut}(K)$ of order n, $F := \mathrm{Fix}(\sigma)$ and D_0 a central F-division algebra. Put $D := D_0 \otimes_F K$, $\tilde{\sigma} := \mathrm{id} \otimes \sigma$, $\alpha := 1$. Then by Remark 2.8.3

$$D((x,\tilde{\sigma})) = (D((t)), \tilde{\sigma}_t, t) \cong D_0((t)) \otimes_{F((t))} (K((t))/F((t)), \tilde{\sigma}_t, t)$$

where the last isomorphism is the one from Example 2) in section 2.7.5.

The exponent of $D_0((t))$ divides the $\mathrm{ind}(D_0((t))) = \mathrm{ind}(D_0)$ The exponent of $(K((t))/F((t)), \tilde{\sigma}_t, t)$ divides $\mathrm{ind}((K((t))/F((t)), \tilde{\sigma}_t, t)) = [K : F] = n$. And therefore the exponent of $D((x,\tilde{\sigma}))$ divides $\mathrm{lcm}(n, \mathrm{ind}(D_0))$. But the index

$$\mathrm{ind}(D((x,\tilde{\sigma}))) = n\,\mathrm{ind}(D_0) > \mathrm{lcm}(n, \mathrm{ind}(D_0)) \text{ if } \gcd(n, \mathrm{ind}(D_0)) \neq 1.$$

Index

Chapter 3

Exercises.

Blatt 1

Aufgabe 1

Sei $d \in \mathbb{Z} - \{0, 1\}$ quadratfrei und $K = \mathbb{Q}(\sqrt{d})$.

(i). Bestimmen Sie eine Ganzheitsbasis von K.

(ii). Bestimmen Sie die Einheitengruppe $\mathbb{Z}_K^*$ im Fall $d < 0$.

Aufgabe 2

Sei $p > 2$ eine Primzahl. Weiter sei $d \in \mathbb{F}_p[X]$ quadratfrei mit $\deg d > 0$. Bestimmen Sie den ganzen Abschluss von $\mathbb{F}_p[X]$ in $\mathbb{F}_p(X, \sqrt{d}) = \mathbb{F}_p(X)[T]/(T^2 - d)$.

Aufgabe 3

(i). Zeigen Sie, dass jeder (kommutative) faktorielle Ring ganzabgeschlossen ist.

(ii). Begründen Sie warum $\mathbb{Z}[\sqrt{5}]$ kein Hauptidealbereich ist.

Aufgabe 4

Sei L/K eine endliche Körpererweiterung. Zeigen Sie:

(i). Jedes $\alpha \in L$ induziert einen Endomorphismus $\mathrm{mult}_\alpha \colon L \to L,\ x \mapsto \alpha x$ des K-Vektorraums L.

(ii). Die Abbildung $\mathrm{mult} \colon L \to \mathrm{End}_K(L), \alpha \mapsto \mathrm{mult}_\alpha$ ist ein injektiver K-Algebrenmorphismus.

(iii). Die Abbildung $S_{L/K} \colon L \to K,\ \alpha \mapsto \mathrm{Spur}(\mathrm{mult}_\alpha)$ ist K-linear.

(iv). Die Abbildung $N_{L/K}\colon L \to K,\ \alpha \mapsto \det(\mathrm{mult}_\alpha)$ ist multiplikativ.

(v). Für jedes $\alpha \in L$ ist $\mu_{\alpha,K}(X) \in K[X]$ irreduzibel von Grad $d := [K(\alpha) : K]$. Ferner ist d ein Teiler von $n := [L : K]$ und erfüllt $\mu_{\alpha,K}^{n/d} = \chi_{\alpha,K} = \chi_{\mathrm{mult}_\alpha}$.

Blatt 2

Sei K ein algebraischer Zahlkörper und $n = [K : \mathbb{Q}]$.

Definition

- Eine Ordnung in K ist ein Teilring von K der auch ein Gitter in $(K, S_{K/\mathbb{Q}})$ ist.
- Zu einem Gitter I in K sei $\mathcal{O}(I) := \{a \in K \mid aI \subseteq I\}$ die zugehörige Ordnung.
- Zu einer Ordnung R in K und einer Primzahl p bezeichne

$$J_p(R) := \{a \in R \mid a^m \in pR \text{ für ein } m \geq 0\}$$

das p-Radikal von R.

Aufgabe 1

Zeigen Sie:

(i). Der Ring der ganzen Zahlen $\mathbb{Z}_K$ ist eine Ordnung und enthält jede Ordnung von K. (Man sagt $\mathbb{Z}_K$ ist die Maximalordnung von K.)

(ii). Jedes von (0) verschiedene Ideal einer Ordnung in K ist ein Gitter.

(iii). Ist I ein Gitter in K so ist $\mathcal{O}(I)$ eine Ordnung in K.

Im Folgenden sei R eine Ordnung in K und p eine Primzahl. Zeigen Sie:

Aufgabe 2

(i). $J_p(R)$ ist ein Ideal von R.

(ii). Es existiert ein $m \geq 0$ so, dass $J_p(R)^m \subseteq pR$. (Es sei $J_p(R)^0 = R$.)

Aufgabe 3

Es gilt:

$$pR \subseteq p\mathcal{O}(J_p(R)) \subseteq J_p(R) \subsetneq R\,.$$

Insbesondere ist $|\mathcal{O}(J_p(R))/R|$ ein Teiler von p^{n-1}.

Aufgabe 4 (Zassenhaus Round 2)

(i). Es ist $S := \{a \in \mathbb{Z}_K \mid p^k a \in R \text{ für ein } k \geq 0\}$ eine Ordnung von K.

(ii). Ist $R = \mathcal{O}(J_p(R))$ so gilt $R = S$.

(iii). p teilt $|\mathbb{Z}_K/R|$ genau dann wenn $R \subsetneq \mathcal{O}(J_p(R))$.

(Hinweis zu (b): Wäre $R \subsetneq S$, so existiert ein $k \geq 0$ mit $J_p(R)^k \cdot S \not\subseteq R$ und $J_p(R)^{k+1} \cdot S \subseteq R$. Wähle $x \in J_p(R)^k \cdot S - R$ und zeige $xJ_p(R) \subseteq J_p(R)$.)

Blatt 3

Aufgabe 1

Bestimmen Sie die Einheitengruppen $\mathbb{Z}^*_{\mathbb{Q}(\sqrt{d})}$ für $d = 2, 3, 5$.

Aufgabe 2

Sei $K = \mathbb{Q}(\zeta_5)$ und $^-$ bezeichne den Automorphismus auf K welcher durch $\zeta_5 \mapsto \zeta_5^{-1}$ definiert wird. Zeigen Sie:

(i). $\varphi\colon \mathbb{Z}_K^* \to \mu(\mathbb{Z}_K^*),\ u \mapsto u/\bar{u}$ ist ein wohldefinierter Gruppenmorphismus.

(ii). -1 liegt nicht im Bild von φ. Insbesondere existiert zu jedem $u \in \mathbb{Z}_K^*$ ein $k \in \mathbb{Z}$ so, dass $\zeta_5^k u \in \mathrm{Fix}_K(\langle^-\rangle)$.

(iii). Es ist $\mathbb{Z}_K^* = \left\langle -\zeta_5,\ \frac{1+\sqrt{5}}{2} \right\rangle$.

Hinweis: In der Vorlesung Algebra wurde $\mathbb{Z}_K = \mathbb{Z}[\zeta_5]$ gezeigt.

Ad (b): Ist $u \in \mathbb{Z}_K^*$ mit $u = -\bar{u}$ so liegt u im $\mathbb{Z}$-Gitter $\left\langle \zeta_5 - \zeta_5^{-1},\ \zeta_5^2 - \zeta_5^{-2} \right\rangle_{\mathbb{Z}}$ und wird daher von $\zeta_5 - \zeta_5^{-1}$ in $\mathbb{Z}_K$ geteilt.

Ad (c): Es ist $\mathrm{Fix}_K(\langle^-\rangle) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) \cong \mathbb{Q}(\sqrt{5})$.

Aufgabe 3

Es sei K ein Zahlkörper mit genau r reellen und $2s$ echt komplexen Einbettungen. Die Menge der Einbettungen heisse G. Zeigen Sie:

(i). Für $t \in \mathbb{R}_{>0}$ ist $X_t := \left\{(z_\tau)_{\tau\in G} \in K_\mathbb{R} : \sum_{\tau\in G} |z_\tau| < t\right\} \subset K_\mathbb{R}$ eine zentralsymmetrische konvexe Menge mit Volumen $2^r\pi^s t^n/n!$.

(ii). In jeder Idealklasse von K gibt es ein ganzes Ideal $\mathfrak{a}$ mit $N_{K/\mathbb{Q}}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$.

(iii). Ist $K \neq \mathbb{Q}$ so ist $|d_K| > 1$.

Aufgabe 4

Bestimmen Sie den Isomorphietyp von $\mathrm{Cl}(\mathbb{Q}(\sqrt{-17}))$ sowie Vertreter aller Idealklassen.

Blatt 4

Aufgabe 1

Sei $K = \mathbb{Q}(\sqrt{-d})$ mit $d = 14$ bzw. $d = 30$. Bestimmen Sie jeweils den Isomorphietyp und ein Vertretersystem von $\mathrm{Cl}(K)$, $\mathrm{Cl}(K)^2$ und $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$.

Aufgabe 2

Sei K ein algebraischer Zahlkörper. Zeigen Sie:

(i). Es sei $\mathfrak{b} = \prod_{i=1}^k \mathfrak{p}_i^{n_i} \trianglelefteq \mathbb{Z}_K$ ein Produkt von paarweise verschiedenen Primidealen. Weiter seien $b_i \in \mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}$. Dann gibt es ein $x \in \mathfrak{b}$ mit $x \equiv b_i \mod \mathfrak{p}_i^{n_i+1}$ für alle $1 \leq i \leq k$.

(ii). Sind $\mathfrak{a} \subseteq \mathfrak{b}$ zwei gebrochene Ideale in K, so ist $\mathfrak{b} = \mathfrak{a} + (x)$ für ein $x \in \mathfrak{b}$.

(iii). Jedes gebrochene Ideal von K kann mit (höchstens) zwei Elementen erzeugt werden.

Hinweis: (a) Chinesischer Restsatz.
(b) Ohne Einschränkung ist $\mathfrak{b} = \prod_{i=1}^k \mathfrak{p}_i^{n_i}$ ganz. Weiter darf man annehmen, dass $\mathfrak{a}$ ebenfalls ein Produkt der Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ ist.Wähle nun x wie in (a) und zeige dass jedes Primideal von $\mathbb{Z}_K$ die Ideale $\mathfrak{b}$ und $\mathfrak{a} + (x)$ mit der selben Vielfachheit teilt.

Aufgabe 3

Es seien p und ℓ zwei Primzahlen und $K = \mathbb{Q}(\zeta_p)$. Zeigen Sie:

(i). $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$.

(ii). $X^p - 1 \in \mathbb{F}_\ell[X]$ hat genau dann eine mehrfache Nullstelle in $\overline{\mathbb{F}}_\ell$ falls $p = \ell$.

(iii). p ist die einzige Primzahl welche in $\mathbb{Z}_K$ verzweigt.

(iv). $\mathfrak{p} := (1 - \zeta_p)$ ist das einzige Primideal von $\mathbb{Z}_K$ welches p enthält und es gilt $e_\mathfrak{p} = p - 1$ sowie $f_\mathfrak{p} = 1$.

(v). Sei $\ell \neq p$ und $\mathfrak{q}$ ein Primideal von $\mathbb{Z}_K$ mit $\ell \in \mathfrak{q}$. Dann ist $e_\mathfrak{q} = 1$ und $f_\mathfrak{q}$ ist die Ordnung von ℓ in $\mathbb{F}_p^*$.

Hinweis: Satz 3.56 der Vorlesung Algebra WS10/11.

Aufgabe 4

Bestimmen Sie die Primidealzerlegung von $\ell\mathbb{Z}[\zeta_7]$ für $\ell = 2, 3, 7, 13, 29$ sowie die Trägheits- bzw. Verzweigungsgrade und Erzeuger der auftretenden Primideale.

Hinweis: Zum Faktorisieren von Polynomen über endlichen Körpern darf ein beliebiges Computeralgebrasystem benutzt werden. Die Faktorisierungsroutinen für Ideale in Dedekindringen dürfen nicht verwendet werden.

Blatt 5

Aufgabe 1

Sei $n \in \mathbb{Z}_{>1}$ und ζ_n eine primitive n-te Einheitswurzel. Zeigen Sie:

(i). Sei $n = p^r$ für eine Primzahl p. Für je zwei zu p teilerfremde Zahlen $i, j \in \mathbb{Z}$ ist dann $(1 - \zeta_n^i)/(1 - \zeta_n^j) \in \mathbb{Z}[\zeta_n]^*$.

(ii). Sei n keine Primzahlpotenz. Dann ist $(1-\zeta_n) \in \mathbb{Z}[\zeta_n]^*$. Genauer gilt $\prod_{i\in(\mathbb{Z}/n\mathbb{Z})^*}(1-\zeta_n^i) = 1$.

Hinweis zu (b). Seien $T = \{d \in \mathbb{Z}_{>1} : d \mid n\}$ und $P = \{t \in T \mid t \text{ ist Primzahlpotenz}\}$. Dann ist $n = \sum_{i=0}^{n-1} 1^i = \prod_{i\in P} \Phi_i(1) \cdot \prod_{i\in T-P} \Phi_i(1)$. Folgere $\Phi_i(1) \in \mathbb{Z}^*$ für alle $i \in T - P$.

Aufgabe 2

Es seien $K \subseteq L \subseteq M$ algebraische Zahlkörper und $\mathfrak{p} \trianglelefteq \mathbb{Z}_M$ ein Primideal. Weiter sei $\mathfrak{P} = \mathfrak{p} \cap \mathbb{Z}_L$. Zeigen Sie:

(i). $e_{M/K}(\mathfrak{p}) = e_{M/L}(\mathfrak{p}) \cdot e_{L/K}(\mathfrak{P})$

(ii). $f_{M/K}(\mathfrak{p}) = f_{M/L}(\mathfrak{p}) \cdot f_{L/K}(\mathfrak{P})$

Aufgabe 3

Sei $K = \mathbb{Q}(\zeta_5, \sqrt{2})$. Weiter sei $p \in \{2, 3, 5, 11\}$ und $\mathfrak{p} \trianglelefteq \mathbb{Z}_K$ ein Primideal das p enthält. Bestimmen Sie die Zerlegungs- und Trägheitsgrade sowie die Zerlegungs- und Trägheitsgruppen von $\mathfrak{p}$.

Aufgabe 4

Es seien $\mathfrak{a}$ und $\mathfrak{b}$ gebrochene Ideale in einem algebraischen Zahlkörper K. Zeigen Sie:

(i). Es existieren $x, y \in K^*$ so, dass $x\mathfrak{a}$ und $y\mathfrak{b}$ ganze teilerfremde Ideale von $\mathbb{Z}_K$ sind.

(ii). Es ist $\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{ab} \oplus \mathbb{Z}_K$ als $\mathbb{Z}_K$-Moduln.

(iii). $\mathfrak{a}$ ist ein projektiver $\mathbb{Z}_K$-Modul.

Hinweis: Aufgabe 2 von Blatt 4 sowie Übungen zur Algebra WS10/11, Aufgabe 1 auf Blatt 11.

Blatt 6

Für einen kommutativen Ring R bezeichne $\mathrm{Spec}(R)$ die Menge der von (0) verschiedenen Primideale von R. Ist $\mathfrak{p}$ ein Primideal in einem Dedekindring R und M ein R-Modul so sei $M_\mathfrak{p} := M \otimes_R R_\mathfrak{p}$ die Komplettierung von M an $\mathfrak{p}$.

Aufgabe 1

Es sei R ein Dedekindring. Weiter seien V ein endlich dimensionaler $\mathrm{Quot}(R)$-Vektorraum und L, L' zwei volle R-Gitter in V. Zeigen Sie:

(i). Ist M ein endlich erzeugter R-Modul mit $M_\mathfrak{p} = 0$ für alle $\mathfrak{p} \in \mathrm{Spec}(R)$, so ist $M = 0$.

(ii). $\{\mathfrak{p} \in \mathrm{Spec}(R) \mid L_\mathfrak{p} \neq L'_\mathfrak{p}\}$ ist endlich.

(iii). Es ist $L = L'$ genau dann wenn $L_\mathfrak{p} = L'_\mathfrak{p}$ für alle $\mathfrak{p} \in \mathrm{Spec}(R)$ gilt.

Aufgabe 2

Sei R ein Noetherscher ganzabgeschlossener Integritätsbereich. Zeigen Sie, dass die folgenden Aussagen äquivalent sind.

(i). Jedes von (0) verschiedene Primideal von R ist maximal, d.h. R ist ein Dedekindring.

(ii). Für alle $\mathfrak{p} \in \mathrm{Spec}(R)$ ist $R_{(\mathfrak{p})}$ ein diskreter Bewertungsring.

Aufgabe 3

Sei p eine Primzahl. Bestimmen Sie die Menge der Quadrate in $\mathbb{Z}_p^*$, $\mathbb{Z}_p$ sowie $\mathbb{Q}_p^*$. Bestimmen Sie ferner Erzeuger sowie den Isomorphietyp von $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$ bzw. $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.

Hinweis: Im Fall $p > 2$ fixiere man ein Nichtquadrat $\varepsilon \in \mathbb{F}_p^*$. Der Fall $p = 2$ ist gesondert zu betrachten.

Aufgabe 4

Faktorisieren Sie $X^{15} - 1 \in \mathbb{Z}_p[X]$ für $p \in P := \{2, 3, 11\}$. Die auftretenden p-adischen Zahlen sind modulo p^4 zu approximieren. Bestimmen Sie ferner die Primidealzerlegung sowie die Trägheits- und Zerlegungsgrade von $p\mathbb{Z}[\zeta_{15}]$ in $\mathbb{Z}[\zeta_{15}]$ für alle $p \in P$.

Blatt 7

Aufgabe 1

Bestimmen Sie (bis auf Isomorphie) alle Erweiterungen von $\mathbb{Q}_5$ von Grad 4.

Aufgabe 2

Sei K ein algebraischer Zahlkörper. Zeigen Sie: Die Menge der in $K/\mathbb{Q}$ verzweigten Primzahlen ist endlich. Ist ferner $K \neq \mathbb{Q}$ so verzweigt mindestens eine Primzahl in K.

Aufgabe 3

(i). Bestimmen Sie $\mathbb{Q}_3(\sqrt{3})^*$.

(ii). Bestimmen Sie $\mathbb{Q}_3(\sqrt{-3})^*$.

(iii). Sei p eine Primzahl. Bestimmen Sie Erzeuger von $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^3$.

Aufgabe 4

(i). Es seien E/L und L/K endliche separable Erweiterungen. Zeigen Sie

$$D(E/K) = N_{L/K}(D(E/L))D(L/K)^{[E:L]}\,.$$

(ii). Es seien K_1/K und K_2/K endliche separable Erweiterungen und $L := K_1K_2$. Zeigen Sie: Sind $D(K_1/K)$ und $D(K_2 : K)$ teilerfremd und gilt $[L : K] = [K_1 : K][K_2 : K]$, so ist

$$D(L/K) = D(K_1/K)^{[K_2:K]}D(K_2/K)^{[K_1:K]}\,.$$

(iii). Es seien $K_1 = \mathbb{Q}(i)$, $K_2 = \mathbb{Q}(\sqrt{5})$, $K_3 = \mathbb{Q}(\sqrt{-5})$ und $L = \mathbb{Q}(i, \sqrt{5})$. Bestimmen Sie $D(L/\mathbb{Q})$, $D(K_i/\mathbb{Q})$ sowie $D(L/K_i)$ für $i = 1, 2, 3$. Gibt es ein Primideal in $\mathbb{Z}_{K_3}$ welches in $\mathbb{Z}_L$ verzweigt?

Hinweis zu (a): Ohne Einschränkung ist K vollständig diskret bewertet. Für (b) siehe Lemma 1.7.6.

"Ubung Algebraische Zahlentheorie II

Prof. Dr. Nebe **(WS 11/12)**

Aufgabe 1. (Die Brauergruppe der reellen Zahlen.)
(a) Zeigen Sie, dass $\mathrm{Br}(\mathbb{R}) \cong C_2$.
(b) Bestimmen Sie die Signatur der Spurbilinearform von $\mathbb{R}^{2\times 2}$ und von $\mathbb{H}$ (den Hamilton

Quaternionen).
(c) Entwerfen Sie einen Algorithmus, der den Isomorphietyp einer in ihrer regulären Darstellung gegebenen halbeinfachen $\mathbb{R}$-Algebra A bestimmt.
(d)* Implementieren Sie (c) in einem Computeralgebra-System.

Aufgabe 2. (Zerfällungskörper) Sei D eine K-Divisionsalgebra und L eine maximal kommutative Teilalgebra von D. Zeigen Sie
(a) $K \leq Z(D) \leq L$, $L = C_D(L)$ und L ist ein Körper.
(b) $L \otimes_{Z(D)} D \cong L^{n\times n}$ wobei n der Index von D als zentral einfache $Z(D)$-Algebra ist.
(c) Sei $D = \langle 1, i, j, k\rangle_{\mathbb{Q}}$ mit $i^2 = j^2 = k^2 = -1$, $k = ij$. Zeigen Sie dass D eine Divisionsalgebra ist und bestimmen Sie einen expliziten Isomorphismus wie in (b) für $L = \mathbb{Q}[i]$.
(d) Sei D wie in (c). Bestimmen Sie ein $a \in D^*$ mit $aia^{-1} = j$.
(e) Ist $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ eine Divisionsalgebra für $p = 2, 3, 5$?

Aufgabe 3. (Divisionsalgebren über p-adischen Zahlen)
Sei p eine Primzahl, $z \in \overline{\mathbb{Q}}_p$ ein primitive (p^2-1)-te Einheitswurzel und

$$Z := \begin{pmatrix} z & 0 \\ 0 & z^p \end{pmatrix},\ P := \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$$

Sei weiter $A = \langle I_2, Z, P, ZP\rangle_{\mathbb{Q}_p} \leq \mathbb{Q}_p[z]^{2\times 2}$.
(a) Zeigen Sie, dass A eine $\mathbb{Q}_p$-Divisionsalgebra ist.
(b) Bestimmen Sie einen expliziten Isomorphismus $\mathbb{Q}_p[z] \otimes_{\mathbb{Q}_p} A \to \mathbb{Q}_p[z]^{2\times 2}$.
(c) Zeigen Sie, dass jede quadratische Erweiterung von $\mathbb{Q}_p$ ein maximaler Teilkörper von A ist.

Aufgabe 4. Sei R ein Dedekindbereich mit Quotientenkörper K und V ein endlich dimensionaler K-Vektorraum. Sei L ein R-Gitter in V.
(a) Ist M ein R-Gitter in V, so gilt $M_\wp = L_\wp$ für fast alle maximalen Ideale $\wp \trianglelefteq R$.
(b) Sei für alle $\wp \trianglelefteq_{\max} R$ ein $R_\wp$-Gitter $X(\wp)$ in V gegeben so dass $X(\wp) = L_\wp$ für fast alle maximalen Ideale $\wp \trianglelefteq R$. Dann ist $M := \bigcap_\wp X(\wp)$ ein Gitter in V mit $M_\wp = X(\wp)$ für alle $\wp$.
(c) Ist $\wp$ ein maximales Ideal von R, so liefert die Abbildung $M \mapsto M_\wp$ eine Bijektion zwischen

$$\{M \leq L \mid L/M \text{ ist } \wp\text{-torsion}\} \to \{M \leq L_\wp \mid M \text{ volles Gitter }\}$$

(d) Die Mengen der $R_\wp$-Gitter in V und die der $\hat{R}_\wp$-Gitter in der Vervollständigung $\hat{K}_\wp \otimes V$ stehen in Bijektion.

Aufgabe 5. Sei R Dedekindbereich, $\wp \trianglelefteq R$ ein maximales Ideal und $S := (R - \wp)^{-1}R$ die Lokalisierung von R an $\wp$. Zeigen Sie:
Ist

$$0 \to A \xrightarrow{a} B \xrightarrow{b} C \to 0$$

eine kurze exakte Sequenz endlich erzeugter R-Moduln, so ist

$$0 \to S \otimes_R A \xrightarrow{id\otimes a} S \otimes_R B \xrightarrow{id\otimes b} S \otimes_R C \to 0$$

exakt. Kurz: Lokalisieren ist ein exakter Funktor.
Zeigen Sie auch dass Komplettieren ein exakter Funktor ist.

Aufgabe 6. (a) Sei Λ eine R-Maximalordnung in der separablen K-Algebra A. Dann ist der Matrixring $\Lambda^{n\times n}$ ein R-Maximalordnung in $A^{n\times n}$, insbesondere ist $R^{n\times n}$ eine R-Maximalordnung in $K^{n\times n}$.
(b) (unabhängig von (a)) Sei R ein Dedekindbereich und M ein volles R-Gitter in A. Dann ist $O_r(M) := \{a \in A \mid aM \subseteq M\}$ eine R-Ordnung in A.
Zeigen Sie, dass für jedes maximale Ideal $\wp \trianglelefteq R$ gilt

$$O_r(M_\wp) = O_r(M)_\wp \text{ und } O_r(\hat{M}_\wp) = \widehat{O_r(M)}_\wp.$$

Aufgabe 7. (Quaternionenalgebren) Sei K ein Körper der Charakteristik $\neq 2$ und D eine zentral einfache K-Algebra der Dimension 4. Zeigen Sie:
(a) Es gibt $a, b \in K^*$, $i, j \in D$ mit $i^2 = a$, $j^2 = b$, $ij = -ji$. Bezeichnung: $D = \left(\frac{a,b}{K}\right)$.
(b) Für die reduzierte Norm gilt $N(x + yi + zj + tij) = x^2 - ay^2 - bz^2 + (ab)t^2$.
(c) Die Abbildung $x + yi + zj + tij \mapsto x - yi - zj - tij$ ist ein K-Algebren Isomorphismus zwischen D und D^{op}.
(d) Ist D eine Divisionsalgebra, so hat $[D]$ Ordnung 2 in $\mathrm{Br}(K)$.
(e) $\left(\frac{a,b}{K}\right) \cong \left(\frac{\alpha,\beta}{K}\right)$ genau dann wenn die 3-dimensionalen quadratischen K-Vektorräume $(K^3, \mathrm{diag}(-a, -b, ab))$ und $(K^3, \mathrm{diag}(-\alpha, -\beta, \alpha\beta))$ isometrisch sind.
(f) $D^*/K^* \cong SO(\mathrm{diag}(-a, -b, ab)) = \{A \in \mathrm{SL}_3(K) \mid A\,\mathrm{diag}(-a, -b, ab)A^{tr} = \mathrm{diag}(-a, -b, ab)\}$

Aufgabe 8.
(a) $\left(\frac{a,b}{\mathbb{R}}\right)$ ist eine Divisionsalgebra, genau dann wenn $a < 0$ und $b < 0$.
(b) Sind $a, b \in \mathbb{Z}$, so ist $\Lambda := \langle 1, i, j, ij\rangle_\mathbb{Z}$ eine $\mathbb{Z}$-Ordnung in $\left(\frac{a,b}{\mathbb{Q}}\right)$. Bestimmen Sie $\Lambda^\#$ und $|\Lambda^\#/\Lambda|$.
(c) Zeigen Sie, dass für $a, b \in \mathbb{Z}$ die Hasse Invariante von $\left(\frac{a,b}{\mathbb{Q}}\right) \otimes \mathbb{Q}_p$ trivial ist, falls p kein Teiler von $2ab$ ist.
(d) Bestimmen Sie die Hasse Invarianten von $\left(\frac{a,b}{\mathbb{Q}}\right) \otimes \mathbb{Q}_p$ für alle p und folgende Paare (a, b): $(-1, -1)$, $(-1, -3)$, $(2, 5)$, $(-2, -5)$, $(-2, 5)$, $(2, -5)$.
(e) Sei $D = \left(\frac{-2,-5}{\mathbb{Q}}\right)$. Zeigen Sie, dass $E = \mathbb{Q}[\zeta_5]$ ein Zerfällungskörper für D ist, jedoch kein echter Teilkörper von E die Divisionsalgebra D zerfällt.

Aufgabe 9.
Sei $A = \langle 1, \rho, i, \rho i\rangle_\mathbb{Q} \cong \mathbb{Q}[\rho] \oplus \mathbb{Q}[\rho]i$, wo $\rho^2 + \rho + 3 = 0$, $i^2 = -1$, $(i\rho)^2 = -3$.
(a) Sei $\Lambda := \langle 1, \rho, i, \rho i\rangle_\mathbb{Z}$. Zeigen Sie, dass Λ eine Maximalordnung in A ist.
(b) Bestimmen Sie alle Hasse Invarianten von A.
(c) Sei $\Gamma = \langle 1, \rho + i, 2i, \frac{1+\rho i}{2}\rangle_\mathbb{Z}$. Zeigen Sie, dass Γ eine Maximalordnung ist.
(d) Bestimmen Sie die Einheitengruppen von Γ und von Λ und folgern Sie, dass Λ und Γ nicht isomorph sind.

Zyklische Algebren. Sei $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ zyklisch der Ordnung $n > 1$,

$$A := (L/K, \sigma, a) := \bigoplus_{j=0}^{n-1} u^j L,\ xu = ux^\sigma,\ u^n = a \in L^*.$$

Aufgabe 10. Sei $g : G \times G \to L^*$ ein normalisiertes Faktorensystem. Dann ist $(L/K, g) \cong (L/K, \sigma, a)$ wobei $a = \prod_{j=0}^{n-1} g_{\sigma,\sigma^j} \in K^*$.
Folgern Sie, dass $H^2(G, L^*) \cong K^*/N_{L/K}(L^*)$. Der Exponent von $H^2(G, L^*)$ teilt also insbesondere die Ordnung von G.

Aufgabe 11. Seien $a, b \in K^*$.
(a) $(L/K, \sigma, a) \cong (L/K, \sigma^s, a^s)$ für alle $s \in \mathbb{Z}$, $\mathrm{ggT}(s, n) = 1$.
(b) $(L/K, \sigma, 1) \cong K^{n\times n}$.
(c) $(L/K, \sigma, a) \cong (L/K, \sigma, b) \Leftrightarrow b = N_{L/K}(c)a$ für ein $c \in L^*$.
(d) $(L/K, \sigma, a) \otimes_K (L/K, \sigma, b) \cong (L/K, \sigma, ab)^{n\times n}$.
(e) Jedes $[A] \in \mathrm{Br}(L/K)$ hat eine Ordnung, die n teilt.

Aufgabe 12.
(a) Sei E/K weitere Körpererweiterung, $F := E \cap L$, $G = \langle\sigma\rangle = \mathrm{Gal}(L/K)$, $H := \langle\sigma^k\rangle = \mathrm{Gal}(L/F) = \mathrm{Gal}(EL/E)$.
Dann ist $E \otimes_K (L/K, \sigma, a) \cong (EL/E, \sigma^k, a)$.
(b) Sei $E \underbrace{\supseteq}_{r} L \underbrace{\supseteq}_{s} K$, $G = \mathrm{Gal}(E/K) = \langle\sigma\rangle$, $H = \mathrm{Gal}(E/L) = \langle\sigma^r\rangle$, $\overline{G} = \mathrm{Gal}(L/K) = \langle\sigma H = \overline{\sigma}\rangle = G/H$.
Für alle $a \in K^*$ ist $(L/K, \overline{\sigma}, a) \sim (E/K, \sigma, a^r)$.

Aufgabe 13. Sei $\mathcal{A}$ eine $\mathbb{Q}$-Algebra, $\mathcal{A} := \langle\alpha, \tau\rangle_{\mathbb{Q}-Alg.}$ mit $\alpha^4 + 4\alpha^2 + 2 = 0, \tau^4 = 2, \tau\alpha\tau^{-1} = 3\alpha + \alpha^3$.
Schreiben Sie $\mathcal{A}$ als $\mathbb{Q}$-Teilalgebra von $\mathbb{Q}[a]^{4\times4}$, mit $a^4 + 4a^2 + 2 = 0$.
Zeigen Sie $\mathcal{A} \cong \mathbb{Q}^{4\times4}$.
(Hinweis: $\mathbb{Q}[a] \to \mathbb{Q}[a] : a \mapsto 3a + a^3$ erzeugt $\mathrm{Gal}(\mathbb{Q}[a]/\mathbb{Q})$ und $N(a) = 2$.)

Aufgabe 14. Sei $K := \mathbb{Q}[\sqrt{-7}]$. Bestimmen Sie eine zentrale K-Divisionsalgebra D mit Hasse Invarianten $\frac{1}{3}$ und $\frac{2}{3}$ an den beiden Primstellen über 2 und 0 an allen anderen Stellen. Bestimmen Sie D^{op}.
Hinweis: $\mathbb{Q}[\zeta_7]$ ist ein maximaler Teilkörper von D.
Ist $[D]$ im Bild von $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(K)$?

Aufgabe 15. Sei $\mathcal{A}$ eine $\mathbb{Q}$-Algebra, $\mathcal{A} := \langle\alpha, \tau\rangle_{\mathbb{Q}-Alg.}$ mit $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0, \tau^4 = 2, \tau\alpha\tau^{-1} = \alpha^2$.

(i) Bestimmen Sie Matrizen in $\mathbb{Q}[\zeta_5]^{4\times4}$ (ζ_5 bezeichne eine primitive 5-te Einheitswurzel), welche die Relationen von α und τ erfüllen und eine zu $\mathcal{A}$ isomorphe $\mathbb{Q}$-Teilalgebra von $\mathbb{Q}[\zeta_5]^{4\times4}$ erzeugen. Zeigen Sie, daß $\mathcal{A}$ zentral einfache $\mathbb{Q}$-Algebra ist.

(ii) Zeigen Sie: $\mathbb{Q}_2 \otimes_{\mathbb{Q}} \mathcal{A}$ hat Schurindex 4 und bestimmen Sie die Hasseinvariante von $\mathbb{Q}_2 \otimes_{\mathbb{Q}} \mathcal{A}$.
(Hinweis: $\mathbb{Q}_2[\alpha]$ ist unverzweigt über $\mathbb{Q}_2$.)

(iii) Sei $\Lambda := \mathbb{Z}[\alpha, \tau] \leq \mathcal{A}$. Bestimmen Sie die Diskriminante von Λ bzgl. der reduzierten Spur.

(iv) Folgern Sie aus (iii) dass $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{A} \cong \mathbb{Q}_p^{4\times4}$ für alle Primzahlen $p \neq 2, 5.$ und dass $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \Lambda$ die Maximalordnung in $\mathbb{Q}_2 \otimes_{\mathbb{Q}} \mathcal{A}$ ist.

(v) Geben Sie einen Epimorphismus $\mathbb{Z}_5 \otimes_{\mathbb{Z}} \Lambda \to \mathbb{F}_{5^4}$ an und schließen Sie mit (iii), daß $\mathbb{Q}_5 \otimes_{\mathbb{Q}} \mathcal{A}$ eine Divisionsalgebra ist.
(Hinweis: $\tau \mapsto 2^{\frac{1}{4}}, \alpha \mapsto 1$.)

(vi) Bestimmen Sie die Hasseinvariante von $\mathbb{Q}_5 \otimes_{\mathbb{Q}} \mathcal{A}$.
(Hinweis: $\pi_{\mathcal{A}} := \alpha - 1$ erzeugt das maximale Ideal $J(\mathbb{Z}_5 \otimes_{\mathbb{Z}} \Lambda)$ von $\mathbb{Z}_5 \otimes_{\mathbb{Z}} \Lambda$, und $\mathbb{Q}_5[\tau]$ ist ein über $\mathbb{Q}_5$ unverzweigter maximaler Teilkörper von $\mathbb{Q}_5 \otimes_{\mathbb{Q}} \mathcal{A}$. Berechnen Sie die Potenz des Frobeniusautomorphismus, welche $\pi_{\mathcal{A}}$ auf $\mathbb{Z}_5 \otimes_{\mathbb{Z}} \Lambda / J(\mathbb{Z}_5 \otimes_{\mathbb{Z}} \Lambda) \cong \mathbb{F}_5 \otimes_{\mathbb{Z}_5} \mathbb{Z}_5[\tau] \cong \mathbb{F}_{5^4}$ induziert.)

(vii) Zeigen Sie $\mathbb{R} \otimes_{\mathbb{Q}} \mathcal{A} \cong \mathbb{R}^{4\times 4}$.

Aufgabe 16. Ein **Absolutbetrag** eines Schiefkörpers K ist eine Funktion $|\cdot| : K \to \mathbb{R}$ mit
(i) $|x| \geq 0$ und $|x| = 0 \Leftrightarrow x = 0$. (ii) $|xy| = |x||y|$. (iii) $|x + y| \leq |x| + |y|$.
Zwei Beträge $|\cdot|_1$ und $|\cdot|_2$ heissen **äquivalent**, wenn sie dieselbe Topologie definieren.
(a) Zeigen Sie: $|\cdot|_1$ und $|\cdot|_2$ sind genau dann äquivalent, wenn es ein $s \in \mathbb{R}_{>0}$ gibt mit $|x|_1 = |x|_2^s$ für alle $x \in K$.
(b) Zeigen Sie: $|\cdot|_1$ und $|\cdot|_2$ sind genau dann äquivalent, wenn für alle $x \in K$ gilt $|x|_1 < 1$ $\Rightarrow |x|_2 < 1$.
(c) (Der schwache Approximationssatz) Sind $|\cdot|_i$ paarweise inäquivalente Beträge von K $(i = 1, \ldots, n)$ und $a_1, \ldots, a_n \in K$ gegeben, so gibt es zu jedem $\epsilon > 0$ ein $x \in K$ mit $|x - a_i|_i < \epsilon$ für alle $i = 1, \ldots, n$.
(Hinweis: Kap. II Abschnitt 3 in Neukirch, algebraische Zahlentheorie.)
(d) Verschiedene Stellen eines algebraischen Zahlkörpers K definieren inäquivalente Beträge.
(e) Der (sehr) starke Approximationssatz sagt aus, dass für globale Körper K unter der Voraussetzung von (c) und der zusätzlichen Annahme, dass $|\cdot|_0$ eine von $|\cdot|_1, \ldots, |\cdot|_n$ verschiedene Stelle von K gegeben ist, ein $x \in K$ gefunden werden kann, das $|x - a_i|_i < \epsilon$ erfüllt für alle $i = 1, \ldots, n$ und $|x|_k \leq 1$ für alle Stellen $|\cdot|_k \neq |\cdot|_i$ $(i = 0, \ldots, n)$, also x ganz ist bei allen anderen Stellen (ausser einer vorgegebenen $|\cdot|_0$).

Aufgabe 17. (Steinitzinvariante) R sei ein Dedekindbereich, J_i, I_k gebrochene Ideale. Dann gilt:

$$J_1 \oplus \ldots \oplus J_n \cong I_1 \oplus \ldots \oplus I_m \Leftrightarrow n = m \text{ und } J_1 \cdots J_n \cong I_1 \cdots I_m$$

in der Idealklassengruppe von R. Folgern Sie, dass die multiplikative Idealklassengruppe von R und die additive Idealklassengruppe von R isomorph sind.

Aufgabe 18. Sei L/K eine endliche Erweiterung algebraischer Zahlkörper, $R = \mathbb{Z}_K$, $S = \mathbb{Z}_L$. Sei Λ eine Maximalordnung in einer zentral einfachen L-Algebra A. Für ein Primideal $P \trianglelefteq R$ sei $PS = P_1^{e_1} \cdots P_d^{e_d}$. Sei $\wp_i$ das Primideal von Λ das $P_i\Lambda$ enthält. Dann ist $P_i\Lambda = \wp_i^{m_i}$ wobei $\hat{A}_{P_i} = D_i^{k_i \times k_i}$ und $[D_i : L_{P_i}] = m_i^2$. Weiter ist $P\Lambda = \prod_{i=1}^{d} \wp_i^{e_i m_i}$ und

$$\Lambda^{\#} := \{a \in A \mid trace(a\Lambda) \subseteq S\} = \prod_{P_i \trianglelefteq_{max} S} \wp_i^{1-m_i}\Lambda$$

Definite Quaternionenalgebren: Mit $\mathcal{Q}_{\alpha,p_1,\ldots,p_s}$ bezeichnen wir die definite Quaternionenalgebra mit Zentrum $K := \mathbb{Q}[\alpha]$ (ein total reeller Zahlkörper) die unter Vervollständigung an der Stelle $\wp$ genau dann eine Divisionsalgebra ist, wenn $\wp$ eine der Stellen p_i ist.

Aufgabe 19.

a) Sei K ein imaginär quadratischer Zahlkörper. Zeigen Sie dass $\mathbb{Z}_K^* = \langle -1 \rangle$ außer für $K = \mathbb{Q}[\sqrt{-1}]$ und $K = \mathbb{Q}[\sqrt{-3}]$, wo $\mathbb{Z}_K^* \cong C_4$ resp. C_6.

b) Zeigen Sie, dass $\mathcal{Q}_{\infty,3}$ Typenzahl und Klassenzahl 1 hat. Die Maximalordnung dieser Divisionsalgebra ist ein (Links) Euklidischer Bereich.

c) Bestimmen Sie die Klassenzahl und Typenzahl der Quaternionenalgebra $\mathcal{Q}_{\infty,13}$.

d) Bestimmen Sie die Klassenzahl und Typenzahl der Quaternionenalgebra $\mathcal{Q}_{\infty,2,5,7}$.

Aufgabe 20. Bestimmen Sie (mit einem CAS, z.B. Magma) Klassenzahl, Typenzahl, das Brandtsche Gruppoid, Vertreter der Konjugiertenklassen von Maximalordnungen für die Quaternionenalgebra $\mathcal{Q}_{\sqrt{7},\infty,\infty}$.
Hinweis: $\zeta_K(-1) = \frac{2}{3}$ und die Klassenzahl $h(\mathbb{Z}_K) = 1$ für $K = \mathbb{Q}[\sqrt{7}] = Z(\mathcal{Q})$.

Aufgabe 21. Zeigen Sie, dass für jede Maximalordnung Λ_i die Ordnung der Automorphismengruppe des $\mathbb{Z}_K$-Gitters (Λ_i, N) gegeben ist als

$$|\operatorname{Aut}(\Lambda_i, N)| = \underbrace{\omega_i^1}_{left\ mult.} \underbrace{\omega_i 2^s H_i^{-1}}_{\kappa(normalizer)} \cdot \underbrace{2}_{-1} \cdot \underbrace{2}_{quat.conj.} .$$