We want to collect some standard facts from commutative algebra. Here we will be rather sketchy because many good references are available. Some of the proofs are outlined in exercises.

0.1 Localization

We consider commutative rings with identity A,B homomorphisms between rings send the identity to the identity. If R is a ring and $\phi : R \longrightarrow A$ is a homomorphism, then we say that A is a R-algebra.

We define $\mathrm{Spec}(A)$ as the ordered set of prime ideals of A.
If A is a field then $\mathrm{Spec}(A)$ consists of one element, namely the ideal (0).

For any A with $1_A \neq 0$ we have $\mathrm{Spec}(A) \neq \emptyset$
An ideal $\mathfrak{m} \subset A,(1_A \notin A)$ is called maximal if one of the two equivalent conditions is satisfied
a) There is no ideal $\mathfrak{a} \supset \mathfrak{m},1_A \notin \mathfrak{a},\mathfrak{a} \neq \mathfrak{m}$
b) The residue ring $A/\mathfrak{m}$ is a field
(needs Zorns lemma)

Let $S \subset A$ be a subset, which is closed under multiplication and we have $0 \notin S,1_A \in S$ then we can form the quotient ring

$$A_S = \{\frac{a}{s} \mid a \in A,s \in S : \frac{a_1}{s_1} = \frac{a_2}{s_2} \iff \exists s \in S \text{ such that } s(s_2a_1 - s_1a_2) = 0\}$$

We can make an analogous definition for any A-module M

$$M_S = \{\frac{m}{s} \mid m \in A,s \in S : \frac{m_1}{s_1} = \frac{m_2}{s_2} \iff \exists s \in S \text{ such that } s(s_2m_1 - s_1m_2) = 0\}$$

If $\mathfrak{p}$ is a prime ideal in A then we can consider the set $S_\mathfrak{p} = A \setminus \mathfrak{p}$. By definition of prime ideal this set is closed under multiplication. Then the quotient ring $A_{S_\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}_{S_\mathfrak{p}}$.
Here we simplify the notation: We put

$$A_\mathfrak{p} := A_{S_\mathfrak{p}},\mathfrak{p}_{S_\mathfrak{p}} := \mathfrak{p}_\mathfrak{p} \text{ or simply } := \mathfrak{p}$$

The radical

$$\mathrm{Rad}(A) = \cap_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$$

can also be defined as the ideal of nilpotent elements i.e. those elements $f \in A,\exists n \in \mathbb{N}$ such that $f^n = 0$.
An example: Let $A = \mathbb{Z}$ and let p be a prime number. Then the principal ideal (p) is a maximal prime ideal and we define

$$\mathbb{Z}_{(p)} = \{\frac{a}{b}|a,b \in \mathbb{Z},b \notin (p)\}$$

this is the first example of a discrete valuation ring.
A ring is called *reduced* if its radical $\mathrm{Rad}(A) = 0$.

Proposition 0.1.1. *If the radical of A is a finitely generated ideal then there exists a number $n \in \mathbb{N}$ such that the product of any n elements in $\mathrm{Rad}(A)$ is equal to zero, i.e. $\mathrm{Rad}(A)^n = 0$. The descending chain*

$$\mathrm{Rad}(A) \supset \mathrm{Rad}(A)^2 \supset \cdots \supset \mathrm{Rad}(A)^n = (0)$$

stops at zero after a finite number of steps.

0.2 Finite A-Algebras

Definition 0.2.1. *An A-module M is called* **finitely generated** *if there are elements $m_1, m_2, \ldots, m_r \in B$ such that for any $m \in M$ we can find $a_i \in A$ such that $m = a_1 m_1 + \ldots + a_r m_r$.*

If $\phi : A \longrightarrow B$ is a homomorphism of rings, then we say that an element $b \in B$ **is integral over** A if it is the zero of a monic polynomial, i.e. we can find a polynomial (with highest coefficient equal to 1)

$$P(X) = a_0 + a_1 X \ldots + X^n \in A[X] \tag{0.1}$$

such that

$$P(b) = \varphi(a_0) + \varphi(a_1)b + \ldots + b^n = 0. \tag{0.2}$$

Definition 0.2.2. *A morphism $\phi : A \to B$ between two commutative rings is called* **finite** *if one of the following two equivalent conditions is satisfied*

1. *The A-module B is finitely generated.*
2. *The A-algebra B is finitely generated and all elements of B are finite over A.*

It is immediately clear that 2. implies 1. because we can use the polynomials to reduce the degree of the generating monomials. The proof that 1. implies 2. is amusing, we leave it as an exercise. (See also [Ei], Chap. I section 4 and [At-McD]). The following exercise gives a hint.

Exercise 1.

1. We have to show that any $b \in B$ is a zero of a monic polynomial in $A[X]$, i.e. it is integral over A. To see this we multiply the generators b_i by b and express the result again as A-linear combination of the b_i. This gives us an $r \times r$-matrix M with coefficients in A. If $\underline{b}$ is the column vector formed by the b_i we get a relation $b\underline{b} = M\underline{b}$ or $(M - b\,\mathrm{Id})\underline{b} = 0$. From this we have to conclude that $\det(M - b\,\mathrm{Id}) = 0$. This is clear if A is integral, but it suffices to know that the identity of B is contained in the module generated by the b_i, I refrain from giving a hint. Hence we see that b is a zero of the characteristic polynomial of the matrix M, but this polynomial equation has highest coefficient 1 and the other coefficients are in A.
2. This argument generalizes: Let us consider any A-algebra $A \to B$, but assume that B is integral. Show that an element $b \in B$ is integral over A if we can find a finitely generated A-submodule $Y \subset B, Y \neq 0$, which is invariant under multiplication by b, i.e. $bY \subset Y$.

If we have a morphism $\phi : A \longrightarrow B$, then the **integral closure** of A in B consists of all those elements in B, which are integral over A. It is an easy consequence of the two exercises above that the integral closure is an A-sub algebra of B. (For two integral elements b_1,b_2 consider the finitely generated module $\{b_1^\nu b_2^\mu\}$.)

Definition 0.2.3. *An ring A is* **normal** *if it is integral an if it is equal to its integral closure in its quotient field K, i.e. if any element $x \in K$, which is integral over A is already in A. For any integral ring A the integral closure of A in its quotient field is called the* **normalization.**

Synonymously we use the terminology A **is integrally closed** for A is normal.

Definition 0.2.4. *An element a in an integral ring A is* **irreducible** *if it is not a unit and if in any multiplicative decomposition $a = bc$ one of the factors is a unit. An integral ring A is called* **factorial** *if any element $x \in A$ has a finite decomposition $x = x_1 \dots x_n$ into irreducible elements, where the irreducible factors are unique up to units and permutations.*

Exercise 2. 1. Show that a factorial ring is normal.

2. Show that an integral ring is factorial if for any irreducible element $\pi \in A$ the principal ideal (π) is a prime ideal.

3. Show that for any factorial ring A the polynomial ring $A[X]$ is again factorial. (This is essentially due to Gauss)

   Hint: Let K be the field of fractions. Let $P(X) = a_0+a_1X+\cdots+a_nX^n \in A[X]$,$a_n \neq 0$. Assume that this polynomial splits in $K[X]$. Then we find a $c \in A$,$c \neq 0$ such that we can factorize

   $$ca_0 + ca_1X + \cdots + ca_nX^n = (b_0 + b_1X + \cdots + b_rX^r)(c_0 + c_1X + \cdots + c_sX^s)$$

   into a product of two polynomials in$A[X]$ of smaller degree. Now use 2) to show that for any irreducible divisor π of c one of the factors must be zero $\mod (\pi)$, hence we can divide on both sides by π. This process stops. Therefore we see that a polynomial in $A[X]$, which becomes reducible in $K[X]$ is also reducible in $A[X]$. Then the rest is clear.

4. Show that the ring of integers $\mathbb{Z}$ and the ring $k[X]$ of polynomials over a field k are normal.

5. Let us assume that $A \longrightarrow B$ are both integral and that $K \to L$ is the corresponding extension of their quotient fields. Let us assume that L/K is a finite extension. Furthermore we assume that A normal. For $x \in L$ we have a unique monic polynomial of minimal degree $P(X) \in K[X]$ such that $P(x) = 0$. The multiplication by x induces a linear transformation l_x of the K-vector space L. It is well known that x is a zero of the characteristic polynomial $\det(X\,\mathrm{Id} - l_x)$ of l_x. Show that

   $$x \text{ is integral over } A \Longleftrightarrow P[X] \in A[X] \Longleftrightarrow \det(XId - l_x) \in A[X]$$

   Hint: The polynomial $P(X)$ is called the minimal polynomial of x. Look at the K-algebra homomorphisms σ from L into an algebraic closure $\bar{K}$ of K (See (0.3). Galois theory tells us how the coefficients of $P(X)$ can be expressed in terms of the symmetric functions of the $\sigma(x)$. From this we see that the coefficients are in K and they are integral over A. Hence they are in A.

To finish the argument we have to relate $P(X)$ and the characteristic polynomial.

6. Under the above assumptions we have $\mathrm{tr}_{L/K}(x) \in A$ for any element $x \in L$, which is integral over A.

7. Again under the assumptions of 3. we can say: For any $x \in L$ we can find a non zero element $a \in A$ such that ax becomes integral over A

8. If an A module M is locally free of rank of one then we can find a finite covering $X = \mathrm{Spec}(A) = \bigcup X_{f_i}$,$X_{f_i} = \mathrm{Spec}(A_{f_i})$ such that $M \otimes A_{f_i}$ is free of rank one, i.e. $M \otimes A_{f_i} = A_{f_i} s_i$, where $s_i \in M$.

   Show that this implies that M is isomorphic to an ideal $\mathfrak{a}$, which is locally principal.

   Show that for a factorial ring A any locally principal ideal $\mathfrak{a} \subset A$ is itself principal Hint: Show that either $\mathfrak{a} = A$ or we can find an irreducible element π, which divides all elements of $\mathfrak{a}$ and hence $\mathfrak{a} \ \subset \pi^{-1}\mathfrak{a} \subset A$. The ideal $\pi^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$. We apply the same argument to $\pi^{-1}\mathfrak{a}$ and get get an ascending chain of locally principal ideals. This chain has to stop because a non zero element of $\mathfrak{a}$ has only finitely many irreducible divisors.

   This implies that any locally free module of rank one over a factorial ring is free (See [Ma], Thm. 20.7)

The item (3) in the exercise above implies the following theorem, which we will use several times (See for instance [J-S], Chap. IV, Satz 4.4.)

Theorem 0.2.5. *For any factorial ring A the polynomial ring $A[X_1,X_2,\ldots,X_n]$ is factorial.*

We have the following fundamental theorem for finite morphisms

Theorem 0.2.6 (Going up and down)**.** *Assume that the ring homomorphism $\phi : A \to B$ is finite and injective. Then the induced map ${}^t\phi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective, has finite fibers and the elements in the fibers are incomparable with respect to the order on* $\mathrm{Spec}(B)$.

This means in other words: For any $\mathfrak{p} \in \mathrm{Spec}(A)$ we can find a $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $A \cap \mathfrak{q} = \mathfrak{p}$. The number of such $\mathfrak{q}$ is finite, whenever we have two of them $\mathfrak{q}_1$,$\mathfrak{q}_2$ we have $\mathfrak{q}_1 \not\subset \mathfrak{q}_2$. (See [Ei], I. 4.4,prop. 4.15, cor. 4.18)
To prove the theorem we need another famous result from commutative algebra, namely the Lemma of Nakayama.

Lemma 0.2.7. *[Nakayama] Let A be a local ring with maximal ideal $\mathfrak{m}$ and let M be a finitely generated A-module. If*

$$M \otimes (A/\mathfrak{m}) = M/\mathfrak{m}M = 0$$

then $M = 0$.

To see this we use the same trick as above: Express a system of generators of M as a linear combination of these generators but now with coefficients in $\mathfrak{m}$. We find that 1_A is a zero of a characteristic polynomial of a matrix with coefficients in $\mathfrak{m}$, which is only possible for the 0×0 -matrix. □

Now we sketch the proof of the going up and down theorem. We pick a prime $\mathfrak{p} \in \operatorname{Spec}(A)$. The residue class ring $A/\mathfrak{p}$ is integral, we have $\operatorname{Spec}(A/\mathfrak{p}) \hookrightarrow \operatorname{Spec}(A)$ and the zero ideal (0) is mapped to $\mathfrak{p}$. We localize at (0) and we get the quotient field $(A/\mathfrak{p})_{(0)}$. Taking fibered products we get a diagram of affine schemes

$$\begin{tikzcd}
\operatorname{Spec}(A) & \operatorname{Spec}(B) \arrow[l] \\
\operatorname{Spec}(A/\mathfrak{p}) \arrow[u] & \operatorname{Spec}(B \otimes_A (A/\mathfrak{p})) \arrow[l] \arrow[u] \\
\operatorname{Spec}(A/\mathfrak{p})_{(0)} \arrow[u] & \operatorname{Spec}(B \otimes_A (A/\mathfrak{p})_{(0))} \arrow[l] \arrow[u]
\end{tikzcd}$$

The vertical arrows are inclusions and it is clear that the prime ideals $\mathfrak{q} \in \operatorname{Spec}(A)$, for which $\mathfrak{q} \cap A$ are exactly the elements in $\operatorname{Spec}(B \otimes_A (A/\mathfrak{p})_{(0)})$. To prove the surjectivity we have to show that this scheme is not empty. This follows from the lemma of Nakayama because we can obtain $\operatorname{Spec}(A/\mathfrak{p})_{(0)}$ also as the residue field $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ of the local ring $A_\mathfrak{p}$. We have $B \otimes_A A_\mathfrak{p} \neq 0$ (only the zero divisors of $S = A \setminus \mathfrak{p}$ go to zero in this tensor product) and hence we get by Nakayama that $B \otimes_A A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \neq 0$ and this implies $\operatorname{Spec}(B \otimes_A A_\mathfrak{p}/\mathfrak{m}_p) \neq \emptyset$. Now we have that $B \otimes_A (A/\mathfrak{p})_{(0)}$ is a finite dimensional vector space over the field $(A/\mathfrak{p})_{(0)}$, it is a finite $(A/\mathfrak{p})_{(0)}$-algebra. This implies that any prime ideal $\mathfrak{q} \in \operatorname{Spec}(B \otimes_A (A/\mathfrak{p})_{(0)})$ is maximal because the residue ring is automatically a field. Then it is also clear that $\operatorname{Spec}(B \otimes_A (A/\mathfrak{p})_{(0)})$ must be finite. The map

$$B \otimes_A (A/\mathfrak{p})_{(0)} \longrightarrow \prod_\mathfrak{q} B \otimes_A (A/\mathfrak{p})_{(0)}/\mathfrak{q}$$

is easily seen to be surjective. Hence we have proved that the fibers are finite and non empty and we have seen that the prime ideals in the fibers are incomparable.

0.2.1 Rings With Finiteness Conditions

In this section formulate some finiteness for rings collect some facts about these rings. We will not give proofs because these facts are easily available in the literature. On the other hand it may be a good exercise if the reader tries to find the proofs her(him)self.

Definition 0.2.8. *A commutative ring A with identity is called* **noetherian** *if it satisfies one of the following equivalent four conditions*

1. *Any ideal $\mathfrak{a} \subset A$ is finitely generated.*
2. *Any submodule N of a finitely generated A-module M is finitely generated.*
3. *Any ascending chain $\mathfrak{a}_\nu \subseteq \mathfrak{a}_{\nu+1} \subseteq \dots \mathfrak{a}_n \subseteq \dots$ becomes stationary, i.e. there exists an n_0 such that $\mathfrak{a}_{n_0} = \mathfrak{a}_{n_0+1} \dots = \mathfrak{a}_{n_0+m}$ for all $m \geq 0$.*
4. *Any ascending chain of A-submodules $N_\nu \subseteq N_{\nu+1} \subseteq \dots$ of a finitely generated A-module M becomes stationary.*

Example 1. *The ring $\mathbb{Z}$ is noetherian and of course we know that fields are so too.*

Theorem 0.2.9 (E. Lasker)**.** *Let A be a reduced noetherian ring. Then the set of minimal prime ideals is finite. To any minimal prime ideal $\mathfrak{p}$ we can find an $f \in A \setminus \mathfrak{p}$ such that*

$$\mathfrak{p} = \operatorname{Ann}_A(f) = \{x \in A | xf = 0\}.$$

I want to indicate the steps of the proof and leave it to the reader to fill the gaps.

Exercise 3. We prove that there exist minimal prime ideals. This is clear if A is integral. If not, then we find $f, g \in A \setminus \{0\}$ such that $fg = 0$.

1a) Consider $\operatorname{Ann}_A(f) = \mathfrak{a}$ and prove: If $\mathfrak{a}$ is not prime then we can find an $x \in A$ such that $f_1 = xf \neq 0$ and such that $\mathfrak{a}_1 = \operatorname{Ann}_A(f_1)$ is strictly larger than $\mathfrak{a} = \operatorname{Ann}_A(f)$.

1b) Show that this implies that we can find an $y \in A$ such that $\operatorname{Ann}_A(fy) = \mathfrak{p}$ is a prime ideal and that this prime ideal is minimal. Hence we see that minimal primes exist.

Let us write $yf = f_\mathfrak{p}$. It is clear that $f_\mathfrak{p} \notin \mathfrak{p}$.

Exercise 4. Prove that any prime ideal $\mathfrak{q}$ contains a minimal prime ideal $\mathfrak{p} \subset \mathfrak{q}$ of the form $\operatorname{Ann}_A(f_\mathfrak{p})$ and hence all minimal prime ideals are of this form.

Let us assume we picked an $f_\mathfrak{p}$ for any minimal prime ideal.

Exercise 5. Prove that for two minimal prime ideals $\mathfrak{p} \neq \mathfrak{p}_1$ the product $f_\mathfrak{p} f_{\mathfrak{p}_1} = 0$.

Exercise 6. Consider the ideal generated by these $f_\mathfrak{p}$ and combine the fact that this ideal is finitely generated and Exercise 5 above to show that these $f_\mathfrak{p}$ form a finite set.

Exercise 7. Let A be an arbitrary noetherian ring, let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the set of minimal prime ideals. Let us also assume that the spaces $\operatorname{Spec}(A/\mathfrak{p}_i)$ are disjoint. Then there is a unique collection of elements $e_1, \dots, e_r$ such that

$$\begin{aligned} e_i \notin \mathfrak{p}_i \text{ and } e_i \in \mathfrak{p}_j & & \text{for all } j \neq i \\ e_i^2 =& e_i & \text{for all } i \\ e_i e_j =& 0 & \text{for all } i \neq j \\ \sum_{i=1}^{r} e_i =& 1_A & \end{aligned}$$

(See [Ei], I. 7.3.) We give a hint for the solution. Our assumption that the spaces $\operatorname{Spec}(A/\mathfrak{p}_i)$ are disjoint implies that we can find e_i' such that $e_i' \equiv 1 \mod \mathfrak{p}_i$ and $e_i \in \mathfrak{p}_j$ for all $j \neq i$. These e_i' satisfy all the relations if we compute modulo the radical $\operatorname{Rad}(A)$. Now we can modify $e_i' \to e_i' + r_i = e_i$ such that we have the idempotency $e_i^2 = e_i$. (Use the next exercise to show that $\sum_i e_i'$ is a unit.) Then all the other requirements are also fulfilled.

Exercise 8. If we have any noetherian ring R and if we consider the homomorphism $R \longrightarrow R/\operatorname{Rad}(R)$ then the group $R^\times$ of units of R is the inverse image of the units in $R/\operatorname{Rad}(R)$

This decomposition of $1_A = e_1 + \ldots + e_r$ is called the decomposition into orthogonal idempotents. It gives a decomposition of the ring

$$A = \bigoplus_i Ae_i$$

If our ring has no radical, the $f_{\mathfrak{p}_i} = u_i e_i$ where u_i is a unit in Ae_i .

0.3 Low Dimensional Rings

A noetherian ring is of dimension zero if every prime ideal is maximal (and minimal). In this case it is clear from Theorem 0.2.9 that $\mathrm{Spec}(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ is a finite set. Then the local rings $A_{\mathfrak{p}_i}$ are also of dimension zero and $A_{\mathfrak{p}_i}$ has only one prime ideal, which we call $\mathfrak{m}_{\mathfrak{p}_i}$ and hence $\mathfrak{m}_{\mathfrak{p}_i}$ is also the radical of this local ring. We get an isomorphism

$$A \longrightarrow \bigoplus_{i=1}^{t} A_{\mathfrak{p}_i} = \bigoplus_{i=1}^{t} Ae_{\mathfrak{p}_i}.$$

The $e_{\mathfrak{p}_i}$ are the idempotents (See Exercise 1 (5)).

Definition 0.3.1. *A ring is called* **artinian** *if any descending chain of ideals becomes stationary.*

The rings $A_{\mathfrak{p}_i}$ are local artinian and hence A is also artinian.

Finite k-Algebras

If k is a field, then a finite k-algebra A is a k-algebra, which is finite dimensional as a k-vector space. Then it is clear that this is a zero dimensional k-algebra and hence we apply step 5) in the proof of Theorem 0.2.9, we get $A \xrightarrow{\sim} \bigoplus Ae_\nu$, where the the Ae_ν are local finite (artinian) k-algebras. The k-algebra structure of Ae_ν is given by the injection $i_\nu : x \mapsto xe_\nu$.
Such a finite k-algebra A is called absolutely reduced or separable, if $A \otimes_k \overline{k}$ does not contain nilpotent elements. This is clearly equivalent to

$$A \otimes_k \overline{k} \xrightarrow{\sim} \bigoplus_{i=1}^{\dim A} \overline{k}. \tag{0.3}$$

The set of indices in this decomposition can be identified to the set $\mathrm{Hom}_k(A,\bar{k})$ of k-algebra homomorphisms $\phi : A \longrightarrow \bar{k}$, (i.e. we have $\phi(x+y) = \phi(x) + \phi(y)$,$\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ and for $a \in k$,$x \in A$ we $\phi(ax) = a\phi(x)$): For any index we have the projection homomorphism $p_\nu : \bigoplus_{i=1}^{\dim A} \overline{k} \longrightarrow \bar{k}$ to the $\nu-$th coordinate, the composition $A \longrightarrow A \otimes_k \overline{k} \xrightarrow{p_\nu} \bar{k}$ is a k-algebra homomorphism from A to $\bar{k}$. They are all different and we get all the elements of $\mathrm{Hom}_k(A,\bar{k})$ this way. (See formula below)

We have a simple criterion for separability. To formulate this criterion, we define the trace $\mathrm{tr}_{A/k} : A \longrightarrow k$. To any element $x \in A$ we consider the linear endomorphism $L_x : y \mapsto xy$ and we put $\mathrm{tr}_{A/k}(x) = \mathrm{tr}(L_x)$. Then it is clear that:

Proposition 0.3.2. *The finite k-algebra A is separable if and only if the bilinear map $(x,y) \mapsto tr_{A/k}(xy)$ from $A \times A$ to k is non degenerate.*

To see that this is so one has to observe that degeneracy or non degeneracy are preserved, if we extend k to $\overline{k}$. For a nilpotent element $x \in A \otimes_k \overline{k}$ we have $\mathrm{tr}_{A \otimes_k \overline{k}/\overline{k}}(xy) = 0$ for all y. If we have a finite separable k-algebra A then we have

$$A \otimes_k \overline{k} = \oplus_{\mathrm{Hom}_k(A,\overline{k})} \overline{k}$$

where the isomorphism is given by $x \otimes a \mapsto \sum_{\sigma \in \mathrm{Hom}_k(A,\overline{k})} \sigma(x)a$. The linear map L_x is diagonal with eigenvalues $\sigma(x)$. Therefore we get the formula

$$\mathrm{tr}_{A/k}(x) = \sum_{\sigma \in \mathrm{Hom}_k(A,\overline{k})} \sigma(x) \tag{0.4}$$

for the trace. (This is the well know formula from an elementary course in algebra, which says that the trace of an element is the sum of its conjugates.)
At this point I recall an important fact from Galois theory: The elements $\sigma \in \mathrm{Hom}_k(A,\bar{k})$ can also be viewed as elements in $\mathrm{Hom}_{k,\text{vector-space}}(A,\bar{k})$. We have theorem of *linear independence auf automorphisms*

Theorem 0.3.3. *The elements $\sigma \in \mathrm{Hom}_{k,vector\text{-}space}(A,\bar{k}) = \mathrm{Hom}_{\bar{k},vector\text{-}space}(A \otimes \overline{k},\bar{k})$ are linear independent over $\overline{k}$. If a linear combination $\sum a_\sigma \sigma$ defines a linear map from A to k (i.e. $\sum a_\sigma \sigma(x) \in k$, for all $x \in A$ then the linear map is of the form $a\,\mathrm{tr}_{A/k}$ for some $a \in k$.*

This is rather obvious from the above.

One Dimensional Rings and Basic Results from Algebraic Number Theory

Now we consider integral rings A with $\dim(A) = 1$. This means that every non-zero prime ideal $\mathfrak{p}$ is already maximal. If we have any ideal $(0) \neq \mathfrak{a} \neq A$, then $\dim(A/\mathfrak{a}) = 0$ and $\mathrm{Spec}(A/\mathfrak{a}) \subset \mathrm{Spec}(A)$ is a finite subset by the previous results.
Hence we see that for a one dimensional ring A the open sets $U \subset \mathrm{Spec}(A)$ are the complements of a finite set of closed points (maximal prime ideals) and of course the empty set.

Definition 0.3.4. *If A is integral, of dimension one and local, then* $\mathrm{Spec}(A)$ *consists of two points $\{\mathfrak{p},(0)\}$. Such a ring is A is called a* **discrete valuation ring** *if $\mathfrak{p}$ is a principal ideal, i.e. we can find an element $\pi_\mathfrak{p}$ such that $\mathfrak{p} = A \cdot \pi_\mathfrak{p} = (\pi_\mathfrak{p})$. The element $\pi_\mathfrak{p}$ is called an* **uniformizing element**.

A uniformizing element $\pi_\mathfrak{p}$ is of course not unique in general, it can be multiplied by a unit and is still a uniformizing element. It is quite clear that any element $a \in A$ can be written as

$$a = \epsilon\, \pi_\mathfrak{p}^{\nu_\mathfrak{p}(a)} \tag{0.5}$$

where ϵ is a unit and where $\nu_\mathfrak{p}(a)$ is an integer. This exponent is called the order of a and can be considered as the order of vanishing of a at $\mathfrak{p}$.

The elements of the quotient field K are of the form

$$x = \frac{b}{c} = \frac{\epsilon\,\pi_\mathfrak{p}^{\nu_\mathfrak{p}(b)}}{\epsilon'\,\pi_\mathfrak{p}^{\nu_\mathfrak{p}(c)}} = \epsilon'' \cdot \pi_\mathfrak{p}^{\nu_\mathfrak{p}(a)-\nu_\mathfrak{p}(b)} = \epsilon'' \cdot \pi_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}. \tag{0.6}$$

We clearly have $\nu_\mathfrak{p}(x) \geq 0$ if and only if $x \in A$. We may say that x has a pole of order $-\nu_\mathfrak{p}(x)$ if $\nu_\mathfrak{p}(x) < 0$.
A very important class of one dimensional rings is provided by the Dedekind rings. We have the following

Definition 0.3.5. *A noetherian one-dimensional integral ring A is called a* **Dedekind ring** *if one of the following equivalent conditions is satisfied.*

1. *The ring is normal, i.e. integrally closed in its quotient field (See 0.2.3)*

2. *For every prime ideal $\mathfrak{p} \neq (0)$ the local ring $A_\mathfrak{p}$ is a discrete valuation ring.*

Proof: The inclusion 2. ⇒ 1. is quite clear: We consider our element $x \in K$ and assume that it satisfies an equation as as in 0.1. We claim that for any $\mathfrak{p} \neq (0)$ we must have $x \in A_\mathfrak{p}$. Otherwise we could write $x = \epsilon\pi_\mathfrak{p}^{-r}$ with $r > 0$ and ϵ a unit in $A_\mathfrak{p}$. But then x can not satisfy the polynomial equation, because we can multiply the equation by $\pi_\mathfrak{p}^{rn}$ and then the first term is non zero $\mod \mathfrak{p}$ and the other terms are zero $\mod \mathfrak{p}$. But if $x \in A_\mathfrak{p}$ for all $\mathfrak{p}$ then it follows from proposition **??** that $x \in A$.
The direction 1. ⇒ 2. is a not so easy. Of course we may assume that A is already local. If $\mathfrak{p}$ is the maximal ideal then we consider the A-module $\mathfrak{p}^{-1}$ of all elements $x \in K$, which satisfy $x\mathfrak{p} \subset A$. We clearly have $\mathfrak{p}^{-1} \supset A$. The decisive point is to show that we can find an element $y \in \mathfrak{p}^{-1}$, which is not in A. To see this we pick a non zero element $b \in \mathfrak{p}$. The ring $A/(b)$ has dimension zero and therefore, the image of $\mathfrak{p}$ in this ring is equal to the radical. This implies that a suitable power $\mathfrak{p}^n \subset (b)$, we choose n minimal with this property. Then we know that we can find elements $p_1, \dots, p_{n-1} \in \mathfrak{p}$ such that the element $y = p_1 p_2 \dots p_{n-1}/b \notin A$. But if we multiply by any further element in $\mathfrak{p}$ then the result lies in A. Now we conclude $y\mathfrak{p} = A$ or $y\mathfrak{p} = \mathfrak{p}$. But the second case is impossible, because exercise 1. 2. implies that y is integral over A. Since A is integrally closed we get $y \in A$ this is a contradiction. The rest is clear: We can find a $\pi \in \mathfrak{p}$ such that $y\pi = 1$ and therefore $\mathfrak{p} = (\pi)$ because if $p \in \mathfrak{p}$ then $yp = a \in A$ and this gives $p = \pi a$. □
This proposition is fundamental for the foundation of the theory of algebraic numbers.

If we have a Dedekind ring A and a non-zero ideal $(0) \neq \mathfrak{a} \subset A$, then the quotient $A/\mathfrak{a}$ has dimension zero and we just saw that

$$A/\mathfrak{a} = \prod_{\mathfrak{p} \supset \mathfrak{a}} (A/\mathfrak{a})_\mathfrak{p}.$$

If $\mathfrak{a}_\mathfrak{p}$ is the image of $\mathfrak{a}$ in the localization $A_\mathfrak{p}$ then $(A/\mathfrak{a})_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$. Now we know that $A_\mathfrak{p}$ is a discrete valuation ring hence we have $\mathfrak{a}_p = (\pi_p^{\nu_\mathfrak{p}(\mathfrak{a})})$ and $\nu_\mathfrak{p}(\mathfrak{a})$ is called the order of $\mathfrak{a}$ at $\mathfrak{p}$. It is not difficult to show that $A/\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})} = A_\mathfrak{p}/(\pi_p^{\nu_\mathfrak{p}(\mathfrak{a})})$ and hence we get

$$A/\mathfrak{a} = \bigoplus_{\mathfrak{p} \supset \mathfrak{a}} A/\mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}.$$

:

Exercise 9. a) Show this assertion implies $\mathfrak{a} = \prod_{\mathfrak{p}\supset\mathfrak{a}} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$.
Hint: What is in general the relation between the product $\mathfrak{a}\mathfrak{b}$ and the intersection of two ideals $\mathfrak{a}$,$\mathfrak{b}$ in an arbitrary ring A? Show that there is always an inclusion in one direction. Then verify that this inclusion becomes an equality if the two ideals generate the ring, or in other words if $\operatorname{Spec}(A/\mathfrak{a}) \cap \operatorname{Spec}(A/\mathfrak{b}) = \emptyset$.

b) Show: For any maximal prime ideal $\mathfrak{p}$ we can find an $x \in K$ (the field of fractions) such that $\operatorname{ord}_\mathfrak{p}(x) = -1$ and $\operatorname{ord}_\mathfrak{q}(x) \geq 0$ for all the other maximal ideals. Then $xp \in A$ for all $p \in \mathfrak{p}$.

Definition 0.3.6. *A* **fractional ideal** $\mathfrak{b}$ *of a Dedekind ring A is a finitely generated non zero A-submodule in the field of fractions K.*

For any fractional ideal $\mathfrak{b}$ we can find an $x \in K^*$ such that $x\mathfrak{b} \subset A$ becomes an integral (ordinary) ideal. We can multiply such fractional ideals and our previous results imply that:

Lemma 0.3.7. *The fractional ideals in a Dedekind ring form a group under multiplication.*

Definition 0.3.8. *The neutral element is obviously given by the ring A itself and exercise 9 b) above gives the inverse $\mathfrak{p}^{-1} = (1,x)$. This group is the free abelian group generated by the prime ideals. It is also called the group of* **divisors** $\operatorname{Div}(A)$*. This group of divisors contains the subgroup of principal divisors $P(A)$, these are the ideals of the form (x) with $x \neq 0$. The quotient group*

$$\operatorname{Pic}(A) = \operatorname{Div}(A)/P(A)$$

is the so called **ideal class group** *of A. Sometimes it is also called the* **Picard group***.*

The Picard group is an important invariant of the ring. By definition it is trivial if and only if A is a principal ideal domain.

If we have a Dedekind ring A with quotient field K and if L/K is an extension of finite degree, then we may consider the integral closure of A in L. This is the ring B consisting of those elements b, which satisfy an equation $b^n + a_1 b^{n-1} + \dots a_0 = 0$ with $a_i \in A$. We have seen in exercise 1 that they form an A-algebra.
We have the

Theorem 0.3.9 (Krull - Akizuki)**.** *The integral closure of a Dedekind ring in a finite extension of its quotient field is again a Dedekind ring.*

This is not an easy theorem, we refer to the book of [**?**], prop. 12.8. The main problem is to show that B is again noetherian.

The following fundamental theorem is easier, we drop the assumption that A is a Dedekind ring, we only assume that it is integral, noetherian and normal (See 0.2.3).

Theorem 0.3.10. *1. Let A be an integral ring, which is noetherian and normal. Let K be its quotient field and let L/K be a finite separable extension. Then the integral closure B of A in L is a finitely generated A- module. Hence B is clearly again an integral, normal and noetherian ring*

2. *If A is a normal integral ring, which is a finitely generated algebra over a field k, i. e. $A = k[x_1, \ldots, x_n]$ and if L is any finite extension of the quotient field K of A, then the integral closure B of A in L is again a finitely generated algebra over k and hence noetherian and normal.*

For a proof see [Ei], II, 13.3, as an alternative the reader may fill the gaps in the following sketch of the proof.
To see that that first assertion is true we start from a basis $a_1, \cdots, a_n$ of the field L over K, which consists of integral elements over A. Write an element $b \in B$ as linear combination $b = a_1x_1 + a_2x_2 \ldots a_nx_n$ with $x_i \in K$. We use the separability to invert this system of equations for the x_i. The traces $\mathrm{tr}_{L/K}(ba_\nu)$ are integral (use Exercise 1), and we find the relations

$$\mathrm{tr}_{L/K}(ba_\nu) = \sum \mathrm{tr}_{L/K}(a_i\, a_\nu)x_i.$$

Conclude that we can find an element $a \in A$, which does not depend on b such that $a_i a \in A$, hence $B \subset A\frac{a_1}{a} + \ldots + A\frac{a_n}{a}$ and therefore, is finitely generated.
To prove the second assertion we check that we may assume that L/K is normal (in the sense of field extensions). Then we have a maximal purely inseparable sub extension L_i/K. This is obtained by successive extraction of p-th roots. Hence we prove the assertion for extensions of the form $L = K[r^{1/p}]$ (not so easy) and proceed by induction and apply the first assertion at the end.
Without any further assumption on A or the extension L/K the assertion of the theorem above may become false.

We return to our assumption that A is a Dedekind ring. The theorem above has the following implication: Let us assume that we have a Dedekind ring A with quotient field K and a finite extension L/K and we assume that the assumptions of 1) or 2) are valid. Then we know that the integral closure B of A in L is a finitely generated A-module. Let us pick a maximal prime ideal $\mathfrak{p} \subset A$. We consider the $A/\mathfrak{p}$ algebra $B/\mathfrak{p}B$. First of all we claim that the dimension of $B/\mathfrak{p}B$ as an $A/\mathfrak{p}$-vector space is equal to the degree $[L : K] = \dim_K L$. This is almost obvious, we may assume that A is local and then B must be a free A-module of rank $[L : K]$ and this implies the claim. Now we have seen that

$$B/\mathfrak{p}B = \bigoplus_{\mathfrak{P}\supset\mathfrak{p}B} B/\mathfrak{P}^{\nu_{\mathfrak{P}}(\mathfrak{p}B)}e_{\mathfrak{P}} \tag{0.7}$$

where the $e_{\mathfrak{P}}$ are the idempotents. Then $B/\mathfrak{P}^{\nu_{\mathfrak{P}}(\mathfrak{p}B)}$ is a local $A/\mathfrak{p}$ algebra.
For a $\mathfrak{P} \supset \mathfrak{p}$ we get a finite extension of residue fields $(B/\mathfrak{P})/(A/\mathfrak{p})$ and we denote its degree by $f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}]$. Moreover we know that for any integer m the quotient $\mathfrak{P}^m/\mathfrak{P}^{m+1}$ is a $B/\mathfrak{P}$-vector space of dimension one and hence an $A/\mathfrak{p}$-vector space of dimension $f_{\mathfrak{P}}$. Therefore $B/\mathfrak{P}^{\nu_{\mathfrak{P}}}(\mathfrak{p}B)$ is an $A/\mathfrak{p}$-vector space of dimension $f_{\mathfrak{P}}\nu_{\mathfrak{P}}(\mathfrak{p}B)$. We call the numbers $\nu_{\mathfrak{P}}(\mathfrak{p}B) = \nu_{\mathfrak{P}}$ ramification indices. Counting the dimensions yields the formula

$$[L : K] = \sum_{\mathfrak{P}\supset\mathfrak{p}B} f_{\mathfrak{P}}\nu_{\mathfrak{P}}. \tag{0.8}$$

Definition 0.3.11. *The extension is called* **unramified at $\mathfrak{p}$** *if all the $\nu_{\mathfrak{P}} = 1$ and if the extensions $(B/\mathfrak{P})/(A/\mathfrak{p})$ are separable.*

Since B is free over A we can define the trace $\mathrm{tr}_{B/A}$ in the same way as we did this in 2.4.1 and it is clear (we still assume that A is local):

Proposition 0.3.12. *The extension B/A is unramified if and only if the pairing*

$$B \times B \longrightarrow A,(x,y) \mapsto \mathrm{tr}_{B/A}(xy)$$

is non degenerate, i.e. if for $x \in B$ the trace $\mathrm{tr}_{B/A}(xy) \in \mathfrak{p}$ for all $y \in B$ then it follows that $x \in \mathfrak{p}B$.

Let us now assume that our field extension L/K is a normal, separable extension. Let us denote its Galois group by $\mathrm{Gal}(L/K)$. Let A,B be as above, let $\mathfrak{p}$ be a non zero prime ideal in A, we have the decomposition

$$B/\mathfrak{p}B = \bigoplus_{\mathfrak{P}\supset\mathfrak{p}B} B/\mathfrak{P}^{\nu_{\mathfrak{P}}(\mathfrak{p}B)} = \bigoplus_{\mathfrak{P}\supset\mathfrak{p}B} (B/\mathfrak{p}B)e_{\mathfrak{P}}.$$

The Galois group $\mathrm{Gal}(L/K)$ acts on B and permutes the prime ideals $\mathfrak{P} \supset \mathfrak{p}$ and the idempotents $e_{\mathfrak{P}}$.

Definition 0.3.13. *Let us denote by $D_{\mathfrak{P}} \subset \mathrm{Gal}(L/K)$ the stabilizer of $\mathfrak{P}$, this is the* **decomposition group** *of $\mathfrak{P}$.*

We anticipate the theorem below, which asserts that this action on the set of primes is transitive. This implies that the subgroups $D_{\mathfrak{P}}$ are conjugate to each other, the degrees $[(B/\mathfrak{P}) : (A/\mathfrak{p})]$ and the ramification indices $\nu_{\mathfrak{P}}$ are independent of $\mathfrak{P}$ let us call them $f_{\mathfrak{p}}$,$\nu_{\mathfrak{p}}$. The index of $D_{\mathfrak{P}}$ in the Galois group is $g_{\mathfrak{p}}$ and this is the number of primes $\mathfrak{P} \supset \mathfrak{p}$. Our equation (0.8) becomes

$$[L : K] = g_{\mathfrak{p}} f_{\mathfrak{p}} \nu_{\mathfrak{p}} \tag{0.9}$$

We get homomorphisms

$$r_{\mathfrak{P}} : D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p})). \tag{0.10}$$

Definition 0.3.14. *The kernel of the homomorphism $r_{\mathfrak{P}} : D_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p})$ is the* **inertia group** *$I_{\mathfrak{P}}$.*

For us the following result is basic for the theory of algebraic numbers.

Theorem 0.3.15. *Let K,L,A,B,$\mathfrak{p}$ as above. The action of the Galois group on the primes above $\mathfrak{p}$ is transitive. If L/K is unramified at the prime $\mathfrak{p}$ then for any $\mathfrak{P} \supset \mathfrak{p}$ the homomorphism $D_{\mathfrak{P}} \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$ is an isomorphism.*

To see the transitivity we look at the orbit $\mathfrak{P}$,$\sigma(\mathfrak{P}), \dots$ of the prime ideal $\mathfrak{P}$ and assume that we find a prime ideal $\mathfrak{P}' \supset B\mathfrak{p}$ which is not in the orbit of $\mathfrak{P}$. Then we can find an element $x \in B$ which maps to $\sum_\sigma e_{\sigma(\mathfrak{P})}$. Then $\sigma(x) \notin \mathfrak{P}$ for all σ in the Galois group. Hence the norm $a = \prod \sigma(x) \notin \mathfrak{P}$. Since $a \in A$ we get $a \notin \mathfrak{p}$. But now $x \in \mathfrak{P}'$ and therefore $a \in \mathfrak{P}'$ and hence $a \in \mathfrak{p}$ a contradiction.
Assume that the homomorphism $r_{\mathfrak{P}}$ is not surjective, let $\bar{D}_{\mathfrak{P}} \subset \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$ be the image, let $m_{\mathfrak{P}} = m$ the order of the kernel of $r_{\mathfrak{P}}$, it is independent of $\mathfrak{P} \supset \mathfrak{p}$. We find an element $y_{\mathfrak{P}} \in B/\mathfrak{P}$ such that

$$\sum_{\sigma\in\bar{D}_{\mathfrak{P}}} \sigma(y_{\mathfrak{P}}) \notin A/\mathfrak{p}$$

See Thm. 0.3.3. We find an element $x \in B$ which maps to $y_{\mathfrak{P}}$. Then $\mathrm{tr}_{L/K}(x) \in A$, the image of this element in $A/\mathfrak{p}$ is of the form $a\sum_{\mathfrak{P}'} e_{\mathfrak{P}'}$ with $a \in A/\mathfrak{p}$. We get

$$\mathrm{tr}_{L/K}(x) = \sum \sigma(x) = m(\cdots + (\sum_{\sigma\in\bar{D}_{\mathfrak{P}}} \sigma(y_{\mathfrak{P}}))e_{\mathfrak{P}} + \ldots).$$

Now $m > 0$ is an integer, which may become zero in $A/\mathfrak{p}$, this will be the case if the characteristic of $A/\mathfrak{p}$ divides m. But then $\mathrm{tr}_{L/K}(y) = 0 \mod \mathfrak{p}$ for all $y \in B$, this is not possible because L/K is unramified at $\mathfrak{p}$. But if m is not zero then we get that $\mathrm{tr}_{L/K} \notin A/\mathfrak{p}$, this is again a contradiction. The surjectivity of $r_{\mathfrak{P}}$ implies $f_{\mathfrak{p}}|\#(D_{\mathfrak{P}})$ and then it follows from equation (0.9) that $r_{\mathfrak{P}}$ must be an isomorphism.

□

The surjectivity of $r_{\mathfrak{P}}$ is always true and will be proved later.

Definition 0.3.16. *A finite extension K of $\mathbb{Q}$ is called an* **algebraic number field**.

Since the ring $\mathbb{Z}$ is a Dedekind ring we now know that its integral closure $\mathcal{O}_K$ in K is always a Dedekind ring. This ring is called the ring of **integers in K.** The study of these rings of integers is the subject of algebraic number theory. We briefly state a basic theorem of this theory. We need a little bit of notation. We consider the base extension $K \otimes_{\mathbb{Q}} \mathbb{R}$, this is a finite $\mathbb{R}$ algebra and hence a direct sum of copies of $\mathbb{R}$ and $\mathbb{C}$. Then

$$K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2},$$

this defines the numbers r_1 and r_2.

Theorem 0.3.17. *For any algebraic number field $K/\mathbb{Q}$ the ideal class group* $\mathrm{Pic}(\mathcal{O}_K)$ *is a finite abelian group.*
The group of units $\mathcal{O}_K^\times$ is a finitely generated group, it is the product $W \times E$, where W is the finite (cyclic) group of roots of unity and E is free of rank $r_1 + r_2 - 1$.

If in our situation above L/K is a finite normal extension of algebraic number fields and if this extension is unramified at a prime $\mathfrak{p}$ of $A = \mathcal{O}_K$, then the extensions $(B/\mathfrak{P})/(A/\mathfrak{p})$ are extensions of finite fields. Let $N(\mathfrak{p}) = \#(A/\mathfrak{p})$. Then we know that the Galois group of these extensions is the cyclic group generated by the Frobenius element $\Phi_{\mathfrak{P}} : x \mapsto x^{N(\mathfrak{p})}$. Hence we find a unique element, also called $\Phi_{\mathfrak{P}} \in D_{\mathfrak{P}} \subset \mathrm{Gal}(L/K)$, which maps to this generator. This elements of the Galois group are also called **Frobenius elements**. These Frobenii $\Phi_{\mathfrak{P}'}$ to the different $\mathfrak{P}' \supset \mathfrak{p}$ form a conjugacy class attached to $\mathfrak{p}$, it is the **Frobenius class**.
Since we are very close to it, we also state the simplest version of the main theorem of class field theory. We consider an algebraic number field L with its ring of integers $\mathcal{O}_L$. We consider finite normal extensions F/L, with the property that their Galois group $\mathrm{Gal}(F/L)$ is abelian, and which are unramified at all prime $\mathfrak{p}$ of $\mathcal{O}_L$. If we have two such extensions F_1,F_2 then we can form the tensor product $F_1 \otimes F_2$ and decompose this into a sum of fields

$$F_1 \otimes F_2 = \bigoplus_{\nu} F_\nu.$$

These extensions F_ν are again unramified and have an abelian Galois group.
Let us pick any such an extension. We construct a homomorphism from the group of fractional ideals to $\mathrm{Gal}(F/L)$: To do this we observe that the group of fractional ideals is the free abelian group generated by the prime ideals. To any prime ideal $\mathfrak{p}$ we pick a prime ideal $\mathfrak{P}$ and our homomorphism sends $\mathfrak{p}$ to the Frobenius element $\Phi_{\mathfrak{P}}$. Since our extension is abelian this extension does not depend on the choice of $\mathfrak{P}$. Now we can formulate the celebrated theorem, which has been proved by E. Artin in his paper [**?**]:

Theorem 0.3.18. *The above homomorphism is trivial on the principal ideals and hence it induces a homomorphism*

$$Art\colon \mathrm{Pic}(\mathcal{O}_L) \longrightarrow \mathrm{Gal}(F/L).$$

This homomorphism is surjective and there exists a maximal abelian, unramified extension H/L, for which this homomorphism becomes an isomorphism.

This maximal abelian, unramified extension is called the *Hilbert class field.*
Of course it is clear that for any normal ring A, which is also factorial, the Picard group $\mathrm{Pic}(A) = 0$. The opposite direction is also true if the ring is noetherian, see [**?**] , Cor. 11.7.

0.4 Quadratic fields

The results imply that we have abundantly many Dedekind rings. First of all we know that $\mathbb{Z}$ and $k[X]$ are Dedekind rings, here k is any field. The quotient fields are $\mathbb{Q}$ and $k(X)$. Let K any of these two fields.
For any finite (separable in second case) extension L/K we can define the integral closure of $\mathbb{Z}$ (resp. $k[X]$) in L, this is the ring $\mathcal{O}_L$ of integral elements.

The theorem 0.3.9 above and the going up and down theorem imply that $\mathcal{O}_L$ is again a Dedekind ring

The simplest examples are the rings of integers in a quadratic extension of $\mathbb{Q}$. Choose an integer $d \in \mathbb{Z}, d \neq 1$ and assume that it does not contain any non trivial square factor. Then we define the field $\mathbb{Q}(\sqrt{d}) = a + b\sqrt{d}, a,b \in \mathbb{Q}$ where $\sqrt{d}$ is a number which satisfies $(\sqrt{d})^2 = d$, this is the only information we want to use about this number.
Then we put

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

Show that the ring of integers in $L = \mathbb{Q}(\sqrt{d})$ is

$$\mathcal{O}_L = \{a + b\omega \mid a,b \in \mathbb{Z}\}$$

The element ω satisfies the quadratic equation

$$\omega^2 - p_0\omega + q_0 = 0$$

where $p_0 = 0, q_0 = -d$ in the case $d \equiv 2,3 \mod 4$ and $p_0 = 1, q_0 = \frac{1-d}{4}$ in the case $d \equiv 1 \mod 4$.
We have a dramatic difference between the cases $d > 0$ (real quadratic fields) and $d < 0$ (imaginary quadratic fields.)

Exercise : Discuss the structure of the group $\mathcal{O}_L^\times$ of units in the two situations.

If we want to describe the group of units $\mathcal{O}_L^\times$ then we have to exploit the fact that our field has a nontrivial automorphism σ which sends ω to $\omega' = 1 - \omega$. This allows to define the norm homomorphism

$$N : a + b\omega \mapsto (a + b\omega)(a + b\omega') = a^2 + p_0 ab + q_0 b^2$$

Show that the norm of a unit must be ±1. Hence to get units we have to solve the diophantine equation

$$x^2 + p_0 xy + q_0 y^2 = \pm 1$$

in integers x,y.
If $p_0 = 0$ then this reduces to Pell's equation.

$$x^2 - dy^2 = \pm 1$$

For $d < 0$ it is not too difficult to find all solutions, in the case $d > 0$ we have to use the method of continued fraction expansion, this can be done in examples and will be discussed later.

0.4.1 Decomposition law for quadratic fields "Zerlegungsgesetz"

We consider the general theorem 0.3.15 in the special case of quadratic field extensions of $\mathbb{Q}$. We have the relation $e_p f_p g_p = 2$ (see (0.9)).
Pick a prime p, we have to study the structure of the $\mathbb{F}_p$ algebra

$$\mathbb{F}_p[\omega] = \mathbb{F}_p[X]/(X^2 - p_0 X + p_0)$$

It turns out to be reasonable to distinguish the cases $p = 2$ and $p > 2$.

First case $p = 2$:
In this case $\mathbb{F}_2[\omega]$ has non zero nilpotent elements if and only if $p_0 = 0$. The decomposition group $D_{(2)}$ is trivial

If $p_0 = 1$ then the polynomial is separable, it decomposes into two different factors if and only if $q_0 = 0$. In this case $g_2 = 2$.

If $q_0 = 1$ then our algebra $\mathbb{F}_2[\omega]$ is a field, it is isomorphic to $\mathbb{F}_4$, we have $f_{(2)} = 2$ and $D_{(2)}$ is the cyclic group of order 2. It is generated by the Frobenius element.
We have ramification at 2 if and only if $p_0 = 0$ or in other words $d \equiv 2,3 \mod 4$.

Second case $p > 2$:

In this case we have ramification if an only if the two roots of the equation become equal and this means that p divides $-4a_0^2 + p_0^2 = d$. We have $e_p = 2$ and the decomposition group $D_{(p)}$ is cyclic of order 2. (Here we use again that d is square free)
If p does not divide d then we get

$$\mathbb{F}_p[\omega] \text{ is the sum of two copies of } \mathbb{F}_2 \text{ if } d \in \mathbb{F}_p^\times \text{ is a square.}$$

$$\mathbb{F}_p[\omega] \text{ is isomorphic to } \mathbb{F}_4 \text{ if } d \in \mathbb{F}_p \text{ is a not a square.}$$

In this last case $D_{(2)}$ is again cyclic of order 2 and generated by the Frobenius element. If p is not ramified in our quadratic field, the we say that p *splits* and write $(p) = \mathfrak{p} \cdot \mathfrak{p}'$ if $\mathbb{F}_p[\omega]$ is is sum of two fields and otherwise we say that (p) is *inert* .

0.4.2 Quadratic fields and the group $\mathrm{SL}_2(\mathbb{Z})$

Our field L is a two dimensional vector space over $\mathbb{Q}$, it comes with a distinguished basis $\{1,\omega\}$ We have the homomorphism

$$\iota : L \longrightarrow \mathrm{End}_{\mathbb{Q}}(L)$$

which is defined by

$$\iota : \alpha = a + b\omega \mapsto L_\alpha = \{x + y\omega \mapsto \alpha(x + y\omega)\}$$

With respect to the above basis the the endomorphism L_α is given by the matrix

$$L_\alpha = \begin{pmatrix} a & bq_0 \\ b & a + bp_0 \end{pmatrix}$$

in other words ι provides a homomorphism

$$\iota : L \mapsto M_2(\mathbb{Q})$$

This yields group homomorphisms

$$\iota_{\mathbb{Q}} : L^\times \longrightarrow \mathrm{GL}_2(\mathbb{Q})$$

and

$$\iota_{\mathbb{Z}} : \mathcal{O}_L^\times \longrightarrow \mathrm{GL}_2(\mathbb{Z}).$$

0.4.3 The action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$

The upper half plane is the set

$$\mathbb{H} = \{z = x + iy \mid x,y \in \mathbb{R}, y > 0\} \subset \mathbb{C}$$

The group $\mathrm{SL}_2(\mathbb{R})$ acts upon $\mathbb{H}$:

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az + b}{cz + d}$$

Verify that this is an action.
We can restrict this action to $L^\times(1) \subset \mathrm{SL}_2(\mathbb{Q})$, these are the elements of norm 1.
We have two embeddings $i_+,i_- : L \hookrightarrow \mathbb{C}$, we normalize them so that $i_+(\sqrt{d})$ becomes the positive root if $d > 0$ and $i\sqrt{-d}$ where the square root is again the positive one.

Theorem 0.4.1. *If $d < 0$ then the action of $L^\times(1)$ on $\mathbb{H}$ has exactly one fixed point, namely the point namely $i_+(\omega)$.*
If $d > 0$ then we extend the action to an action to an action on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{R}) = \mathbb{H} \cup \mathbb{R} \cup \{\infty\} = \bar{\mathbb{H}}$, then $L^\times(1)$ has the two fixed points $i_-(\omega),i_+(\omega) \in \mathbb{R}$. The semicircle in $\mathbb{H}$, which goes from $i_-(\omega)$ to $i_+(\omega)$ and hits the real line orthogonally, is invariant under the action of $L^\times(1)$.
The subgroup $L^\times(1)$ is the stabilizer of $i_+(\omega)$ in $\mathrm{SL}_2(\mathbb{Q})$, it also stabilizes $i_-(\omega)$.

Exercise: Prove this theorem.

0.4.4 The continued fraction expansion

We introduce the following two matrices

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

For any real number $\alpha_0 = \alpha > 0$ we define a sequence $cf(\alpha) = [a_0,a_1,a_2,\dots]$ of integers by the following rule

$$T^{a_0}(\alpha) \in (-1,0] = \beta_0,\ \alpha_1 = -1/\beta_0 = ST^{a_0}(\alpha_0)$$

If $\alpha_1 = \infty$ the sequence stops, otherwise we define a_1 again by

$$T^{a_1}(\alpha_1) \in (-1,0]$$

and continue forever unless the sequence stops.

Theorem 0.4.2. *The continued fraction expansion stops if and only if $\alpha \in \mathbb{Q}$. It yields the generation of $\mathrm{SL}_2(\mathbb{Z})$ by S,T.*

Proof and explanation in Robert's lecture on Friday.
This continued fraction expansion is different from the usual one. Usually we shift α into the half open interval $[0,1)$, i.e. the first step is

$$T^{a_0'}(\alpha) \in [0,1) = \beta_0',\ \alpha_1' = 1/\beta_0'$$

This yields the classical continued fraction expansion

$$\alpha = \{a_0',a_1',\dots\}$$

We observe that the transformation $x \mapsto 1/x$ is induced by the matrix $S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which is not in $\mathrm{SL}_2(\mathbb{Z})$. Therefore we get a generation of $\mathrm{GL}_2(\mathbb{Z})$ by the matrices S_1,T and $t_0 = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. Since we can express $t_0 = STS_1T^{-1}S_1T$ we get that $\mathrm{GL}_2(\mathbb{Z})$ is generated by S_1,T.

More difficult is the following:

Theorem 0.4.3. *The continued fraction expansion*

$$i_+(\omega) = [a_0,\overline{a_1,\dots,a_r}]$$

is periodic after the first step. The matrix

$$A = T^{a_r - a_0} S T^{a_{r-1}} \dots S T^{a_1} S T^{a_0}.$$

fixes $I_+(\omega)$ and generates the group of totally positive units.
If we do this for the classical continued fraction expansion, then we get a matrix

$$A_1 = T^{a'_r - a'_0} S_1 T^{a'_{r-1}} \dots S_1 T^{a'_1} S_1 T^{a'_0}.$$

which is a fundamental unit.

There is a way to prove the theorem above if we believe the Dirichlet-unit theorem. This theorem asserts that the group of units of $\mathcal{O}_F^\times$ is a product of the group $W = \{\pm 1\}$ of roots of unity and an infinite cyclic group which is generated by a fundamental unit ϵ_0. An element $a + b\omega \in L^\times$ is called totally positive if $a + b\, i_+(\omega) > 0$ and $a - b\, i_+(\omega) > 0$. The group of totally positive units is also cyclic and generated by ϵ_0^2 or ϵ. Let

$$\epsilon = x + y i_+(\omega)$$

be a generator of the group of totally positive units. We may assume that $x > 0$ and then we have $0 < y < x$. Under the above map ι this element is mapped to

$$\iota(\epsilon) = \begin{pmatrix} x & y\, q_0 \\ y & x + y\, p_0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Let $A = \begin{pmatrix} u & * \\ v & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ where $u > v > 0$. Then Robert showed in his lecture

Exercise: (a) If $cf(u/v) = [a_0,a_1,\dots,a_r]$ then

$$T^{a_r}\; S\; T^{a_{r-1}} \dots S\; T^{a_0} A = \begin{pmatrix} 0 & 1 \\ -1 & b \end{pmatrix} = S \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

where b is an integer (depending on the entries in the second column).

(b) Let $\alpha \in \mathbb{R}$ and assume $u/v < \alpha$ and $\alpha - u/v < 1/v^2$, i.e. u/v is a very good approximation of α, then the beginning of the continuous fraction expansion of α coincides with the expansion of u/v.

(c) Since we have $A(i_+(\omega)) = i_+(\omega)$ we get

$$T^{a_r}\; S\; T^{a_{r-1}} \dots S\; T^{a_0}(i_+(\omega)) = S \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} (i_+(\omega))$$

Show that x/y is a very good approximation of $i_+(\omega)$. Show that this implies $b = a_0$ and hence we get the periodicity of the continued fraction expansion

$$cf(i_*(\omega)) = [a_0,a_1,\dots,a_r,a_1,\dots]$$

The continued fraction expansion is very useful if we want to identify a rational number which is only given by an approximating decimal expansion.
Example and exercise:
One of the most interesting power series expansion is the expansion of the Ramanujan Δ -function

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1742q^4 \cdots = \sum_{n=1}^{\infty}\tau(n)q^n$$

Associated to this power series we define a so called L -function

$$L(\Delta,s) = \frac{\Gamma(s)}{(2\pi)^s}\sum_{n=1}^{\infty}\tau(n)n^{-s}$$

where s is a complex variable. ($\Gamma(s)$ is the Γ-function) This series is absolutely convergent for $\mathrm{Re}\,(s) \geq 13/2$. A not very precise computation yields

$$L(\Delta,11) \approx 0.005958964989578306 1617, F(\Delta,9) \approx 0.002541756054196711 0753$$

We have a theorem by Manin and Shimura which asserts that the ratio

$$\frac{L(\Delta,9)}{L(\Delta,11)} \in \mathbb{Q},$$

i.e. it is a rational number.
From above we get the numerical approximation

$$\frac{L(\Delta,9)}{L(\Delta,11)} \approx 0.42654320987654967221$$

Use the continued fraction expansion to guess the value of this rational number.

The value $\frac{L(\Delta,8)}{L(\Delta,10)}$ is also a rational number. Only if you are very courageous yo may try to compute this number.

0.5 Various comments

Supplement to equation (0.6)

Let A be any discrete valuation ring (π) its maximal ideal, let K be its field of fractions. For $x \in K$ we define the order $\mathrm{ord}(x)$ by

$$x = \pi^{\mathrm{ord}(x)}\epsilon \text{ with } \epsilon \in A^\times.$$

If $\mathrm{ord}(x) > 0$ then we say that x has a zero of order $\mathrm{ord}(x)$ if $\mathrm{ord}(x) < 0$ then we say that x has a pole of order $\mathrm{ord}(x)$.
We have

$$\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y),$$

$$\text{ord}(x+y) \geq \min(\text{ord}(x), \text{ord}(y)) \text{ and we have equality if} \, \text{ord}(x) \neq \text{ord}(y)$$

This last assertion has an important consequence: If x_1,$x_2, \dots$,$x_n \in K$ and if $\sum_i x_i \in A$ and if $\min(\text{ord}(x_i)) < 0$ then this minimum is attained more than one times.
This is used to prove $\mathcal{O}_\mathfrak{p}[\Pi_\mathfrak{P}] = \mathcal{O}_L$ in case of total ramification.

Supplement to Nakayamas' Lemma (0.6)

Let A is any local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated A module.
Then $M \otimes A/\mathfrak{m}$ is a finite dimensional $A/\mathfrak{m}$ -vector space and hence has a basis e_1,$e_2, \dots$,e_n. Let $\widetilde{e}_1$,$\widetilde{e}2, \dots$,$\widetilde{e}_n$ be liftings of these basis elements(this means that they map to the e_i under the reduction map $M \longrightarrow M/\mathfrak{m}M = M \otimes A/\mathfrak{m}$. Then these elements $\widetilde{e}_1$,$\widetilde{e}_2, \dots$,$\widetilde{e}_n$ generate the A-module M.
If A is a discrete valuation ring and if M is torsion free, then these $\widetilde{e}_1$,$\widetilde{e}2, \dots$,$\widetilde{e}_n$ form a basis of the A-module M.
Proof: Let $\sum a_i \widetilde{e}_i = 0$, assume not all the a_i are zero. Let $r = \min(\text{ord}(a_i))$. Then we have

$$\pi^r (\sum_i \frac{a_i}{\pi^r} \widetilde{e}_i) = 0$$

and since M is torsion free already the inner sum

$$\sum_i \frac{a_i}{\pi^r} \widetilde{e}_i = 0,$$

where $a_i/\pi^r \in A$. If we map this relation to $M \otimes A/\mathfrak{m}$ we get a non trivial linear relation among the e_i, a contradiction.
Hence: *A torsion free, finitely generated module over a discrete valuation ring is free.*

Remark on Δ

Go back to 0.4.3. We introduce the variable $z \in \mathbb{H}$ and put $q = e^{2\pi i z}$. We change our notation and put

$$\Delta(z) = e^{2\pi i z} \prod_{n=1}^{n=\infty} (1 - e^{2\pi i z})^{24}$$

This infinite product converges locally uniformly in $\mathbb{H}$ and defines a holomorphic function on $\mathbb{H}$.
Theorem : We have $\Delta(z+1) = \Delta(z)$ and $\Delta(-\frac{1}{z}) = z^{12}\Delta(z)$
Proof: The first assertion is obvious the second one is difficult, (any book on modular forms).
This implies that for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$:

$$\Delta(\gamma(z)) = \Delta(\frac{az+b}{cz+d}) = (cz+d)^{12}\Delta(z) \tag{0.11}$$

Exercise Show that

$$\int_0^\infty \Delta(iy)y^s \frac{dy}{y} = L(\Delta,s)$$

There are minor problems with convergence if $y \longrightarrow 0$ but good convergence properties for $y \longrightarrow \infty$.
Split the integral into two terms $\int_0^1 + \int_1 \infty$ and use 0.11 to transform the first integral also into an integral from 1 to ∞.
Excercise: Derive an expression for $L(\Delta,s)$ which is the sum of two rapidly converging series.
Now you are ready to compute $\frac{L(\Delta,8)}{L(\Delta,10)}$.

Comments on Exercises

Problem sheet 5 Exercise 1)
Let k be a field, $\alpha \in k,\alpha \neq 0$. Let $n > 1$ be an integer. Consider the k-algebra $k[X]/(X^n - \alpha) = k[\beta]$.
Compute the trace map $(x,y) \longrightarrow \mathrm{tr}_{k[\beta]/k}(x,y)$, i.e. compute it for any power $\beta^m,0 \leq m < n$, and show: The k-algebra $k[\beta]$ is separable if and only if ???
In exercise 2 the 119 has to be replaced by 120.

Comments on $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$

Let A be a discrete valuation ring, let K be its fraction field, assume its characteristic is zero. Let p be a prime and assume that the principal ideal (p) is the maximal ideal, i.e. assume that (p) is prime. Let $m = p^r$. We define the cyclotomic polynomial

$$\Phi_m(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + \cdots + X^{p^{r-1}\nu} + \cdots + X^{p^{r-1}} + 1$$

We consider the extension $L = K(\zeta_m)$. Apply Theorem 0.3.15 to this situation and show

The extension L/K is totally ramified at p the ramification index is $\varphi(p^m) = p^{m-1}(p-1)$. The Tate character gives an isomorphism

$$\alpha : \mathrm{Gal}(L/K) \xrightarrow{\sim} (\mathbb{Z}/p^r\mathbb{Z})^\times$$

and the cyclotomic polynomial $\Phi_m(X) \in K[X]$ is irreducible.
The ring of integers in L is $B = A[\zeta_m]$.
Every body is invited to write a formal proof of this assertion, it will be included in these notes.

Let $\mathcal{O}_K$ be the ring of integers in an algebraic number field K. We assume that the principal ideal $(p) = p\mathcal{O}_K$ is totally unramified at p, i.e. $p\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \ldots \mathfrak{P}_r$ (all the $\nu_\mathfrak{P} = 1$). We still assume $m = p^r$. Then we have a similar conclusion

The the cyclotomic polynomial $\Phi_m(X) \in K[X]$ is irreducible and the ring of integers in $K(\zeta_m)$ is

$$\mathcal{O}_{K(\zeta_m)} = \mathcal{O}_K[\zeta_m].$$

Cyclotomic units

We have the still pending problem to prove the existence of non trivial solutions of Pell's equation, or in other words the existence of non trivial units in real quadratic fields. (Theorem 0.4.3).
We discuss a special case. Let $p > 2$ be a prime, assume $p \equiv 1 \mod 4$. We consider the following element in $\mathbb{Q}(\zeta_p)$:

$$\epsilon = \prod_{a \in \mathbb{F}_p^\times} (1 - \zeta_p^a)^{\left(\frac{a}{p}\right)}$$

a) Show that this element is a unit in $\mathbb{Z}[\omega]$, of course $\omega = \frac{1+\sqrt{p}}{2}$.

b) Compute this number in the case $p = 5$.

c) (Not so easy) Show that this number is not equal to ± 1. (Hints available on request) Therefore it is a non trivial unit in $\mathbb{Z}[\omega]^\times$.

d) Write a little program that computes ϵ for larger primes.

e) Compute the fundamental unit ϵ_0 for $p = 229$ and $p = 401$ using Theorem 0.4.3

f) Try to use d) to compute the unit ϵ for these two cases, relate ϵ to ϵ_0.

0.5.1 Comments on Theorem 0.3.15

Recall the basic situation: We start from a global field K, let L/K be a finite separable extension. Let $A \subset K$ be a Dedekind ring in K, if K is a number field then A may be the ring of integers. If K is a finite separable extension of $\mathbb{F}_q(t)$ then A can be the integral closure of $\mathbb{F}_q[t]$ (or of $\mathbb{F}_q[t^{-1}]$.)
Let $B \subset L$ be the integral closure of A in L. We know that B is again a Dedekindring (see (0.3.5), this is a definition and a theorem). If $\mathfrak{p} \subset A$ is a non zero prime ideal, then $B/\mathfrak{p}B$ is a finite dimensional $A/\mathfrak{p} = k(\mathfrak{p})$ algebra, hence there are only finitely many primes $\mathfrak{P} \supset \mathfrak{p}B$ and

$$\widetilde{r} : B/\mathfrak{p}B \xrightarrow{\sim} \bigoplus_{\mathfrak{P} \supset B/\mathfrak{p}B} B/\mathfrak{p}Be_{\mathfrak{P}} \tag{0.12}$$

Here the $e_{\mathfrak{P}} \in B/\mathfrak{p}B$ form a system of orthogonal idempotents: We have $e_{\mathfrak{P}}^2 = e_{\mathfrak{P}}, e_{\mathfrak{P}} \cdot e_{\mathfrak{P}'} = 0$ if $\mathfrak{P} \neq \mathfrak{P}'$. The $A/\mathfrak{p}$-algebras $B/\mathfrak{p}Be_{\mathfrak{P}}$ are sub algebras, and the isomorphism $\widetilde{r}^{-1}$ is given by $(\dots, x_{\mathfrak{P}}, \dots\} \mapsto \sum x_{\mathfrak{P}}$.

There is a slightly different way of looking on this isomorphism. Let us put $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$,$S_{\mathfrak{P}} = B \setminus \mathfrak{P}$ then we define (abuse of notation)

$$A_{\mathfrak{p}} := A_{S_{\mathfrak{p}}} \ ,B_{\mathfrak{P}} := B_{S_{\mathfrak{P}}} \tag{0.13}$$

This are now discrete valuation rings with maximal ideals which are again called $\mathfrak{p}$,$\mathfrak{P}$ these ideals are principal, we write

$$\mathfrak{p} = (\pi_{\mathfrak{p}})\ ,\ \mathfrak{P} = (\Pi_{\mathfrak{P}})$$

Since $\mathfrak{P} \supset \mathfrak{p}B$ we find a number $\nu_{\mathfrak{p}}$ such that $(\Pi_{\mathfrak{P}}^{\nu_{\mathfrak{p}}}) = (\pi_{\mathfrak{p}})$. We define $k(\mathfrak{P}) = B/\mathfrak{p}$ and put $f_{\mathfrak{P}} = [k(\mathfrak{P}) : k(\mathfrak{p})]$.
In our decomposition (0.12) the summands $B/\mathfrak{p}Be_{\mathfrak{P}} = B_{\mathfrak{P}}/(\pi_{\mathfrak{p}}) = B_{\mathfrak{P}}/(\Pi_{\mathfrak{P}}^{\nu_{\mathfrak{P}}}) = B/\mathfrak{P}^{\nu_{\mathfrak{P}}}$ We have the projection $r_{\mathfrak{P}} : B \longrightarrow B/\mathfrak{P}^{\nu_{\mathfrak{P}}}$ and hence we get a projection

$$r : B \longrightarrow \prod_{\mathfrak{P} \supset \mathfrak{p}} B/\mathfrak{P}^{\nu_{\mathfrak{P}}}$$

Our formula (0.12) tells us that r is surjective (commonly known as Chinese remainder theorem) and the kernel is $\mathfrak{p}B$ in other words we get an isomorphism

$$B/\mathfrak{p}B \xrightarrow{r} \prod_{\mathfrak{P} \supset \mathfrak{p}} B/\mathfrak{P}^{\nu_{\mathfrak{P}}} \tag{0.14}$$

In (0.12) we explicitly wrote down $\widetilde{r}$ and $\widetilde{r}^{-1}$. To invert r in (**??**) we have to find the elements $e_{\mathfrak{P}}$ which map to $(0, \dots ,1,0 \dots)$ where the 1 is at place $\mathfrak{P}$.
The numbers $\nu_{\mathfrak{P}}$ are called the ramification indices, the prime $\mathfrak{P}$ is called unramified if $\nu_{\mathfrak{P}} = 1$, the prime $\mathfrak{p}$ is unramified in L/K if all $\nu_{\mathfrak{P}} = 1$.
We get

$$[L : K] = \sum_{\mathfrak{P} \supset B/\mathfrak{p}B} f_{\mathfrak{P}} \nu_{\mathfrak{P}} \tag{0.15}$$

If we now compute modulo higher powers of $\mathfrak{p}$ then we get

$$B/\mathfrak{p}^n B \xrightarrow{\sim} \bigoplus B/\mathfrak{P}^{\nu_{\mathfrak{P}} n} \tag{0.16}$$

We defined the projective limit $\widehat{A}_{\mathfrak{p}} = \varprojlim A/\mathfrak{p}^n$ and then we find

$$\varprojlim B/\mathfrak{p}^n B = B \otimes \widehat{A}_{\mathfrak{p}} = \bigoplus_{\mathfrak{P} \supset \mathfrak{p}B} \varprojlim B/\mathfrak{P}^{\nu_{\mathfrak{P}} n} = \bigoplus_{\mathfrak{P} \supset \mathfrak{p}B} \widehat{B}_{\mathfrak{P}} \tag{0.17}$$

Recall that the completions $K_{\mathfrak{p}}$ of K (resp. $L_{\mathfrak{P}}$) with respect to the valuations $|\ \ |_{\mathfrak{p}}$ (resp. $|\ \ |_{\mathfrak{P}}$ are the fields of fractions of $\widehat{A}_{\mathfrak{p}}$ (resp. $\widehat{B}_{\mathfrak{P}}$) we get from here

$$L \otimes K_{\mathfrak{p}} = \bigoplus_{\mathfrak{P} \supset \mathfrak{p}} L_{\mathfrak{P}} \tag{0.18}$$

We get a "completed" variant of our theorem 0.3.15

Theorem 0.5.1. *If L/K is normal then we get an action of the Galois group* $\mathrm{Gal}(L/\mathbb{Q})$ *on $L \otimes K_{\mathfrak{p}}$ This action is transitive on $\{\mathfrak{P} \supset \mathfrak{p}B\}$ and hence it interchanges the direct summands in the above decomposition. If $D_{\mathfrak{P}}$ is the stabilizer of $\mathfrak{P}$ then the homomorphism $D_{\mathfrak{P}} \longrightarrow$* $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ *is an isomorphism.*

Since we have this transitive action it follows that the numbers $f_{\mathfrak{P}}$,$\nu_{\mathfrak{P}}$ are independent of $\mathfrak{P}$ hence we call them $f_{\mathfrak{p}}$,$\nu_{\mathfrak{p}}$.
Then the number of elements in $\{\mathfrak{P} \supset \mathfrak{p}B\}$ is called $g_{\mathfrak{p}}$ and we have (see 0.15)

$$[L : K] = f_{\mathfrak{p}} g_{\mathfrak{p}} \nu_{\mathfrak{p}} \tag{0.19}$$

The number $g_{\mathfrak{p}} = [\mathrm{Gal}(L/K) : D_{\mathfrak{P}}]$ and therefore the order of $D_{\mathfrak{P}}$ is equal to $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. We finish the argument by observing that $L \subset L_{\mathfrak{P}}$ and this implies that the homomorphism is injective.

0.5.2 Local considerations

We still have the homomorphism $D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, it is surjective because Hensel's lemma shows that we can construct intermediate field $K_{\mathfrak{p}} \subset L_{\mathfrak{P}}^{\mathrm{nr}} \subset L_{\mathfrak{P}}$ which is unramified and which satisfies

$$\mathrm{Gal}(L_{\mathfrak{P}}^{\mathrm{nr}}/K_{\mathfrak{p}}) \xrightarrow{\sim} \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$$

Since $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(L_{\mathfrak{P}}^{\mathrm{nr}}/K_{\mathfrak{p}})$ is surjective this removes the assumption that $\mathfrak{p}$ should be unramified from theorem 0.3.15.
The residue fields $k(\mathfrak{P}) \supset k(\mathfrak{p})$ are finite, let $q = \#k(\mathfrak{p})$,$q^{f_{\mathfrak{p}}} = \#k(\mathfrak{P})$. The Galois group $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ is cyclic of order $[k(\mathfrak{P}) : k(\mathfrak{p}))]$ and generated by the Frobenius automorphism $\Phi_q : x \mapsto x^q$. We have $\Phi_q^{f_{\mathfrak{p}}}(x) = x^{q^{f_{\mathfrak{p}}}}(x) = x$ and hence $\Phi_q^{f_{\mathfrak{p}}}$ is the identity on $k(\mathfrak{P})$.
The kernel $I_{\mathfrak{P}}$ of the homomorphism $D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(L_{\mathfrak{P}}^{\mathrm{nr}}/K_{\mathfrak{p}})$ is called the inertia group.
If we look more meticulously then we see a tower of homomorphisms

$$\begin{tikzcd}
D_{\mathfrak{P}} \arrow[r] \arrow[dr] \arrow[dddr] & \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \\
 & \mathrm{Aut}_{\widehat{A}_{\mathfrak{p}}}(\widehat{B}_{\mathfrak{P}}/\mathfrak{P}^2) \arrow[u] \\
 & \vdots \arrow[u] \\
 & \mathrm{Aut}_{\widehat{A}_{\mathfrak{p}}}(\widehat{B}_{\mathfrak{P}}/\mathfrak{P}^{\nu})
\end{tikzcd}$$

the arrows are called r_1,r_2,$\dots$,r_ν,$\dots$, the kernel of r_1 is the inertia group $I_{\mathfrak{P}}$ and we get a descending sequence of subgroups $I_{\mathfrak{P}} = I_{\mathfrak{P}}^{(1)} \supset I_{\mathfrak{P}}^{(2)} \supset \dots I_{\mathfrak{P}}^{(\nu)} \dots$ where $I_{\mathfrak{P}}^{(\mu)} = \ker(r_\mu)$

The inertia group $I_{\mathfrak{P}}$ is of course the Galois group $\mathrm{Gal}(L_{\mathfrak{P}}/L_{\mathfrak{P}}^{\mathrm{nr}})$. Let $\widehat{B}_{\mathfrak{P}}^{\mathrm{nr}}$ be the ring of integers in $L_{\mathfrak{P}}^{\mathrm{nr}}$ then the maximal ideal in this ring of integers is still $(\pi_{\mathfrak{p}})$. We know that

$$\widehat{B}_{\mathfrak{P}} = \widehat{B}_{\mathfrak{P}}^{\mathrm{nr}}[\Pi_{\mathfrak{P}}]$$

We want to understand the action of the Galois group $\mathrm{Gal}(L_{\mathfrak{P}}/L_{\mathfrak{P}}^{\mathrm{nr}}) = I_{\mathfrak{P}}$, since any $\sigma \in I_{\mathfrak{P}}$ leaves the ideal $(\Pi_{\mathfrak{P}})$ invariant, we see

$$\sigma \Pi_{\mathfrak{P}} = u(\sigma)\Pi_{\mathfrak{P}} \tag{0.20}$$

where $u : I_{\mathfrak{P}} \longrightarrow B_{\mathfrak{P}}^{\times}$ is a 1-cocycle: it satisfies $u(\sigma\tau) = u(\sigma)\sigma(u(\tau))$.
The map u is injective and it is clear that

$$I_{\mathfrak{P}}^{(\nu)} = \{\sigma \in I_{\mathfrak{P}} \mid u(\sigma) \equiv 1 \mod (\Pi_{\mathfrak{P}}^{\nu-1})\}.$$

The following is now rather easy to show
a)*For $\nu = 1$ we can send $u(\sigma) \in B_{\mathfrak{P}}^{\times}$ to $k(\mathfrak{P})^{\times}$ and get an injective homomorphism*

$$I_{\mathfrak{P}}/I_{\mathfrak{P}}^{(2)} \hookrightarrow k(\mathfrak{P})^{\times}$$

b) *For $\nu > 1$ and $\sigma \in I^{(\nu)}$ we can write*

$$u(\sigma) = 1 + v(\sigma)\Pi_{\mathfrak{P}}^{\nu-1}$$

The map $\sigma \mapsto v(\sigma)$ induces an injective homomorphism

$$I^{(\nu)}/I^{(\nu+1)} \longrightarrow k(\mathfrak{P}),$$

to the additive group of the field.
Therefore it becomes clear that $I^{(2)}$ is a p group (Here p is of course the characteristic of $k(\mathfrak{p})$) and actually it is the p-Sylow-subgroup.
Our extension $L_{\mathfrak{P}}$ is called tamely ramified if $I^{(2)}$ is trivial.
c)*Show that there is a maximal totally ramified, tamely ramified extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ and*

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \xrightarrow{\sim} k(\mathfrak{p})^{\times}.$$

d) Show that a tamely ramified abelian extension $L/\mathbb{Q}_p$ is contained in $\mathbb{Q}_p[\zeta_m]$ where $m = pm_0$ and m_0 prime to p

0.5.3 Adeles and Ideles

The adele ring of a global field

Let K be a global field let S_∞ be the set of archimedian places (this may be empty). For any place v let K_v be the completion, the finite (non archimedian places) are denoted by $\mathfrak{p}$,$\mathfrak{q}$, the completion at $\mathfrak{p}$ is denoted by $K_{\mathfrak{p}}$ and the discrete valuation ring in $K_{\mathfrak{p}}$ is denoted by $\mathcal{O}_{\mathfrak{p}}$, this is the projective limit over $\mathcal{O}/\mathfrak{p}^n$. (We drop the hat $\widehat{\mathcal{O}}$).
For any $S \supset S_\infty$ we put

$$\mathbb{A}_K^{(S)} = \prod_{v \in S} K_v \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}$$

This is a ring where addition and multiplication are defined componentwise.
If $S' \supset S$ then we have an inclusion $\mathbb{A}_K^{(S)} \subset \mathbb{A}_K^{(S')}$ and we define

$$\mathbb{A}_K = \bigcup_S \mathbb{A}_K^{(S)} = \{\underline{x} \mid \underline{x} \in \prod_{v \text{all places}} K_v, \exists S \text{ finite such that } x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} \text{ for all } \mathfrak{p} \notin S\}$$

We define a topology on $\mathbb{A}_K$: A basis for the family of open sets is given by subsets

$$U_S \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}$$

where S runs over all finite sets $S \supset S_\infty$ and $U_S \subset \prod_{v \in S} K_v$ is open.

Endowed with this topology $\mathbb{A}_K$ becomes a locally compact topological ring.

This is a consequence of the theorem of Tychonoff, but since the indexing set is countable we do not need the axiom of choice(or Zorn's lemma)

A subset $B \subset \mathbb{A}$ is compact if and only if we can find a finite set $S \supset S_\infty$ and a real number $T > 0$ such that $B \subset \mathbb{A}_K^{(S)}$ and for all $\underline{b} \in B$ we have $|b_v|_v < T$ for all $v \in S$

The idele group of a global field

The idele group $\mathbb{I}_K$ of K is the group of units of $\mathbb{A}_K$. We put

$$\mathbb{I}_K^{(S)} = \prod_{v \in S} K_v^\times \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}^\times$$

and then we define

$$\mathbb{I}_K = \bigcup_S \mathbb{I}_K^{(S)}.$$

We have a topology on $\mathbb{I}_K$, a basis for the open sets consists of sets of the form

$$V_S \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}^\times \subset \mathbb{I}_K$$

where $V_S \subset \prod_{v \in S} K_v^\times$ is an open subset.

Endowed with this topology $\mathbb{I}_K$ becomes a locally compact topological group.

A subset $C \subset \mathbb{I}_K$ is compact if and only if we can find a finite set $S \supset S_\infty$ and a real number $T > 1$ such that $C \subset \mathbb{I}_K^{(S)}$ and for all $\underline{b} \in C$ we have $1/T < |b_v|_v < T$ for all $v \in S$.
We have a homomorphism $|\ \ | : \mathbb{I}_K \longrightarrow \mathbb{R}_{>0}^\times$ this is the idele norm map and defined as

$$| \ | : \underline{x} \mapsto \prod_v |x_v|_v$$

The kernel of this homomorphism is $\mathbb{I}_K^{(1)}$, these are the ideles with idele norm 1. The image of $| \ |$ is equal to $\mathbb{R}_{>0}^\times$ if K is an algebraic number field. If $K \supset \mathbb{F}_q(t)$ is a function field then the image is a subgroup of $\{q^\nu\}$.
An element in $\mathbb{A}_K$ or $\mathbb{I}_K$ will be denoted by $\underline{x}$ it can be thought of as a vector with infinitely many components

$$\underline{x} = (\dots, x_v, \dots)_{v \text{ places of } K}$$

We have obvious (diagonal) embeddings $K \hookrightarrow \mathbb{A}_K$ and $K^\times \hookrightarrow \mathbb{I}_K$. The product formula implies that $K^\times \hookrightarrow \mathbb{I}_K^{(1)}$.
A subgroup Γ in a topological group G is called a *discrete* subgroup if every element $\gamma \in \Gamma$ has an open neighborhood U_γ such that $U_\gamma \cap \Gamma = \{\gamma\}$.

Theorem 0.5.2. *The subgroups $K \subset \mathbb{A}_K$ and $K^\times \subset \mathbb{I}_K$ are discrete. The quotients*

$$\mathbb{A}_K/K \text{ and } \mathbb{I}_K^{(1)}/K^\times$$

are compact.

The last assertion is equivalent to the the finiteness of the class number in conjunction with Dirichlets theorem on units. The theorem will be discussed in the lecture.

0.5.4 Metric lattices

A metric lattice is a pair (M,h) where M is a free $\mathbb{Z}$-module of finite rank n and where $h : M_\mathbb{R} = M \otimes \mathbb{R} \longrightarrow \mathbb{R}$ is a positive definite quadratic form.
The datum of such a form is essentially the same as an euclidian scalar product, we define

$$< x,y >_h = 1/2(f(x+y) - f(x) - f(y)) \tag{0.21}$$

then $< x,x >_h = h(x)$. We can define the length of a vector by $|x|_h = \sqrt{h(x)}$.
From our scalar product we also get a volume form vol_h on $M_\mathbb{R}$. The volume of the box spanned by a system of orhonormal vectors is one. If $\omega_1,\omega_2,\dots,\omega_n$ is a basis of our $\mathbb{Z}$-module M then we define

$$V((M,h)) = \mathrm{vol}_h\{\sum_i x_i\omega_i | 0 \le x_i \le 1\} \tag{0.22}$$

Let $B_n(r)$ be the ball of radius r in $M_\mathbb{R}$ in then $\mathrm{vol}_h(B_n(r)) = r^n \,\mathrm{vol}_h(B_n(1)) = r^n b_n$

Theorem 0.5.3. *For any metric lattice (M,h) any ball with radius $r > 2(\frac{V((M,h))}{b_n})^{\frac{1}{n}}$ contains a non zero lattice point.*

Proof: See Neukirch.

The space of isomorhism classes of lattices

It is of course clear what an isomorphism between two metric lattices $(M,h),(M_1,h_1)$ is: This simply an isomorphism $\phi : M \xrightarrow{\sim} M_1$ of the $\mathbb{Z}$-modules which induces an isometry $\phi_{\mathbb{R}} : M_{\mathbb{R}} \xrightarrow{\sim} M_{1,\mathbb{R}}$.
We also have the notion of conformal equivalence. If (M,h) is a metric lattice and $\alpha \neq 0$ is a real number, then we can consider the new lattice $\alpha M \subset M_{\mathbb{R}}$. The multiplication by α induces an isomorphism of $\mathbb{Z}$-lattices but this not an isometry, the metric is changed by a a scalar, we have $h(\alpha x) = \alpha^2 h(x)$.
It is clear that any conformal class of lattices contains a unique lattice with $V((M,h)) = 1$.
We also have the notion of an oriented metric lattice, this is a triple (M,h,Ω) where Ω is a generator of the rank one $\mathbb{Z}$-module $\Lambda^n(M)$.
If we choose a basis $\omega_1,\omega_2,\dots,\omega_n$ of our oriented module M (i.e. $\omega_1 \wedge \omega_2 \dots \omega_n = \Omega$) then we can form the positive definite $n \times n$ matrix $(<\omega_i,\omega_j>_h)$ it is symmetric and its determinant is $V((M,h,\Omega))$. If we replace our basis by another oriented one, i.e. we write

$$\omega'_i = \sum a_{ij}\omega_j \tag{0.23}$$

then the matrix $A = (a_{ij})$ is in $\mathrm{SL}_n(\mathbb{Z})$ and

$$(<\omega'_i,\omega'_j>_h) = A(<\omega_i,\omega_j>_h)^t A \tag{0.24}$$

Let X_n be the space of positive definite $n \times n$ matrices with coefficients in $\mathbb{R}$ and determinant equal to 1. On this set $\mathrm{SL}_n(\mathbb{Z})$ is acting as described above.

We have a bijection

$$\{\text{ The set isomorphism classes of oriented lattices of volume } 1\} \xrightarrow{\sim} \mathrm{SL}_n(\mathbb{Z})\backslash X$$

The metric lattice $(\mathcal{O}_K,B_{\mathrm{tr}}^{(+)})$.

Let $K/\mathbb{Q}$ be an algebraic number field, let $\mathcal{O}_K$ be its ring of algebraic integers, it is a free $\mathbb{Z}$ module. We have the trace $\mathrm{tr}_{K/\mathbb{Q}} : \mathcal{O}_K \longrightarrow \mathbb{Z}$. We have seen that this defines the non degenerate bilinear form

$$B_{\mathrm{tr}} : K \times K \longrightarrow \mathbb{Q} \tag{0.25}$$

The bilinear form B_{tr} extends to a bilinear form

$$B_{\mathrm{tr}} : K_\infty \times K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R} \times K \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow \mathbb{R}. \tag{0.26}$$

We know how to describe the $\mathbb{R}$-algebra K_∞: We look at the set of embeddings $\Sigma_K = \mathrm{Hom}(K,\mathbb{C})$. This set is the union of the set of real embeddings Σ_K^{real} and the set of complex embeddings $\Sigma_K^{\mathrm{complex}}$ On the second set we have the action of complex conjugation, the complex embeddings come in pairs $(\sigma,c \circ \sigma) = (\sigma,\bar{\sigma})$. We choose a representative for each of these pairs, this defines a subset $\Sigma_K^{(c,1)} \subset \Sigma_K^{\mathrm{complex}}$. We know that we can identify $\Sigma_K/$modulo conjugation $= \Sigma_K^{\mathrm{real}} \cup \Sigma_K^{(c,1)} = S_\infty$ the set of archimedian valuations. Then

$$K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_{\sigma:\Sigma_K^{\text{real}}} \mathbb{R} \oplus \bigoplus_{\sigma\in\Sigma_K^{(c,1)}} \mathbb{C} \tag{0.27}$$

The trace of an element $x \in K$ is given by $\mathrm{tr}_{K/\mathbb{Q}}(x) = \sum_{\sigma\in\Sigma_K} \sigma(x) = \sum_{\sigma\in\Sigma_K^{\text{real}}} \sigma(x) + \sum_{\Sigma_K^{(c,1)}} (\sigma(x) + c\circ\sigma(x)) = \sum_{\sigma\in\Sigma_K^{\text{real}}} \sigma(x) + \sum_{\Sigma_K^{(c,1)}} (\mathrm{tr}_{\mathbb{C}/\mathbb{R}}(\sigma(x))$.
Therefore the extension of the trace to $\mathrm{tr}_{K\infty/\mathbb{R}} : K_\infty \longrightarrow \mathbb{R}$ is given by

$$\mathrm{tr}_{K\infty/\mathbb{R}} : (\dots,x_\sigma,\dots) \mapsto \sum_{\sigma:\Sigma_K^{\text{real}}} x_\sigma + \sum_{\sigma\in\Sigma_K^{(c,1)}} \mathrm{tr}_{\mathbb{C}/\mathbb{R}}(x_\sigma). \tag{0.28}$$

For $\sigma \in \Sigma_K^{(c,1)}$ we decompose $x_\sigma = u_\sigma + iv_\sigma$ into its real and imaginary part. Then we get for the quadratic form defined by the trace

$$B_{\mathrm{tr}}(x) = \mathrm{tr}_{K_\infty/\mathbb{R}}(x^2) = \sum_{\sigma\in\Sigma_K^{\text{real}}} x_\sigma^2 + 2\sum_{\sigma\in\Sigma_K^{(c,1)}} (u_\sigma^2 - v_\sigma^2) \tag{0.29}$$

We modify B_{tr}: We put

$$B_{\mathrm{tr}}^{(+)}(x) = \mathrm{tr}_{K_\infty/\mathbb{R}}(x^2) = \sum_{\sigma\in\Sigma_K^{\text{real}}} x_\sigma^2 + 2\sum_{\sigma\in\Sigma_K^{(c,1)}} (u_\sigma^2 + v_\sigma^2) \tag{0.30}$$

and endowed with the quadratic form we get an arithmetic lattice $(\mathcal{O}_K, B_{\mathrm{tr}}^{(+)})$.
The two quadratic forms B_{tr} and $B_{\mathrm{tr}}^{(+)}$ define the same volume form hence we get

$$V((\mathcal{O}_K, B_{\mathrm{tr}}^{(+)})) = \mathrm{vol}_{B_{\mathrm{tr}}}(K_\infty/\mathcal{O}_K) = \sqrt{|D_{K/\mathbb{Q}}|} \tag{0.31}$$

If we write

$$K_\infty = \bigoplus_{S_\infty} K_v \tag{0.32}$$

where $K_v = \mathbb{R}$ for v real and $\mathbb{C}$ for v complex, then our form can also be written as

$$B_{\mathrm{tr}}^{(+)}(x) = \sum_{v \text{ real}} x_v^2 + 2\sum_{v \text{ complex}} x_v\bar{x}_v \tag{0.33}$$

Let $\underline{t}$ be an element from the group $\mathbb{I}_K$ of ideles. Using this element we define a new lattice

$$(\underline{t}_f\mathcal{O}_K, t_\infty B_{\mathrm{tr}}^{(+)}) \tag{0.34}$$

We describe this lattice: The idele $\underline{t}$ decomposes into its finite part and its component at infinity, we write

$$\underline{t} = (\underline{t}_\infty,\underline{t}_f) = \{\dots,t_v,\dots,t_{\mathfrak{p}},\dots\} \tag{0.35}$$

The new lattice will be

$$\underline{t}_f\mathcal{O}_K = \{x \in K \,|t_{\mathfrak{p}}^{-1}x \in \widehat{\mathcal{O}}_{\mathfrak{p}} \text{ for all finite places } \mathfrak{p}\} \tag{0.36}$$

(this modifies the lattice at a finite number of places because the set of $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(t_{\mathfrak{p}}) \neq 0$ is finite).
Remark: If we have $\mathrm{ord}_{\mathfrak{p}}(t_{\mathfrak{p}}) \geq 0$ for all $\mathfrak{p}$ then we have $\underline{t}_f\mathcal{O}_K \subset \mathcal{O}_K$ and it follows easily from the definitions

$$[\mathcal{O}_K : \underline{t}_f\mathcal{O}_K] = \prod_{\mathfrak{p}} |t_{\mathfrak{p}}|_{\mathfrak{p}}^{-1}$$

and this is equivalent to

$$V((\underline{t}_f\mathcal{O}_K,B_{\mathrm{tr}}^{(+)})) = V((\mathcal{O}_K,B_{\mathrm{tr}}^{(+)}))\prod_{\mathfrak{p}} |t_{\mathfrak{p}}|_{\mathfrak{p}}^{-1} \tag{0.37}$$

and clearly this is always true, independently of our assumption $\mathrm{ord}_{\mathfrak{p}} \geq 0$.

Now we also modify the metric, i.e. our quadratic form. We refer to (0.33)

$$(t_\infty B_{\mathrm{tr}}^{(+)})(x) = \sum_{v \text{ real}} t_v^{-2}x_\sigma^2 + 2\sum_{v \text{ complex}} (t_v\bar{t}_v)^{-1}x_v\bar{x}_v \tag{0.38}$$

It is clear that

$$V((\underline{t}_f\mathcal{O}_K,t_\infty B_{\mathrm{tr}}^{(+)}) = V_h((\mathcal{O}_K,B_{\mathrm{tr}}^{(+)})||\ \underline{t}\ ||^{-1} \tag{0.39}$$

where $||\ \underline{t}\ ||$ is the idele norm of $\underline{t}$. Hence for any idele $\underline{t}$ which has idele norm one, i.e. $\prod_v |t_v|_v = 1$ we get the equality

$$V_h((\underline{t}_f\mathcal{O}_K,t_\infty B_{\mathrm{tr}}^{(+)}) = \sqrt{D_{K/\mathbb{Q}}} \tag{0.40}$$

We observe that for an element $a \in K^\times$ the multiplication by a induces an isomorphism

$$(\underline{t}_f\mathcal{O}_K,t_\infty B_{\mathrm{tr}}^{(+)}) \xrightarrow{\sim} (a\underline{t}_f\mathcal{O}_K,(at_\infty)B_{\mathrm{tr}}^{(+)}).$$

From this we get easily the compactness of $\mathbb{I}_K(1)/K^\times$: Let $\underline{t} \in \mathbb{I}_K(1)$. The metric lattice $(\underline{t}_f\mathcal{O}_K,t_\infty B_{\mathrm{tr}}^{(+)})$ has a shortest non zero vector $a \in K$. We can modify $\underline{t}$ by an element $K^\times$ (product formula) and get an isomorphic metric lattice. Hence we may assume

that this shortest vector is the identity element 1. *(*)*

It follows from Minkowski‘s theorem that the square length of this vector $1 = (1,\dots,1,\dots) \in K_\infty$ is less than $4(\frac{|D_{K/\mathbb{Q}}|}{b_n^2})^{\frac{1}{n}} + \epsilon$, where $\epsilon > 0$ is arbitrarily small. Hence

$$\sum_{v \text{ real}} t_v^{-2} + 2\sum_{v \text{ complex}} (t_v\bar{t}_v)^{-1} < 4(\frac{|D_{K/\mathbb{Q}}|}{b_n^2})^{\frac{1}{n}} + \epsilon \tag{0.41}$$

This implies that there exists a constant $c_K > 0$ such that t_v^2 and $t_v\bar{t}_v > c_K$. We have the product formula

$$\prod_{v\in S_\infty} |t_v|_v \prod |t_\mathfrak{p}|_\mathfrak{p} = 1 \tag{0.42}$$

By our above assumption (*) we have $t_\mathfrak{p}^{-1}\cdot 1 \in \widehat{\mathcal{O}}_{K,\mathfrak{p}}$ and this implies that $\mathrm{ord}_\mathfrak{p}(t_\mathfrak{p}^{-1}) = n_\mathfrak{p} \geq 0$ and $|t_\mathfrak{p}|_\mathfrak{p} = \# k(\mathfrak{p})^{n_\mathfrak{p}} \geq 1$ for all $\mathfrak{p}$. Since in our last formula the product over the infinite places is bounded away from 0 by a constant $C_K > 0$ it follows that the product over the finite places can be estimated

$$1 \leq \prod |t_\mathfrak{p}|_\mathfrak{p} = \prod \# k(\mathfrak{p})^{n_\mathfrak{p}} \leq C_K^{-1} \tag{0.43}$$

We have only a finite set S' of finite places for which $\# k(\mathfrak{p}) \leq C_K^{-1}$ hence we have $n_\mathfrak{p} = 0$ for all $\mathfrak{p} \notin S'$. For $\mathfrak{p} \in S'$ we get

$$1 \leq |t_\mathfrak{p}|_\mathfrak{p} \leq C_K^{-1} \tag{0.44}$$

If $S = S_\infty \cup S'$ then we have shown that

$$\underline{t} \in \prod_{v\in S} K_v^\times \times \prod_{\mathfrak{p}\notin S} \widehat{\mathcal{O}}_{K,\mathfrak{p}}^\times$$

For $\mathfrak{p} \in S'$ we have (0.44) and for $v \in S_\infty$ we had $t_v^2, t_v\bar{t}_v > c_K > 0$. Then the product formula implies that we also have and estimate for the $|t_v|_v$ from above. This altogether proves that under the assumption (*) we can find a constant $0 < c < 1$ such that

$$\underline{t} \in \mathbb{I}_K^{(S)}[c] = \prod_{v\in S} K_v^\times[c] \times \prod_{\mathfrak{p}\notin S} \widehat{\mathcal{O}}_{K,\mathfrak{p}}^\times \tag{0.45}$$

where $K_v^\times[c] = \{x_v \in K_v^\times | c \leq |x_v|_v \leq c^{-1}\}$. This finishes the proof.

The growth of the Discriminant

Of course we have an explicit formula for the volume of the n-dimensional ball of radius 1:

$$b_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} \tag{0.46}$$

It is not so difficult to show that the identity element $1 \in K$ is a shortest vector in $(\mathcal{O}_K, B_{\mathrm{tr}}^{(+)})$. Clearly we have $B_{\mathrm{tr}}^{(+)}(1) = n$, this is the square of its length and (0.41) implies that

$$n < 4\Big(\frac{|D_{K/\mathbb{Q}}|}{\frac{\pi^n}{(\Gamma(\frac{n}{2}+1))^2}}\Big)^{\frac{1}{n}} + \epsilon \tag{0.47}$$

and this implies

$$|D_{K/\mathbb{Q}}| \geq n^n(\frac{\pi}{4})^n/(\Gamma(\frac{n}{2}+1))^2 \tag{0.48}$$

We apply the Stirling formula and find

$$|D_{K/\mathbb{Q}}| \geq \frac{e}{2n}(\frac{e\pi}{2})^{n-1}\cdot V_n \tag{0.49}$$

where V_n tends to one if n tends to infinity.
The estimate is weaker than the estimate in Neukirch's book, but one checks easily that the estimate in (0.48) implies that $|D_{K/\mathbb{Q}}| > 2$ unless we have $n = 1$ and this implies

Theorem 0.5.4. *There is no non trivial unramified extension of* $\mathbb{Q}$..

0.5.5 Numerics of ζ

The computations done in the lecture yield

$$\frac{\Gamma(\frac{s}{2})}{\pi^{\frac{s}{2}}}\zeta(s) = \frac{1}{\pi^{\frac{s}{2}}}\sum_{n=1}^{\infty}\frac{1}{n^s}\Gamma(\pi n^2 T,\frac{s}{2}) + \frac{1}{\pi^{\frac{1-s}{2}}}\sum_{n=1}^{\infty}\frac{1}{n^{1-s}}\Gamma(\frac{\pi n^2}{T},\frac{1-s}{2}) + \frac{1}{s-1}T^{\frac{s-1}{2}} - \frac{1}{s}T^{\frac{s}{2}} \tag{0.50}$$

where $\Gamma(s,A)$ is the incomplete Γ-function, it is defined by

$$\Gamma(s,A) = \int_A^\infty e^{-y}y^s\frac{dy}{y} \tag{0.51}$$

Exercise: a) Show that the two sums are very rapidly converging.
b) Show that $\Lambda(s) = \frac{\Gamma(\frac{s}{2})}{\pi^{\frac{s}{2}}}\zeta(s)$ assumes real values on the critical line $s = \frac{1}{2} + i\cdot t$
c) Use the formula to compute the values $\zeta(-1)$,$\zeta(-3)$ to a high precision. What do you observe?
d) Plot the function $\Lambda(\frac{1}{2} + i\cdot t)$ in the range $13 \leq t \leq 15$
e) Compute the first zero of $\zeta(s)$ on the critical line up to high accuracy.

Literature
[Ei] Eisenbud, D. *Commutative Algebra*
[L] Lang, S. *Algebraic Number Theory*
[N] Neukirch, J. *Algebraic Number Theory*

Updated versions of this text can be found in
`http://www.math.uni-bonn.de/people/harder/Manuscripts/buch/`