Algebraic Number Theory 2007/2008

1. Algebraic prerequisites

1.1. General

1.1.1.

Definition. For a field F define the ring homomorphism $\mathbb{Z} \to F$ by $n \mapsto n \cdot 1_F$. Its kernel I is an ideal of $\mathbb{Z}$ such that $\mathbb{Z}/I$ is isomorphic to the image of $\mathbb{Z}$ in F. The latter is an integral domain, so I is a prime ideal of $\mathbb{Z}$, i.e. $I = 0$ or $I = p\mathbb{Z}$ for a prime number p. In the first case F is said to have *characteristic 0*, in the second – *characteristic* p.

Definition–Lemma. Let F be a subfield of a field L. An element $a \in L$ is called *algebraic over* F if one of the following equivalent conditions is satisfied:
(i) $f(a) = 0$ for a non-zero polynomial $f(X) \in F[X]$;
(ii) elements $1, a, a^2, \dots$ are linearly dependent over F;
(iii) F-vector space $F[a] = \{\sum a_i a^i : a_i \in F\}$ is of finite dimension over F;
(iv) $F[a] = F(a)$.

Proof. (i) implies (ii): if $f(X) = \sum_{i=0}^n c_i X^i$, $c_0, c_n \neq 0$, then $\sum c_i a^i = 0$.
(ii) implies (iii): if $\sum_{i=0}^n c_i a^i = 0$, $c_n \neq 0$, then $a^n = -\sum_{i=0}^{n-1} c_n^{-1} c_i a^i$, $a^{n+1} = a \cdot a^n = -\sum_{i=0}^{n-1} c_n^{-1} c_i a^{i+1} = -\sum_{i=0}^{n-2} c_n^{-1} c_i a^{i+1} + c_n^{-1} c_{n-1} \sum_{i=0}^{n-1} c_n^{-1} c_i a^i$, etc.
(iii) implies (iv): for every $b \in F[a]$ we have $F[b] \subset F[a]$, hence $F[b]$ is of finite dimension over F. So if $b \notin F$, there are d_i such that $\sum d_i b^i = 0$, and $d_0 \neq 0$. Then $1/b = -d_0^{-1} \sum_{i=1}^n d_i b^{i-1}$ and hence $1/b \in F[b] \subset F[a]$.
(iv) implies (i): if $1/a$ is equal to $\sum e_i a^i$, then a is a root of $\sum e_i X^{i+1} - 1$.

For an element a algebraic over F denote by

$$f_a(X) \in F[X]$$

the monic polynomial of minimal degree such that $f_a(a) = 0$.

This polynomial is irreducible: if $f_a = gh$, then $g(a)h(a) = 0$, so $g(a) = 0$ or $h(a) = 0$, contradiction. It is called *the monic irreducible polynomial of* a *over* F.

For example, $f_a(X)$ is a linear polynomial iff $a \in F$.

Lemma. *Define a ring homomorphism* $F[X] \to L,\ g(X) \mapsto g(a)$. *Its kernel is the principal ideal generated by* $f_a(X)$ *and its image is* $F(a)$, *so*

$$F[X]/(f_a(X)) \simeq F(a).$$

Proof. The kernel consists of those polynomials g over F which vanish at a. Using the division algorithm write $g = f_a h + k$ where $k = 0$ or the degree of k is smaller than that of f_a. Now $k(a) = g(a) - f_a(a)h(a) = 0$, so the definition of f_a implies $k = 0$ which means that f_a divides g.

Definition. A field L is called *algebraic over* its subfield F if every element of L is algebraic over F. The extension L/F is called *algebraic*.

Definition. Let F be a subfield of a field L. The dimension of L as a vector space over F is called the *degree* $|L : F|$ of the extension L/F.

If a is algebraic over F then $|F(a) : F|$ is finite and it equals the degree of the monic irreducible polynomial f_a of a over F.

Transitivity of the degree $|L : F| = |L : M||M : F|$ follows from the observation: if α_i form a basis of M over F and β_j form a basis of L over M then $\alpha_i\beta_j$ form a basis of L over F.

Every extension L/F *of finite degree is algebraic*: if $\beta \in L$, then $|F(\beta) : F| \leqslant |L : F|$ is finite, so by (iii) above β is algebraic over F. In particular, if α is algebraic over F then $F(\alpha)$ is algebraic over F. If α, β are algebraic over F then the degree of $F(\alpha, \beta)$ over F does not exceed the product of finite degrees of $F(\alpha)/F$ and $F(\beta)/F$ and hence is finite. Thus all elements of $F(\alpha, \beta)$ are algebraic over F.

An algebraic extension $F(\{a_i\})$ of F is is the composite of extensions $F(a_i)$, and since a_i is algebraic $|F(a_i) : F|$ is finite, thus *every algebraic extension is the composite of finite extensions*.

1.1.2. Definition. An extension F of $\mathbb{Q}$ of finite degree is called an *algebraic number field*, the degree $|F : \mathbb{Q}|$ is called the *degree of* F.

Examples. 1. Every quadratic extension L of $\mathbb{Q}$ can be written as $\mathbb{Q}(\sqrt{e})$ for a square-free integer e. Indeed, if $1, \alpha$ is a basis of L over $\mathbb{Q}$, then $\alpha^2 = a_1 + a_2\alpha$ with rational a_i, so α is a root of the polynomial $X^2 - a_2X - a_1$ whose roots are of the form $a_2/2 \pm \sqrt{d}/2$ where $d \in \mathbb{Q}$ is the discriminant. Write $d = f/g$ with integer f, g and notice that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{dg^2}) = \mathbb{Q}(\sqrt{fg})$. Obviously we can get rid of all square divisors of fg without changing the extension $\mathbb{Q}(\sqrt{fg})$.

2. Cyclotomic extensions $\mathbb{Q}^m = \mathbb{Q}(\zeta_m)$ of $\mathbb{Q}$ where ζ_m is a primitive mth root of unity. If p is prime then the monic irreducible polynomial of ζ_p over $\mathbb{Q}$ is $X^{p-1} + \cdots + 1 = (X^p - 1)/(X - 1)$ of degree $p - 1$.

1.1.3. Definition. Let two fields L, L' contain a field F. A homo(iso)morphism $\sigma: L \to L'$ such that $\sigma|_F$ is the identity map is called a F-homo(iso)morphism of L into L'.

The set of all F-homomorphisms from L to L' is denoted by $\mathrm{Hom}_F(L, L')$. Notice that every F-homomorphism is injective: its kernel is an ideal of F and 1_F does not belong to it, so the ideal is the zero ideal. In particular, $\sigma(L)$ is isomorphic to L.

The set of all F-isomorphisms from L to L' is denoted by $\mathrm{Iso}_F(L, L')$.

Two elements $a \in L, a' \in L'$ are called *conjugate over* F if there is a F-homomorphism σ such that $\sigma(a) = a'$. If L, L' are algebraic over F and isomorphic over F, they are called *conjugate over* F.

Lemma. *(i) Any two roots of an irreducible polynomial over F are conjugate over F.*

(ii) An element a' is conjugate to a over F iff $f_{a'} = f_a$.

(iii) The polynomial $f_a(X)$ is divisible by $\prod(X - a_i)$ in $L[X]$, where a_i are all distinct conjugate to a elements over F, L is the field $F(\{a_i\})$ generated by a_i over F.

Proof. (i) Let $f(X)$ be an irreducible polynomial over F and a, b be its roots in a field extension of F. Then $f_a = f_b = f$ and we have an F-isomorphism

$$F(a) \simeq F[X]/(f_a(X)) = F[X]/(f_b(X)) \simeq F(b), \quad a \mapsto b$$

and therefore a is conjugate to b over F.

(ii) $0 = \sigma f_a(a) = f_a(\sigma a) = f_a(a')$, hence $f_a = f_{a'}$. If $f_a = f_{a'}$, use (i).

(iii) If a_i is a root of f_a then by the division algorithm $f_a(X)$ is divisible by $X - a_i$ in $L[X]$.

1.1.4. Definition. A field is called algebraically closed if it does not have algebraic extensions.

Theorem (without proof). *Every field F has an algebraic extension C which is algebraically closed. The field C is called an algebraic closure of F. Every two algebraic closures of F are isomorphic over F.*

Example. The field of rational numbers $\mathbb{Q}$ is contained in algebraically closed field $\mathbb{C}$. The maximal algebraic extension $\mathbb{Q}^a$ of $\mathbb{Q}$ is obtained as the subfield of complex numbers which contains all algebraic elements over $\mathbb{Q}$. The field $\mathbb{Q}^a$ is algebraically closed: if $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}^a$ then it is a root of a non-zero polynomial with finitely many coefficients, each of which is algebraic over $\mathbb{Q}$. Therefore α is algebraic over the field M generated by the coefficients. Then $M(\alpha)/M$ and $M/\mathbb{Q}$ are of finite degree, and hence α is algebraic over $\mathbb{Q}$, i.e. belongs to $\mathbb{Q}^a$. The degree $|\mathbb{Q}^a : \mathbb{Q}|$ is infinite, since $|\mathbb{Q}^a : \mathbb{Q}| \geqslant |\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$ for every prime p.

The field $\mathbb{Q}^a$ is is much smaller than $\mathbb{C}$, since its cardinality is countable whereas the cardinality of complex numbers is uncountable).

Everywhere below we denote by C an algebraically closed field containing F.

Elements of $\mathrm{Hom}_F(F(a), C)$ are in one-to-one correspondence with distinct roots of $f_a(X) \in F[X]$: for each such root a_i, as in the proof of (i) above we have $\sigma: F(a) \to C$, $a \mapsto a_i$; and conversely each such $\sigma \in \mathrm{Hom}_F(F(a), C)$ maps a to one of the roots a_i.

1.2. Galois extensions

1.2.1. Definition. A polynomial $f(X) \in F[X]$ is called *separable* if all its roots in C are distinct.

Recall that if a is a multiple root of $f(X)$, then $f'(a) = 0$. So a polynomial f is separable iff the polynomials f and f' don't have common roots.

Examples of separable polynomials. Irreducible polynomials over fields of characteristic zero, irreducible polynomials over finite fields.

Proof: if f is an irreducible polynomial over a field of characteristic zero, then its derivative f' is non-zero and has degree strictly smaller than f; and so if f has a multiple root, than a g.c.d. of f and f' would be of positive degree strictly smaller than f which contradicts the irreducibility of f. For the case of irreducible polynomials over finite fields see section 1.3.

Definition. Let L be a field extension of F. An element $a \in L$ is called *separable* over F if $f_a(X)$ is separable. The extension L/F is called *separable* if every element of L is separable over F.

Example. Every algebraic extension of a field of characteristic zero or a finite field is separable.

1.2.2. Lemma. *Let M be a field extension of F and L be a finite extension of M. Then every F-homomorphism $\sigma: M \to C$ can be extended to an F-homomorphism $\sigma': L \to C$.*

Proof. Let $a \in L \setminus M$ and $f_a(X) = \sum c_i X^i$ be the minimal polynomial of a over M. Then $(\sigma f_a)(X) = \sum \sigma(c_i) X^i$ is irreducible over σM. Let b be its root. Then $\sigma f_a = f_b$. Consider an F-homomorphism $\phi: M[X] \to C$, $\phi(\sum a_i X^i) = \sum \sigma(a_i) b^i$. Its image is $(\sigma M)(b)$ and its kernel is generated by f_a. Since $M[X]/(f_a(X)) \simeq M(a)$, ϕ determines an extension $\sigma'': M(a) \to C$ of σ. Since $|L : M(a)| < |L : M|$, by induction σ'' can be extended to an F-homomorphism $\sigma': L \to C$ such that $\sigma'|_M = \sigma$.

1.2.3. Theorem. *Let L be a finite separable extension of F of degree n. Then there exist exactly n distinct F-homomorphisms of L into C, i.e. $|\mathrm{Hom}_F(L, C)| = |L : F|$.*

Proof. The number of distinct F-homomorphisms of L into C is $\leqslant n$ is valid for any extension of degree n. To prove this, argue by induction on $|L : F|$ and use the fact that every F-homomorphism $\sigma: F(a) \to C$ sends a to one of roots of $f_a(X)$ and that root determines σ completely.

To show that there are n distinct F-homomorphisms for separable L/F consider first the case of $L = F(a)$. From separability we deduce that the polynomial $f_a(X)$ has n distinct roots a_i which give n distinct F-homomorphisms of L into C: $a \mapsto a_i$.

Now argue by induction on degree. For $a \in L \setminus F$ consider $M = F(a)$. There are $m = |M : F|$ distinct F-homomorphisms σ_i of M into C. Let $\sigma_i': L \to C$ be an extension of σ_i which exists according to 1.2.2. By induction there are n/m distinct $F(\sigma_i(a))$-homomorphisms τ_{ij} of $\sigma_i'(L)$ into C. Now $\tau_{ij} \circ \sigma_i'$ are distinct F-homomorphisms of L into C.

1.2.4. Proposition. *Every finite subgroup of the multiplicative group $F^\times$ of a field F is cyclic.*

Proof. Denote this subgroup by G, it is an abelian group of finite order. From the standard theorem on the stucture of finitely generated abelian groups we deduce that

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}$$

where m_1 divides m_2, etc. We need to show that $r = 1$ (then G is cyclic). If $r > 1$, then let a prime p be a divisor of m_1. The cyclic group $\mathbb{Z}/m_1\mathbb{Z}$ has p elements of order p and similarly, $\mathbb{Z}/m_2\mathbb{Z}$ has p elements of order p, so G has at least p^2 elements of order p. However, all elements of order p in G are roots of the polynomial $X^p - 1$ which over the field F cannot have more than p roots, a contradiction. Thus, $r = 1$.

1.2.5. Theorem. *Let F be a field of characteristic zero or a finite field. Let L be a finite field extension of F. Then there exists an element $a \in L$ such that $L = F(a) = F[a]$.*

Proof. If F is of characteristic 0, then F is infinite. By 1.2.3 there are $n = |L : F|$ distinct F-homomorphisms $\sigma_i: L \to C$. Put $V_{ij} = \{a \in L : \sigma_i(a) = \sigma_j(a)\}$. Then V_{ij} are proper F-vector subspaces of L for $i \neq j$ of dimension $< n$, and since F is infinite, there union $\cup_{i \neq j} V_{ij}$ is different from L. Then there is $a \in L \setminus (\cup V_{ij})$. Since the set $\{\sigma_i(a)\}$ is of cardinality n, the minimal polynomial of a over F has at least n distinct roots. Then $|F(a) : F| \geqslant n = |L : F|$ and hence $L = F(a)$.

If L is finite, then $L^\times$ is cyclic by 1.2.4. Let a be any of its generators. Then $L = F(a)$.

1.2.6. Definition. An algebraic extension L of F (inside C) is called the *splitting field of polynomials* f_i if $L = F(\{a_{ij}\})$ where a_{ij} are all the roots of f_i.

An algebraic extension L of F is called *a Galois extension* if L is the splitting field of some separable polynomials f_i over F.

Example. Let L be a finite extension of F such that $L = F(a)$. Then L/F is a Galois extension if the polynomial $f_a(X)$ of a over F has $\deg f_a$ distinct roots in L.

So quadratic extensions of $\mathbb{Q}$ and cyclotomic extensions of $\mathbb{Q}$ are Galois extensions.

1.2.7. Lemma. *Let L be the splitting field of an irreducible polynomial $f(X) \in F[X]$. Then $\sigma(L) = L$ for every $\sigma \in \mathrm{Hom}_F(L, C)$.*

Proof. σ permutes the roots of $f(X)$. Thus, $\sigma(L) = F(\sigma(a_1), \dots, \sigma(a_n)) = L$.

1.2.8. Theorem. *A finite extension L of F is a Galois extension iff*
$\sigma(L) = L$ for every $\sigma \in \mathrm{Hom}_F(L, C)$ and $|\mathrm{Hom}_F(L, L)| = |L : F|$.

The set $\mathrm{Hom}_F(L, L)$ equals to the set $\mathrm{Iso}_F(L, L)$ which is a finite group with respect to the composite of field isomorphisms. This group is called the Galois group $\mathrm{Gal}(L/F)$ of the extension L/F.

Sketch of the proof. Let L be a Galois extension of F. The right arrow follows from the previous proposition and properties of separable extensions. On the other hand, if $L = F(\{b_i\})$ and $\sigma(L) = L$ for every $\sigma \in \mathrm{Hom}_F(L, C)$ then $\sigma(b_i)$ belong to L and L is the splitting field of polynomials $f_{b_i}(X)$. If $|\mathrm{Hom}_F(L, L)| = |L : F|$ then one can show by induction that each of $f_{b_i}(X)$ is separable.

Now suppose we are in the situation of 1.2.5. Then $L = F(a)$ for some $a \in L$. L is the splitting field of some polynomials f_i over F, and hence L is the splitting field of their product. By 1.2.7 and induction we have $\sigma L = L$. Then $L = F(a_i)$ for any root a_i of f_a, and elements of $\mathrm{Hom}_F(L, L)$ correspond to $a \mapsto a_i$. Therefore $\mathrm{Hom}_F(L, L) = \mathrm{Iso}_F(L, L)$. Its elements correspond to some permutations of the set $\{a_i\}$ of all roots of $f_a(X)$.

1.2.9. Theorem (without proof). *Let L/F be a finite Galois extension and M be an intermediate field between F and L.*

Then L/M is a Galois extension with the Galois group

$$\mathrm{Gal}(L/M) = \{\sigma \in \mathrm{Gal}(L/F) : \sigma|_M = \mathrm{id}_M\}.$$

For a subgroup H of $\mathrm{Gal}(L/F)$ denote

$$L^H = \{x \in L : \sigma(x) = x \quad \text{for all } \sigma \in H\}.$$

This set is an intermediate field between L and F.

1.2.10. Main theorem of Galois theory (without proof). *Let L/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/F)$.*

Then $H \to L^H$ is a one-to-one correspondence between subgroups H of G and subfields of L which contain F; the inverse map is given by $M \to \mathrm{Gal}(L/M)$. We have $\mathrm{Gal}(L/M) = H$.

Normal subgroups H of G correspond to Galois extensions M/F and

$$\text{Gal}(M/F) \simeq G/H.$$

1.3. Finite fields

Every finite field F has positive characteristic, since the homomorphism $\mathbb{Z} \to F$ is not injective. Let F be of prime characteristic p. Then the image of $\mathbb{Z}$ in F can be identified with the finite field $\mathbb{F}_p$ consisting of p elements. If the degree of $F/\mathbb{F}_p$ is n, then the number of elements in F is p^n. By 1.2.4 the group $F^\times$ is cyclic of order $p^n - 1$, so every non-zero element of F is a root of the polynomial $X^{p^n-1} - 1$. Therefore, all p^n elements of F are all p^n roots of the polynomial $f_n(X) = X^{p^n} - X$. The polynomial f_n is separable, since its derivative in characteristic p is equal to $p^n X^{p^n-1} - 1 = -1$. Thus, F is the splitting field of f_n over $\mathbb{F}_p$. We conclude that $F/\mathbb{F}_p$ is a Galois extension of degree $n = |F : \mathbb{F}_p|$.

Lemma. *The Galois group of $F/\mathbb{F}_p$ is cyclic of order n: it is generated by an automorphism ϕ of F called the Frobenius automorphism:*

$$\phi(x) = x^p \quad \textit{for all } x \in F.$$

Proof. $\phi^m(x) = x^{p^m} = x$ for all $x \in F$ iff $n|m$.

On the other hand, for every $n \geqslant 1$ the splitting field of f_n over $\mathbb{F}_p$ is a finite field consisiting of p^n elements.

Thus,

Theorem. *For every n there is a unique (up to isomorphism) finite field $\mathbb{F}_{p^n}$ consisting of p^n elements; it is the splitting field of the polynomial $f_n(X) = X^{p^n} - X$. The finite extension $\mathbb{F}_{p^{nm}}/\mathbb{F}_{p^n}$ is a Galois extension with cyclic group of degree m generated by the Frobenius automorphism $\phi_n\colon x \mapsto x^{p^n}$.*

Lemma. *Let $g(X)$ be an irreducible polynomial of degree m over a finite field $\mathbb{F}_{p^n}$. Then $g(X)$ divides $f_{nm}(X)$ and therefore is a separable polynomial.*

Proof. Let a be a root of $g(X)$. Then $\mathbb{F}_{p^n}(a)/\mathbb{F}_{p^n}$ is of degree m, so $\mathbb{F}_{p^n}(a) = \mathbb{F}_{p^{nm}}$. Since a is a root of $f_{nm}(X)$, g divides f_{nm}. The latter is separable and so is g.

2. Integrality

2.1. Integrality over rings

2.1.1. Proposition – Definition. Let B be an integral domain and A be its subring.

An element $b \in B$ is called *integral over* A if it satisfies one of the following equivalent conditions:

(i) there exist $a_i \in A$ such that $f(b) = 0$ where $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$;

(ii) the subring of B generated by A and b is an A-module of finite type;

(iii) there exists a subring C of B which contains A and b and which is an A-module of finite type.

Proof. (i) ⇒ (ii): note that the subring $A[b]$ of B generated by A and b coincides with the A-module M generated by $1, \ldots, b^{n-1}$. Indeed,

$$b^{n+j} = -a_0 b^j - \cdots - b^{n+j-1}$$

and by induction $b^j \in M$.

(ii) ⇒ (iii): obvious.

(iii) ⇒ (i): let $C = c_1A + \cdots + c_mA$. Then $bc_i = \sum_j a_{ij}c_j$, so $\sum_j (\delta_{ij}b - a_{ij})c_j = 0$. Denote by d the determinant of $M = (\delta_{ij}b - a_{ij})$. Note that $d = f(b)$ where $f(X) \in A[X]$ is a monic polynomial. From linear algebra we know that $dE = M^*M$ where M^* is the adjugate matrix to M and E is the identity matrix of the same order of that of M. Denote by $\mathcal{C}$ the column consisting of c_j. Now we get $M\mathcal{C} = 0$ implies $M^*M\mathcal{C} = 0$ implies $dE\mathcal{C} = 0$ implies $d\mathcal{C} = 0$. Thus $dc_j = 0$ for all $1 \leqslant j \leqslant m$. Every $c \in C$ is a linear combination of c_j. Hence $dc = 0$ for all $c \in C$. In particular, $d1 = 0$, so $f(b) = d = 0$.

Examples. 1. Every element of A is integral over A.

2. If A, B are fields, then an element $b \in B$ is integral over A iff b is algebraic over A.

3. Let $A = \mathbb{Z}$, $B = \mathbb{Q}$. A rational number r/s with relatively prime r and s is integral over $\mathbb{Z}$ iff $(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$ for some integer a_i. Multiplying by s^n we deduce that s divides r^n, hence $s = \pm 1$ and $r/s \in \mathbb{Z}$. Hence integral in $\mathbb{Q}$ elements over $\mathbb{Z}$ are just all integers.

4. If B is a field, then it contains the field of fractions F of A. Let $\sigma \in \mathrm{Hom}_F(B, C)$ where C is an algebraically closed field containing B. If $b \in B$ is integral over A, then $\sigma(b) \in \sigma(B)$ is integral over A.

5. If $b \in B$ is a root of a non-zero polynomial $f(X) = a_nX^n + \cdots \in A[X]$, then $a_n^{n-1}f(b) = 0$ and $g(a_nb) = 0$ for $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_n^{n-1}a_0$,

$g(a_nX) = a_n^{n-1}f(X)$. Hence a_nb is integral over A. Thus, for every algebraic over A element b of B there is a non-zero A-multiple ab which is integral over A.

2.1.2. Corollary. *Let A be a subring of an integral domain B. Let I be an A-module of finite type, $I \subset B$. Let $b \in B$ satisfy the property $bI \subset I$. Then b is integral over A.*

Proof. Indeed, as in the proof of $(iii) \Rightarrow (i)$ we deduce that $dc = 0$ for all $c \in I$. Since B is an integral domain, we deduce that $d = 0$, so $d = f(b) = 0$.

2.1.3. Proposition. *Let A be a subring of a ring B, and let $b_i \in B$ be such that b_i is integral over $A[b_1, \dots, b_{i-1}]$ for all i. Then $A[b_1, \dots, b_n]$ is an A-module of finite type.*

Proof. Induction on n. $n = 1$ is the previous proposition. If $C = A[b_1, \dots, b_{n-1}]$ is an A-module of finite type, then $C = \sum_{i=1}^m c_iA$. Now by the previous proposition $C[b_n]$ is a C-module of finite type, so $C[b_n] = \sum_{j=1}^l d_jC$. Thus, $C[b_n] = \sum_{i,j} d_jc_iA$ is an A-module of finite type.

2.1.4. Corollary 1. *If $b_1, b_2 \in B$ are integral over A, then $b_1 + b_2, b_1 - b_2, b_1b_2$ are integral over A.*

Certainly b_1/b_2 isn't necessarily integral over A.

Corollary 2. *The set B' of elements of B which are integral over A is a subring of B containing A.*

Definition. B' is called the *integral closure of A in B*. If A is an integral domain and B is its field of fractions, B' is called the *integral closure of A*.

A ring A is called *integrally closed* if A is an integral domain and A coincides with its integral closure in its field of fractions.

Let F be an algebraic number field. The integral closure of $\mathbb{Z}$ in F is called the *ring O_F of (algebraic) integers of F*.

Examples. 1. A UFD is integrally closed. Indeed, if $x = a/b$ with relatively prime $a, b \in A$ is a root of polynomial $f(X) = X^n + \dots + a_0 \in A[X]$, then b divides a^n, so b is a unit of A and $x \in A$.

In particular, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

2. O_F is integrally closed (see below in 2.1.6).

2.1.5. Lemma. *Let A be integrally closed. Let B be a field. Then an element $b \in B$ is integral over A iff the monic irreducible polynomial $f_b(X) \in F[X]$ over the fraction field F of A has coefficients in A.*

Proof. Let L be a finite extension of F which contains B and all $\sigma(b)$ for all F-homomorphisms from B to an algebraically closed field C. Since $b \in L$ is integral over A, $\sigma(b) \in L$ is integral over A for every σ. Then $f_b(X) = \prod(X - \sigma(b))$ has coefficients in F which belong to the ring generated by A and all $\sigma(b)$ and therefore are integral over A. Since A is integrally closed, $f_b(X) \in A[X]$.

If $f_b(X) \in A[X]$ then b is integral over A by 2.1.1.

Examples. 1. Let F be an algebraic number field. Then an element $b \in F$ is integral iff its monic irreducible polynomial has integer coefficients.

For example, $\sqrt{d}$ for integer d is integral.

If $d \equiv 1 \mod 4$ then the monic irreducible polynomial of $(1+\sqrt{d})/2$ over $\mathbb{Q}$ is $X^2 - X + (1-d)/4 \in \mathbb{Z}[X]$, so $(1+\sqrt{d})/2$ is integral. Note that $\sqrt{d}$ belongs to $\mathbb{Z}[(1+\sqrt{d})/2]$, and hence $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{Z}[(1+\sqrt{d})/2]$.

Thus, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ contains the subring $\mathbb{Z}[\sqrt{d}]$ and the subring $\mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \mod 4$. We show that there are no other integral elements.

An element $a + b\sqrt{d}$ with rational a and $b \neq 0$ is integral iff its monic irreducible polynomial $X^2 - 2aX + (a^2 - db^2)$ belongs to $\mathbb{Z}[X]$. Therefore $2a, 2b$ are integers. If $a = (2k+1)/2$ for an integer k, then it is easy to see that $a^2 - db^2 \in \mathbb{Z}$ iff $b = (2l+1)/2$ with integer l and $(2k+1)^2 - d(2l+1)^2$ is divisible by 4. The latter implies that d is a quadratic residue mod 4, i.e. $d \equiv 1 \mod 4$. In turn, if $d \equiv 1 \mod 4$ then every element $(2k+1)/2 + (2l+1)\sqrt{d}/2$ is integral.

Thus, integral elements of $\mathbb{Q}(\sqrt{d})$ are equal to

$$\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \mod 4 \\ \mathbb{Z}[(1+\sqrt{d})/2] & \text{if } d \equiv 1 \mod 4 \end{cases}$$

2. $O_{\mathbb{Q}^m}$ is equal to $\mathbb{Z}[\zeta_m]$ (see section 2.4).

2.1.6. Definition. B is said to be *integral over* A if every element of B is integral over A. If B is of characteristic zero, its elements integral over $\mathbb{Z}$ are called *integral elements* of B.

Lemma. *If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $c \in C$ be a root of the polynomial $f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$ with $b_i \in B$. Then c is integral over $A[b_0, \ldots, b_{n-1}]$. Since $b_i \in B$ are integral over A, proposition 2.1.3 implies that $A[b_0, \ldots, b_{n-1}, c]$ is an A-module of finite type. From 2.1.1 we conclude that c is integral over A.

Corollary. O_F *is integrally closed*

Proof. An element of F integral over O_F is integral over $\mathbb{Z}$ due to the previous lemma.

2.1.7. Proposition. *Let B be an integral domain and A be its subring such that B is integral over A. Then B is a field iff A is a field.*

Proof. If A is a field, then $A[b]$ for $b \in B \setminus 0$ is a vector space of finite dimension over A, and the A-linear map $\varphi\colon A[b] \to A[b], \varphi(c) = bc$ is injective, therefore surjective, so b is invertible in B.

If B is a field and $a \in A \setminus 0$, then the inverse $a^{-1} \in B$ satisfies $a^{-n} + a_{n-1}a^{-n+1} + \dots + a_0 = 0$ with some $a_i \in A$. Then $a^{-1} = -a_{n-1} - \dots - a_0 a^{n-1}$, so $a^{-1} \in A$.

2.2. Norms and traces

2.2.1. Definition. Let A be a subring of a ring B such that B is a free A-module of finite rank n. For $b \in B$ its trace $\mathrm{Tr}_{B/A}(b)$, norm $N_{B/A}(b)$ and characteristic polynomial $g_b(X)$ are the trace, the norm and the characteristic polynomial of the linear operator $m_b\colon B \to B$, $m_b(c) = bc$. In other words, if M_b is a matrix of the operator m_b with respect to a basis of B over A, then $g_b(X) = \det(XE - M_b)$, $\mathrm{Tr}_{B/A}(b) = \mathrm{Tr}\, M_b$, $N_{B/A} = \det M_b$.

If $g_b(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ then from the definition $a_{n-1} = -\mathrm{Tr}_{B/A}(b)$, $a_0 = (-1)^n N_{B/A}(b)$.

2.2.2. First properties.

$$\mathrm{Tr}(b + b') = \mathrm{Tr}(b) + \mathrm{Tr}(b'), \mathrm{Tr}(ab) = a\,\mathrm{Tr}(b), \mathrm{Tr}(a) = na,$$
$$N(bb') = N(b)N(b'), N(ab) = a^n N(b), N(a) = a^n$$

for $a \in A$.

2.2.3. Everywhere below in this section F is either a finite field of a field of characteristic zero. Then every finite extension of F is separable.

Proposition. *Let L be an algebraic extension of F of degree n. Let $b \in L$ and $b_1, \dots, b_n$ be roots of the monic irreducible polynomial of b over F each one repeated $|L : F(b)|$ times. Then the characteristic polynomial $g_b(X)$ of b with respect to L/F is $\prod(X - b_i)$, and $\mathrm{Tr}_{L/F}(b) = \sum b_i, N_{L/F}(b) = \prod b_i$.*

Proof. If $L = F(b)$, then use the basis $1, b, \dots, b^{n-1}$ to calculate g_b. Let $f_b(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0$ be the monic irreducible polynomial of b over F, then the matrix of m_b is

$$M_b = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -c_0 & -c_1 & -c_2 & \dots & -c_{n-1} \end{pmatrix}.$$

Hence $g_b(X) = \det(XE - M_b) = f_b(X)$ and $\det M_b = \prod b_i$, $\operatorname{Tr} M_b = \sum b_i$.

In the general case when $|F(b) : F| = m < n$ choose a basis $\omega_1, \dots, \omega_{n/m}$ of L over $F(b)$ and take $\omega_1, \dots, \omega_1 b^{m-1}, \omega_2, \dots, \omega_2 b^{m-1}, \dots$ as a basis of L over F. The matrix M_b is a block matrix with the same block repeated n/m times on the diagonal and everything else being zero. Therefore, $g_b(X) = f_b(X)^{|L:F(b)|}$ where $f_b(X)$ is the monic irreducible polynomial of b over F.

Example. Let $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$ with square-free integer d. Then

$$g_{a+b\sqrt{d}}(X) = (X - a - b\sqrt{d})(X - a + b\sqrt{d}) = X^2 - 2aX + (a^2 - db^2),$$

so

$$\operatorname{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = 2a, \quad N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2.$$

In particular, an integer number c is a sum of two squares iff $c \in N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}} O_{\mathbb{Q}(\sqrt{-1})}$.

More generally, c is in the form $a^2 - db^2$ with integer a, b and square-free d not congruent to $1 \mod 4$ iff

$$c \in N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} \mathbb{Z}[\sqrt{d}]$$

2.2.4. Corollary 1. *Let σ_i be distinct F-homomorphisms of L into C. Then* $\operatorname{Tr}_{L/F}(b) = \sum \sigma_i b$, $N_{L/F}(b) = \prod \sigma_i(b)$.

Proof. In the previous proposition $b_i = \sigma_i(b)$.

Corollary 2. *Let A be an integral domain, F be its field of fractions. Let L be an extension of F of finite degree. Let A' be the integral closure of A in F. Then for an integral element $b \in L$ over A $g_b(X) \in A'[X]$ and $\operatorname{Tr}_{L/F}(b), N_{L/F}(b)$ belong to A'.*

Proof. All b_i are integral over A.

Corollary 3. *If, in addition, A is integrally closed, then $\operatorname{Tr}_{L/F}(b), N_{L/F}(b) \in A$.*

Proof. Since A is integrally closed, $A' \cap F = A$.

2.2.5. Lemma. *Let F be a finite field of a field of characteristic zero. If L is a finite extension of F and M/F is a subextension of L/F, then the following transitivity* *property holds*

$$\mathrm{Tr}_{L/F} = \mathrm{Tr}_{M/F} \circ \mathrm{Tr}_{L/M}, \qquad N_{L/F} = N_{M/F} \circ N_{L/M}.$$

Proof. Let $\sigma_1, \dots, \sigma_m$ be all distinct F-homomorphisms of M into C ($m = |M : F|$). Let $\tau_1, \dots, \tau_{n/m}$ be all distinct M-homomorphisms of L into C ($n/m = |L : M|$). The field $\tau_j(L)$ is a finite extension of F, and by 1.2.5 there is an element $a_j \in C$ such that $\tau_j(L) = F(a_j)$. Let E be the minimal subfield of C containing M and all a_j. Using 1.2.3 extend σ_i to $\sigma_i' \colon E \to C$. Then the composition $\sigma_i' \circ \tau_j \colon L \to C$ is defined. Note that $\sigma_i' \circ \tau_j = \sigma_{i_1}' \circ \tau_{j_1}$ implies $\sigma_i = \sigma_i' \circ \tau_j|_M = \sigma_{i_1}' \circ \tau_{j_1}|_M = \sigma_{i_1}$, so $i = i_1$, and then $j = j_1$. Hence $\sigma_i' \circ \tau_j$ for $1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n/m$ are all n distinct F-homomorphisms of L into C. By Corollary 3 in 2.2.4

$$N_{M/F}(N_{L/M}(b)) = N_{M/F}(\prod \tau_j(b)) = \prod \sigma_i'(\prod \tau_j(b)) = \prod (\sigma_i' \circ \tau_j)(b) = N_{L/F}(b).$$

Similar arguments work for the trace.

2.3. Integral basis

2.3.1. Definition. Let A be a subring of a ring B such that B is a free A-module of rank n. Let $b_1, \dots, b_n \in B$. Then the *discriminant* $D(b_1, \dots, b_n)$ is defined as $\det(\mathrm{Tr}_{B/A}(b_i b_j))$.

2.3.2. Proposition. *If* $c_i \in B$ *and* $c_i = \sum a_{ij} b_j$, $a_{ij} \in A$, *then* $D(c_1, \dots, c_n) = (\det(a_{ij}))^2 D(b_1, \dots, b_n)$.

Proof. $(c_i)^t = (a_{ij})(b_j)^t$, $(c_k c_l) = (c_k)^t (c_l) = (a_{ki})(b_i b_j)(a_{lj})^t$,
$(\mathrm{Tr}(c_k c_l)) = (a_{ki})(\mathrm{Tr}(b_i b_j))(a_{lj})^t$.

2.3.3. Definition. The *discriminant* $\mathcal{D}_{B/A}$ of B over A is the principal ideal of A generated by the discriminant of any basis of B over A.

2.3.4. Proposition. *Let* $\mathcal{D}_{B/A} \neq 0$. *Let* B *be an integral domain. Then a set* $b_1, \dots, b_n$ *is a basis of* B *over* A *iff* $D(b_1, \dots, b_n)A = \mathcal{D}_{B/A}$.

Proof. Let $D(b_1, \dots, b_n)A = \mathcal{D}_{B/A}$. Let $c_1, \dots, c_n$ be a basis of B over A and let $b_i = \sum_j a_{ij} c_j$. Then $D(b_1, \dots, b_n) = \det(a_{ij})^2 D(c_1, \dots, c_n)$. Denote $d = D(c_1, \dots, c_n)$.

Since $D(b_1, \dots, b_n)A = D(c_1, \dots, c_n)A$, we get $aD(b_1, \dots, b_n) = d$ for some $a \in A$. Then $d(1 - a\det(a_{ij})^2) = 0$ and $\det(a_{ij})$ is invertible in A, so the matrix (a_{ij}) is invertible in the ring of matrices over A. Thus $b_1, \dots, b_n$ is a basis of B over A.

2.3.5. Proposition. *Let F be a finite field or a field of characteristic zero. Let L be an extension of F of degree n and let $\sigma_1, \dots, \sigma_n$ be distinct F-homomorphisms of L into C. Let $b_1, \dots, b_n$ be a basis of L over F. Then*

$$D(b_1, \dots, b_n) = \det(\sigma_i(b_j))^2 \neq 0.$$

Proof. $\det(\mathrm{Tr}(b_i b_j)) = \det(\sum_k \sigma_k(b_i)\sigma_k(b_j)) = \det((\sigma_k(b_i))^t(\sigma_k(b_j))) = \det(\sigma_i(b_j))^2$. If $\det(\sigma_i(b_j)) = 0$, then there exist $a_i \in L$ not all zero such that $\sum_i a_i\sigma_i(b_j) = 0$ for all j. Then $\sum_i a_i\sigma_i(b) = 0$ for every $b \in L$.

Let $\sum a_i'\sigma_i(b) = 0$ for all $b \in L$ with the minimal number of non-zero $a_i' \in A$. Assume $a_1' \neq 0$.

Let $c \in L$ be such that $L = F(c)$ (see 1.2.5), then $\sigma_1(c) \neq \sigma_i(c)$ for $i > 1$.

We now have $\sum a_i'\sigma_i(bc) = \sum a_i'\sigma_i(b)\sigma_i(c) = 0$. Hence $\sigma_1(c)(\sum a_i'\sigma_i(b)) - \sum a_i'\sigma_i(b)\sigma_i(c) = \sum_{i>1} a_i'(\sigma_1(c) - \sigma_i(c))\sigma_i(b) = 0$. Put $a_i'' = a_i'(\sigma_1(c) - \sigma_i(c))$, so $\sum a_i''\sigma_i(b) = 0$ with smaller number of non-zero a_i'' than in a_i', a contradiction.

Corollary. *Under the assumptions of the proposition the linear map $L \to \mathrm{Hom}_F(L, F)$: $b \to (c \to \mathrm{Tr}_{L/F}(bc))$ between n-dimensional F-vector spaces is injective, and hence bijective. Therefore for a basis $b_1, \dots, b_n$ of L/F there is a dual basis $c_1, \dots, c_n$ of L/F, i.e. $\mathrm{Tr}_{L/F}(b_i c_j) = \delta_{ij}$.*

Proof. If $b = \sum a_i b_i$, $a_i \in F$ and $\mathrm{Tr}_{L/F}(bc) = 0$ for all $c \in L$, then we get equations $\sum a_i \,\mathrm{Tr}_{L/F}(b_i b_j) = 0$ – this is a system of linear equations in a_i with nondegenerate matrix $\mathrm{Tr}_{L/F}(b_i b_j)$, so the only solution is $a_i = 0$. Elements of the dual basis c_j correspond to $f_j \in \mathrm{Hom}_F(L, F)$, $f_j(b_i) = \delta_{ij}$.

2.3.6. Theorem. *Let A be an integrally closed ring and F be its field of fractions. Let L be an extension of F of degree n and A' be the integral closure of A in L. Let F be of characteristic 0. Then A' is an A-submodule of a free A-module of rank n.*

Proof. Let $e_1, \dots, e_n$ be a basis of F-vector space L. Then due to Example 5 in 2.1.1 there is $0 \neq a_i \in A$ such that $a_i e_i \in A'$. Then for $a = \prod a_i$ we get $b_i = a e_i \in A'$ form a basis of L/F.

Let $c_1, \dots, c_n$ be the dual basis for $b_1, \dots, b_n$. Claim: $A' \subset \sum c_i A$. Indeed, let $c = \sum a_i c_i \in A'$. Then

$$\mathrm{Tr}_{L/F}(cb_i) = \sum_j a_j \,\mathrm{Tr}_{L/F}(c_j b_i) = a_i \in A$$

by 2.2.5. Now $\sum c_i A = \oplus c_i A$, since $\{c_i\}$ is a basis of L/F.

2.3.7. Theorem (on integral basis). *Let A be a principal ideal ring and F be its field of fractions of characteristic 0. Let L be an extension of F of degree n. Then the integral closure A' of A in L is a free A-module of rank n.*

In particular, the ring of integers O_F of a number field F is a free $\mathbb{Z}$-module of rank equal to the degree of F.

Proof. The description of modules of finite type over PID and the previous theorem imply that A' is a free A-module of rank $m \leqslant n$. On the other hand, by the first part of the proof of the previous theorem A' contains n A-linear independent elements over A. Thus, $m = n$.

Definition. The discriminant d_F of any integral basis of O_F is called *the discriminant of* F. Since every two integral bases are related via an invertible matrix with integer coefficients (whose determinant is therefore ± 1), 2.3.2 implies that d_F is uniquely determined.

2.3.8. Examples. 1. Let d be a square-free integer. By 2.1.5 the ring of integers of $\mathbb{Q}(\sqrt{d})$ has an integral basis $1, \alpha$ where $\alpha = \sqrt{d}$ if $D \not\equiv 1 \mod 4$ and $\alpha = (1+\sqrt{d})/2$ if $d \equiv 1 \mod 4$.

The discriminant of $\mathbb{Q}(\sqrt{d})$ is equal to

$$4d \quad \text{if } d \not\equiv 1 \mod 4, \qquad \text{and } d \quad \text{if } d \equiv 1 \mod 4 .$$

To prove this calculate directly $D(1, \alpha)$ using the definitions, or use 2.3.9.

2. Let F be an algebraic number field of degree n and let $a \in F$ be an integral element over $\mathbb{Z}$. Assume that $D(1, a, \dots, a^{n-1})$ is a square free integer. Then $1, a, \dots, a^{n-1}$ is a basis of O_F over $\mathbb{Z}$, so $O_F = \mathbb{Z}[a]$. Indeed: choose a basis $b_1, \dots, b_n$ of O_F over $\mathbb{Z}$ and let $\{c_1, \dots, c_n\} = \{1, a, \dots, a^{n-1}\}$. Let $c_i = \sum a_{ij} b_j$. By 2.3.2 we have $D(1, a, \dots, a^{n-1}) = (\det(a_{ij})^2 D(b_1, \dots, b_n)$. Since $D(1, a, \dots, a^{n-1})$ is a square free integer, we get $\det(a_{ij}) = \pm 1$, so (a_{ij}) is invertible in $M_n(\mathbb{Z})$, and hence $1, a, \dots, a^{n-1}$ is a basis of O_F over $\mathbb{Z}$.

2.3.9. Example. Let F be of characteristic zero and $L = F(b)$ be an extension of degree n over F. Let $f(X)$ be the minimal polynomial of b over F whose roots are b_i. Then

$$f(X) = \prod (X - b_j), \qquad f'(b_i) = \prod_{j \neq i} (b_i - b_j),$$

$$N_{L/F} f'(b) = \prod_i f'(\sigma_i b) = \prod_i f'(b_i).$$

Then

$$\begin{aligned} D(1, b, \dots, b^{n-1}) &= \det(b_i^j)^2 \\ &= (-1)^{n(n-1)/2} \prod_{i \neq j} (b_i - b_j) = (-1)^{n(n-1)/2} N_{L/F}(f'(b)). \end{aligned}$$

Let $f(X) = X^n + aX + c$. Then

$$b^n = -ab - c, \qquad b^{n-1} = -a - cb^{-1}$$

and

$$e = f'(b) = nb^{n-1} + a = n(-a - cb^{-1}) + a,$$

so

$$b = -nc(e + (n-1)a)^{-1}.$$

The minimal polynomial $g(Y)$ of e over F corresponds to the minimal polynomial $f(X)$ of b; it is the numerator of $c^{-1}f(-nc(y + (n-1)a)^{-1})$, i.e.

$$g(Y) = (Y + (n-1)a)^n - na(Y + (n-1)a)^{n-1} + (-1)^n n^n c^{n-1}.$$

Hence

$$\begin{aligned} N_{L/F}(f'(b)) &= g(0)(-1)^n \\ &= n^n c^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n, \end{aligned}$$

so

$$\begin{aligned} &D(1, b, \dots, b^{n-1}) \\ &= (-1)^{n(n-1)/2}(n^n c^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n). \end{aligned}$$

For $n = 2$ one has $a^2 - 4c$, for $n = 3$ one has $-27c^2 - 4a^3$.

For example, let $f(X) = X^3 + X + 1$. It is irreducible over $\mathbb{Q}$. Its discriminant is equal to (-31), so according to example 2.5.3 $O_F = \mathbb{Z}[a]$ where a is a root of $f(X)$ and $F = \mathbb{Q}[a]$.

2.4. Cyclotomic fi elds

2.4.1. Definition. Let ζ_n be a primitive nth root of unity. The field $\mathbb{Q}(\zeta_n)$ is called the (nth) cyclotomic field.

2.4.2. Theorem. *Let p be a prime number and z be a primitive pth root of unity. The cyclotomic field $\mathbb{Q}(\zeta_p)$ is of degree $p-1$ over $\mathbb{Q}$. Its ring of integers coincides with $\mathbb{Z}[\zeta_p]$.*

Proof. Denote $z = \zeta_p$. Let $f(X) = (X^p - 1)/(X - 1) = X^{p-1} + \dots + 1$. Recall that $z - 1$ is a root of the polynomial $g(Y) = f(1 + Y) = Y^{p-1} + \dots + p$ is a p-Eisenstein polynomial, so $f(X)$ is irreducible over $\mathbb{Q}$, $|\mathbb{Q}(z) : \mathbb{Q}| = p - 1$ and $1, z, \dots, z^{p-2}$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}(z)$.

Let O be the ring of integers of $\mathbb{Q}(z)$. Since the monic irreducible polynomial of z over $\mathbb{Q}$ has integer coefficients, $z \in O$. Since z^{-1} is a primitive root of unity, $z^{-1} \in O$. Thus, z is a unit of O.

Then $z^i \in O$ for all $i \in \mathbb{Z}$ ($z^{-1} = z^{p-1}$). We have $1 - z^i = (1-z)(1 + \dots + z^{i-1}) \in (1-z)O$.

Denote by Tr and N the trace and norm for $\mathbb{Q}(z)/\mathbb{Q}$. Note that $\mathrm{Tr}(z) = -1$ and since z^i for $1 \leqslant i \leqslant p-1$ are primitive pth roots of unity, $\mathrm{Tr}(z^i) = -1$; $\mathrm{Tr}(1) = p-1$. Hence

$$\mathrm{Tr}(1 - z^i) = p \quad \text{for } 1 \leqslant i \leqslant p - 1\,.$$

Furthermore, $N(z-1)$ is equal to the free term of $g(Y)$ times $(-1)^{p-1}$, so $N(z-1) = (-1)^{p-1}p$ and

$$N(1 - z) = \prod_{1\leqslant i\leqslant p-1} (1 - z^i) = p,$$

since $1 - z^i$ are conjugate to $1 - z$ over $\mathbb{Q}$. Therefore $p\mathbb{Z}$ is contained in the ideal $I = (1 - z)O \cap \mathbb{Z}$.

If $I = \mathbb{Z}$, then $1 - z$ would be a unit of O and so would be its conjugates $1 - z^i$, which then implies that p as their product would be a unit of O. Then $p^{-1} \in O\cap\mathbb{Q} = \mathbb{Z}$, a contradiction. Thus,

$$I = (1 - z)O \cap \mathbb{Z} = p\mathbb{Z}.$$

Now we prove another auxiliary result:

$$\mathrm{Tr}((1 - z)O) \subset p\mathbb{Z}.$$

Indeed, every conjugate of $y(1-z)$ for $y \in O$ is of the type $y_i(1-z^i)$ with appropriate $y_i \in O$, so $\mathrm{Tr}(y(1 - z)) = \sum y_i(1 - z^i) \in I = p\mathbb{Z}$.

Now let $x = \sum_{0\leqslant i\leqslant p-2} a_iz^i \in O$ with $a_i \in \mathbb{Q}$. We aim to show that all a_i belong to $\mathbb{Z}$. From the calculation of the traces of z^i it follows that $\mathrm{Tr}((1-z)x) = a_0 \mathrm{Tr}(1-z)+ \sum_{0<i\leqslant p-2} a_i \mathrm{Tr}(z^i - z^{i+1}) = a_0p$ and so $a_0p \in \mathrm{Tr}((1 - z)O) \subset p\mathbb{Z}$; therefore, $a_0 \in \mathbb{Z}$. Since z is a unit of O, we deduce that $x_1 = z^{-1}(x-a_0) = a_1+a_2z+\cdots+a_{p-2}z^{p-3} \in O$. By the same arguments $a_1 \in \mathbb{Z}$. Looking at $x_i = z^{-1}(x_{i-1} - a_{i-1}) \in O$ we conclude $a_i \in \mathbb{Z}$ for all i. Thus $O = \mathbb{Z}[z]$.

2.4.3. The discriminant of $O/\mathbb{Z}$ is the ideal of $\mathbb{Z}$ generated by $D(1, z, \ldots, z^{p-2})$ which by 2.3.9 is equal $(-1)^{(p-1)(p-2)/2}N(f'(z))$. We have $f'(z) = pz^{p-1}/(z - 1) = pz^{-1}/(z - 1)$ and $N(f'(z)) = N(p)N(z)^{-1}/N(z - 1) = p^{p-1}(-1)^{p-1}/((-1)^{p-1}p) = p^{p-2}$. Thus, the discriminant of $O\mathbb{Z}$ is the principal ideal $(-1)^{(p-1)(p-2)/2}\, p^{p-2}\mathbb{Z} = p^{p-2}\mathbb{Z}$.

2.4.4. In general, the extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a Galois extension and elements of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ are determined by their action on the primitive mth root ζ_m of unity:

$$\sigma \mapsto i : \sigma(\zeta_m) = \zeta_m^i, \quad (i, m) = 1.$$

This map induces a group isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times.$$

One can prove that the ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}(\zeta_m)$.

3. Dedekind rings

3.1. Noetherian rings

3.1.1. Recall that a module M over a ring is called a Noetherian module if one of the following equivalent properties is satisfied:

(i) every submodule of M is of finite type;

(ii) every increasing sequence of submodules stabilizes;

(iii) every nonempty family of submodules contains a maximal element with respect to inclusion.

A ring A is called Noetherian if it is a Noetherian A-module.

Example. A PID is a Noetherian ring, since every ideal of it is generated by one element.

Lemma. *Let M be an A-module and N is a submodule of M. Then M is a Noetherian A-module iff N and M/N are.*

Corollary 1. *If N_i are Noetherian A-modules, so is $\oplus_{i=1}^n N_i$.*

Corollary 2. *Let A be a Noetherian ring and let M be an A-module of finite type. Then M is a Noetherian A-module.*

3.1.2. Proposition. *Let A be a Noetherian integrally closed ring. Let K be its field of fractions and let L be a finite extension of K. Let A' be the integral closure of A in L. Suppose that K is of characteristic 0. Then A' is a Noetherian ring.*

Proof. According to 2.3.6 A' is a submodule of a free A-module of finite rank. Hence A' is a Noetherian A-module. Every ideal of A' is in particular an A-submodule of A'. Hence every increasing sequence ideals of A' stabilizes and A' is a Noetherian ring.

3.1.3. Example. The ring of integers O_F of a number field F is a Noetherian ring. It is a $\mathbb{Z}$-module of rank n where n is the degree of F.

Every nonzero element of $O_F \setminus \{0\}$ factorizes into a product of prime elements and units (not uniquely in general).

Indeed, assume the family of principal ideals (a) which are generated by elements O_F which are not products of prime elements is nonempty and then choose a maximal element (a) in this family. The element a is not a unit, and A isn't prime. Hence there is a factorization $a = bc$ with both $b, c \notin O_F^*$. Then $(b), (c)$ are strictly larger than (a), so b and c are products of prime elements. Then a is, a contradiction.

3.2. Dedekind rings

3.2.1. Definition. An integral domain A is called a *Dedekind ring* if
(i) A is a Noetherian ring;
(ii) A is integrally closed;
(iii) every non-zero (proper) prime ideal of A is maximal.

Example. *Every principal ideal domain A is a Dedekind ring.*

Proof: for (i) see 3.1.1 and for (ii) see 2.1.4. If (a) is a prime ideal and $(a) \subset (b) \neq A$, then b isn't a unit of A and b divides a. Write $a = bc$. Since (a) is prime, either b or c belongs to (a). Since b doesn't, c must belong to (a), so $c = ad$ for some $d \in A$. Therefore $a = bc = bda$ which means that b is a unit of A, a contradiction. Thus, property (iii) is satisfied as well.

3.2.2. Lemma. *Let A be an integral domain. Let K be its field of fractions and let L be a finite extension of K. Let B be the integral closure of A in L. Let P be a non-zero prime ideal of B. Then $P \cap A$ is a non-zero prime ideal of A.*

Proof. Let P be a non-zero prime ideal of B. Then $P \cap A \neq A$, since otherwise $1 \in P \cap A$ and hence $P = B$.

If $c, d \in A$ and $cd \in P \cap A$, then either $c \in P \cap A$ or $d \in P \cap A$. Hence $P \cap A$ is a prime ideal of A.

Let $b \in P$, $b \neq 0$. Then b satisfies a polynomial relation $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. We can assume that $a_0 \neq 0$. Then $a_0 = -(b^n + \cdots + a_1 b) \in A \cap P$, so $P \cap A$ is a non-zero prime ideal of A.

3.2.3. Theorem. *Let A be a Dedekind ring. Let K be its field of fractions and let L be a finite extension of K. Let B be the integral closure of A in L. Suppose that K is of characteristic 0. Then B is a Dedekind ring.*

Proof. B is Noetherian by 3.1.2. It is integrally closed due to 2.1.6. By 3.2.2 if P is a non-zero proper prime ideal of B, then $P \cap A$ is a non-zero prime ideal of A. Since A is a Dedeking ring, it is a maximal ideal of A. The quotient ring B/P is integral over the field $A/(P \cap A)$. Hence by 2.1.7 B/P is a field and P is a maximal ideal of B.

3.2.4. Example. The ring of integers O_F of a number field F is a Dedekind ring.

3.3. Factorization in Dedekind rings

3.3.1. Lemma. *Every non-zero ideal in a Dedekind ring A contains some product of maximal ideals.*

Proof. If not, then the set of non-zero ideals which do not contain products of maximal ideals is non-empty. Let I be a maximal element with this property. The ideal I isn't maximal, since it doesn't contain a product of maximal ideals. Therefore there are $a, b \in A$ such that $ab \in I$ and $a, b \notin I$. Since $I + aA$ and $I + bA$ are strictly greater than I, there are maximal ideals P_i and Q_j such that $\prod P_i \subset I + aA$ and $\prod Q_j \subset I + bA$. Then $\prod P_i \prod Q_j \subset (I + aA)(I + bA) \subset I$, a contradiction.

3.3.2. Lemma. *Let a prime ideal P of A contain $I_1 \dots I_m$, where I_j are ideals of A. Then P contains one of I_j.*

Proof. If $I_k \not\subset P$ for all $1 \leqslant k \leqslant m$, then take $a_k \in I_k \setminus P$ and consider the product $a_1 \dots a_m$. It belongs to P, therefore one of a_i belongs to P, a contradiction.

3.3.3. The next proposition shows that for every non-zero ideal I of a Dedekind ring A there is an ideal J such that IJ is a principal non-zero ideal of A. Moreover, the proposition gives an explicit description of J.

Proposition. *Let I be a non-zero ideal of a Dedekind ring A and b be a non-zero element of I. Let K be the field of fractions of A. Define*

$$J = \{a \in K : aI \subset bA\}.$$

Then J is an ideal of A and $IJ = bA$.

Proof. Since $b \in I$, we get $bA \subset I$.

If $a \in J$ then $aI \subset bA \subset I$, so $aI \subset I$. Now we use the Noetherian and integrality property of Dedekind rings: Since I is an A-module of finite type, by Remark in 2.1.1 a is integral over A. Since A is integrally closed, $a \in A$. Thus, $J \subset A$.

The set J is closed with respect to addition and multiplication by elements of A, so J is an ideal of A. It is clear that $IJ \subset bA$. Assume that $IJ \neq bA$ and get a contradiction.

The ideal $b^{-1}IJ$ is a proper ideal of A, and hence it is contained in a maximal ideal P. Note that $b \in J$, since $bI \subset bA$. So $b^2 \in IJ$ and $b \in b^{-1}IJ$, $bA \subset b^{-1}IJ$. By 3.3.1 there are non-zero prime ideals P_i such that $P_1 \dots P_m \subset bA$. Let m be the minimal number with this property.

We have

$$P_1 \dots P_m \subset bA \subset b^{-1}IJ \subset P.$$

By 3.3.2 P contains one of P_i. Without loss of generality we can assume that $P_1 \subset P$. Since P_1 is maximal, $P_1 = P$.

If $m = 1$, then $P \subset bA \subset b^{-1}IJ \subset P$, so $P = bA$. Since $bA \subset I$ we get $P \subset I$. Since P is maximal, either $I = P$ or $I = A$. The definition of J implies in the first case $J = \{a \in K : aI = aP \subset bA = P\} = A$ and $IJ = bA$ and in the second case $b \in J$ implies $bA \subset J = \{a \in K : aA \subset bA\} \subset \{a \in K : a \in bA\} = bA$ and so $J = bA$ and $IJ = bA$.

Let $m > 1$. Note that $P_2 \dots P_m \not\subset bA$ due to the definition of m. Therefore, there is $d \in P_2 \dots P_m$ such that $d \notin bA$. Since $b^{-1}IJ \subset P$, $db^{-1}IJ \subset dP \subset PP_2 \dots P_m \subset bA$. So $(db^{-1}J)I \subset bA$, and the defining property of J implies that $db^{-1}J \subset J$. Since J is an A-module of finite type, by 2.1.1 db^{-1} belongs to A, i.e. $d \in bA$, a contradiction.

3.3.4. Corollary 1 (Cancellation property). *Let I, J, H be non-zero ideals of A, then $IH = JH$ implies $I = J$.*

Proof. Let H' be an ideal such that $HH' = aA$ is a principal ideal. Then $aI = aJ$ and $I = J$.

3.3.5. Corollary 2 (Factorization property). *Let I and J be ideals of A. Then $I \subset J$ if and only if $I = JH$ for an ideal H.*

Proof. If $I \subset J$ and J is non-zero, then let J' be an ideal of A such that $JJ' = aA$ is a principal ideal. Then $IJ' \subset aA$, so $H = a^{-1}IJ'$ is an ideal of A. Now

$$JH = Ja^{-1}IJ' = a^{-1}IJJ' = a^{-1}aI = I.$$

3.3.6. Theorem. *Every proper ideal of a Dedekind ring factorizes into a product of maximal ideals whose collection is uniquely determined.*

Proof. Let I be a non-zero ideal of A. There is a maximal ideal P_1 which contains I. Then by the factorization property 3.3.5 $I = P_1Q_1$ for some ideal Q_1. Note that $I \subset Q_1$ is a proper inclusion, since otherwise $AQ_1 = Q_1 = I = P_1Q_1$ and by the cancellation property 3.3.4 $P_1 = A$, a contradiction. If $Q_1 \neq A$, then there is a maximal ideal P_2 such that $Q_1 = P_2Q_2$. Continue the same argument: eventually we have $I = P_1 \dots P_nQ_n$ and $I \subset Q_1 \subset \dots \subset Q_n$ are all proper inclusions. Since A is Noetherian, $Q_m = A$ for some m and then $I = P_1 \dots P_m$.

If $P_1 \dots P_m = Q_1 \dots Q_n$, then $P_1 \supset Q_1 \dots Q_n$ and by 3.3.2 P_1 being a prime ideal contains one of Q_i, so $P_1 = Q_i$. Using 3.3.4 cancel P_1 on both sides and use induction.

3.3.7. Remark. A maximal ideal P of A is involved in the factorization of I iff $I \subset P$.

Indeed, if $I \subset P$, then $I = PQ$ by 3.3.5.

3.3.8. Example. Let $A = \mathbb{Z}[\sqrt{-5}]$. This is a Dedekind ring, since $-5 \not\equiv 1 \mod 4$, and A is the ring of integers of $\mathbb{Q}(\sqrt{-5})$.

We have the norm map $N(a + b\sqrt{-5}) = a^2 + 5b^2$. If an element u is a unit of A then $uv = 1$ for some $v \in A$, and the product of two integers $N(u)$ and $N(v)$ is 1, thus $N(u) = 1$. Conversely, if $N(u) = 1$ then u times its conjugate u' is one, and so u is a unit of A. Thus, $u \in A^\times$ iff $N(u) \in \mathbb{Z}^\times$.

The norms of $2, 3, 1 \pm \sqrt{-5}$ are $4, 9, 6$. It is easy to see that $2, 3$ are not in the image $N(A)$.

If, say, 2 were not a prime element in A, then $2 = \pi_1\pi_2$ and $4 = N(\pi_1)N(\pi_2)$ with both norms being proper divisors of 4, a contradiction. Hence 2 is a prime element of A, and similarly $3, 1 \pm \sqrt{-5}$ are.

Now $2, 3, 1 \pm \sqrt{-5}$ are prime elements of A and

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Note that $2, 3, 1 \pm \sqrt{-5}$ are not associated with each other (the quotient is not a unit) since their norms differ not by a unit of $\mathbb{Z}$. Thus A isn't a UFD.

The ideals

$$(2, 1 + \sqrt{-5}), (3, 1 + \sqrt{-5}), (3, 1 - \sqrt{-5})$$

are maximal.

For instance, $|A/(2)| = 4$, and it is easy to show that $A \neq (2, 1 + \sqrt{-5}) \neq (2)$, so $|A/(2, 1 + \sqrt{-5})| = 2$, therefore $A/(2, 1 + \sqrt{-5})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, i.e. is a field.

We get factorization of ideals

$$\begin{aligned}
(2) &= (2, 1 + \sqrt{-5})^2,\\
(3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}),\\
(1 + \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}),\\
(1 - \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).
\end{aligned}$$

To prove the first equality note that $(1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5} \in (2)$, so the RHS $\subset$ LHS; we also have $2 = 2(1 + \sqrt{-5}) - 2^2 - (1 + \sqrt{-5})^2 \in$ RHS, so LHS = RHS.

For the second equality use $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 \in (3)$, $3 = 3^2 - (1+\sqrt{-5})(1-\sqrt{-5}) \in$ RHS.

For the third equality use $6 \in (1+\sqrt{-5})$, $1+\sqrt{-5} = 3(1+\sqrt{-5}) - 2(1+\sqrt{-5}) \in$ RHS.

For the fourth equality use conjugate the third equality and use $(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$.

Thus

$$\begin{aligned}
(2) \cdot (3) &= (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})\\
&= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})\\
&= (1 + \sqrt{-5})(1 - \sqrt{-5}).
\end{aligned}$$

3.3.9. Lemma. *Let $I + J = A$. Then $I^n + J^m = A$ for every $n, m \geqslant 1$.*

Proof. We have $A = (I + J)\dots(I + J) = I(...) + J^m \subset I + J^m$, so $I + J^m = A$. Similarly $I^n + J^m = A$.

Proposition. *Let P be a maximal ideal of A. Then there is an element $\pi \in P$ such that*

$$P = \pi A + P^n$$

for every $n \geqslant 2$.

Hence the ideal P/P^n is a principal ideal of the factor ring A/P^n. Moreover, it is the only maximal ideal of that ring.

Every ideal of the ring A/P^n is principal of the form $P^m/P^n = (\pi^m A + P^n)/P^n$ for some $m \leqslant n$.

Proof. If $P = P^2$, then $P = A$ by cancellation property, a contradiction. Let $\pi \in P \setminus P^2$. Since $\pi A + P^n \subset P$, factorization property implies that $\pi A + P^n = PQ$ for an ideal Q.

Note that $Q \not\subset P$, since otherwise $\pi \in P^2$, a contradiction.

Therefore, $P + Q = A$. The Lemma implies $P^{n-1} + Q = A$. Then

$$P = P(Q + P^{n-1}) \subset PQ + P^n = \pi A + P^n \subset P,$$

so $P = \pi A + P^n$.

For $m \leqslant n$ we deduce $P^m \subset \pi^m A + P^n \subset P^m$, so $P^m = \pi^m A + P^n$.

Let I be a proper ideal of A containing P^n. Then by factorization property $P^n = IK$ with some ideal K. Hence the factorization of I involves powers of P only, so $I = P^m$, $0 < m \leqslant n$. Hence ideals of A/P^n are P^m/P^n with $m \leqslant n$.

3.3.10. Corollary. *Every ideal in a Dedekind ring is generated by 2 elements.*

Proof. Let I be a non-zero ideal, and let a be a non-zero element of I. Then $aA = P_1^{n_1} \dots P_m^{n_m}$ with distinct maximal ideals P_i.

By Lemma 3.3.9 we have $P_1^{n_1} + P_k^{n_k} = A$ if $l \neq k$, so we can apply the Chinese remainder theorem which gives

$$A/aA \simeq A/P_1^{n_1} \times \dots \times A/P_m^{n_m}.$$

For the ideal I/aA of A/aA we get

$$I/aA \simeq (I + P_1^{n_1})/P_1^{n_1} \times \dots \times (I + P_m^{n_m})/P_m^{n_m}.$$

Each of ideals $(I + P_i^{n_i})/P_i^{n_i}$ is of the form $(\pi_i^{l_i} A + P_i^{n_i})/P_i^{n_i}$ by 3.3.9. Hence I/aA is isomorphic to $\prod(\pi_i^{l_i} A + P_i^{n_i})/P_i^{n_i}$. Using the Chinese remainder theorem find $b \in A$ such that $b - \pi_i^{l_i}$ belongs to $P_i^{n_i}$ for all i. Then $I/aA = (aA + bA)/aA$ and $I = aA + bA$.

3.3.11. Theorem. *A Dedekind ring A is a UFD if and only if A is a PID.*

Proof. Let A be not a PID. Since every proper ideal is a product of maximal ideals, there is a maximal ideal P which isn't principal. Consider the family $\mathcal{F}$ of non-zero ideals I such that PI is principal. It is nonempty by 3.3.5. Let I be a maximal element of this family and $PI = aA$, $a \neq 0$.

Note that I isn't principal, because otherwise $I = xA$ and $PI = xP = aA$, so a is divisible by x. Put $y = ax^{-1}$, then $(x)P = (x)(y)$ and by 3.3.4 $P = (y)$, a contradiction.

Claim: a is a prime element of A. First, a is not a unit of A: otherwise $P \supset PI = aA = A$, a contradiction. Now, if $a = bc$, then $bc \in P$, so either $b \in P$ or $c \in P$. By 3.3.5 then either $bA = PJ$ or $cA = PJ$ for an appropriate ideal J of A. Since $PI \subset PJ$, we get $aI = IPI \subset IPJ = aJ$ and $I \subset J$. Note that $J \in \mathcal{F}$. Due to maximality of I we deduce that $I = J$, and hence either bA or cA is equal to aA. Then one of b, c is asociated to a, so a is a prime element.

$P \not\subset aA$, since otherwise $aA = PI \subset aI$, so $A = I$, a contradiction.

$I \not\subset aA$, since otherwise $aA \subset I$ implies $aA = I$, I is principal, a contradiction.

Thus, there are $d \in P$ and $e \in I$ not divisible by a. We also have $ed \in PI = aA$ is divisible by the prime element a. This can never happen in UFD. Thus, A isn't a UFD.

Using this theorem, to establish that the ring $\mathbb{Z}[\sqrt{-5}]$ of 3.3.8 is not a unique factorization domain it is sufficient to indicate a non-principal ideal of it.

3.4. The norm of an ideal

In this subsection F is a number field of degree n, O_F is the ring of integers of F.

3.4.1. Proposition. *For a non-zero element $a \in O_F$*

$$|O_F : aO_F| = |N_{F/\mathbb{Q}}(a)|.$$

Proof. We know that O_F is a free $\mathbb{Z}$-module of rank n. The ideal aO_F is a free submodule of O_F of rank n, since if $x_1, \dots, x_m$ are generators of aO_F, then $a^{-1}x_1, \dots, a^{-1}x_m$ are generators of O_F, so $m = n$. By the theorem on the structure of modules over principal ideal domains, there is a basis $a_1, \dots, a_n$ of O_F such that $e_1a_1, \dots, e_na_n$ is a basis of aO_F with appropriate $e_1|\dots|e_n$. Then O_F/aO_F is isomorphic to $\prod \mathbb{Z}/e_i\mathbb{Z}$, so $|O_F : aO_F| = \prod |e_i|$. By the definition $N_{F/\mathbb{Q}}(a)$ is equal to the determinant of the matrix of the linear operator $f : O_F \to O_F$, $b \to ab$. Note that aO_F has another basis: $aa_1, \dots, aa_n$, so $(aa_1, \dots, aa_n) = (e_1a_1, \dots, e_na_n)M$

with an invertible matrix M with integer entries. Thus, the determinant of M is ± 1 and $N_{F/\mathbb{Q}}(a)$ is equal to $\pm \prod e_i$.

3.4.2. Corollary. *$|O_F : aO_F| = |a|^n$ for every non-zero $a \in \mathbb{Z}$.*

Proof. $N_{F/\mathbb{Q}}(a) = a^n$.

3.4.3. Definition. The norm $N(I)$ of a non-zero ideal I of O_F is its index $|O_F : I|$.

Note that if $I \neq 0$ then $N(I)$ is a finite number.

Indeed, by 3.4.1 $N(aO_F) = |N_{F/\mathbb{Q}}(a)|$ for a non-zero a which belongs to I. Then $aO_F \subset I$ and $N(I) \leqslant N(aO_F) = |N_{F/\mathbb{Q}}(a)|$.

3.4.4. Proposition. *If I, J are non-zero ideals of O_F, then $N(IJ) = N(I)N(J)$.*

Proof. Since every ideal factors into a product of maximal ideals by 3.3.6, it is sufficient to show that $N(IP) = N(I)N(P)$ for a maximal ideal P of O_F.

The LHS = $|O_F : IP| = |O_F : I||I : IP|$. Recall that P is a maximal ideal of O_F, so O_F/P is a field.

The quotient I/IP can be viewed as a vector space over O_F/P. Its subspaces correspond to ideals between IP and I according to the description of ideals of the factor ring. If $IP \subset J \subset I$, then by 3.3.5 $J = IQ$ for an ideal Q of O_F.

By 3.3.3 there is a non-zero ideal I' such that II' is a principal non-zero ideal aO_F. Then $IP \subset IQ$ implies $aP \subset aQ$ implies $P \subset Q$. Therefore either $Q = P$ and then $J = IP$ or $Q = O_F$ and then $J = I$. Thus, the only subspaces of the vector space I/IP are itself and the zero subspace IP/IP. Hence I/IP is of dimension one over O_F/P and therefore $|I : IP| = |O_F : P|$.

3.4.5. Corollary. *If I is a non-zero ideal of O_F and $N(I)$ is prime, then I is a maximal ideal.*

Proof. If $I = JK$, then $N(J)N(K)$ is prime, so, say, $N(J) = 1$ and $J = O_F$. So I has no proper prime divisors, and therefore is a maximal ideal.

3.5. Splitting of prime ideals in field extensions

In this subsection F is a number field and L is a finite extension of F. Let O_F and O_L be their rings of integers.

3.5.1. Proposition-Definition. *Let P be a maximal ideal of O_F and Q a maximal ideal of O_L. Then Q is said to lie over P and P is said to lie under Q if one of the following equivalent conditions is satisfied:*
(i) $PO_L \subset Q$;
(ii) $P \subset Q$;
(iii) $Q \cap O_F = P$.

Proof. (i) is equivalent to (ii), since $1 \in O_L$. (ii) implies $Q \cap O_F$ contains P, so either $Q \cap O_F = P$ or $Q \cap O_F = O_F$, the latter is impossible since $1 \notin Q$. (iii) implies (ii).

3.5.2. Proposition. *Every maximal ideal of O_L lies over a unique maximal ideal P of O_F. For a maximal ideal P of O_F the ideal PO_L is a proper non-zero ideal of O_L. Let $PO_L = \prod Q_i$ be the factorization into a product of prime ideals of O_L. Then Q_i are exactly those maximal ideals of O_L which lie over P.*

Proof. The first assertion follows from 3.2.2.

Note that by 3.3.3 for $b \in P \setminus P^2$ there is an ideal J of O_F such that $PJ = bO_F$. Then $J \not\subset P$, since otherwise $b \in P^2$, a contradiction. Take an element $c \in J \setminus P$. Then $cP \subset bO_F$.

If $PO_L = O_L$, then $cO_L = cPO_L \subset bO_L$, so $cb^{-1} \in O_L \cap F = O_F$ and $c \in bO_F \subset P$, a contradiction. Thus, PO_L is a proper ideal of O_L.

According to 3.5.1 a prime ideal Q of O_L lies over P iff $PO_L \subset Q$ which is equivalent by 3.3.7 to the fact that Q is involved in the factorization of PO_L.

3.5.3. Lemma. *Let P be a maximal ideal of O_F which lie under a maximal ideal Q of O_L. Then the finite field O_F/P is a subfield of the finite field O_L/Q.*

Proof. O_L/Q is finite by 3.4.3. The kernel of the homomorphism $O_F \to O_L/Q$ is equal to $Q \cap O_F = P$, so O_F/P can be identified with a subfield of O_L/Q.

3.5.4. Corollary. *Let P be a maximal ideal of O_F. Then $P \cap \mathbb{Z} = p\mathbb{Z}$ for a prime number p and $N(P)$ is a positive power of p.*

Proof. $P \cap \mathbb{Z} = p\mathbb{Z}$ for a prime number p by 3.2.2. Then O_F/P is a vector space over $\mathbb{Z}/p\mathbb{Z}$ of finite positive dimension, therefore $|O_F : P|$ is a power of p.

3.5.5. Definition. Let a maximal ideal P of O_F lie under a maximal ideal Q of O_L. The degree of O_L/Q over O_F/P is called *the inertia degree* $f(Q|P)$. If $PO_L = \prod Q_i^{e_i}$ is the factorization of PO_L with distinct prime ideals Q_i of O_L, then e_i is called *the ramification index* $e(Q_i|P)$.

3.5.6. Lemma. *Let M be a finite extension of L and $P \subset Q \subset R$ be maximal ideals of O_F, O_L and O_M correspondingly. Then $f(R|P) = f(Q|P)f(R|Q)$ and $e(R|P) = e(Q|P)e(R|Q)$.*

Proof. The first assertion follows from 1.1.1. Since $PO_L = Q^{e(Q|P)}\dots$, we get $PO_M = Q^{e(Q|P)}O_M\cdots = (QO_M)^{e(Q|P)}\cdots = (R^{e(R|Q)})^{e(Q|P)}\dots$, so the second assertion follows.

3.5.7. Theorem. *Let $Q_1, \dots Q_m$ be different maximal ideals of O_L which lie over a maximal ideal P of O_F. Let $n = |L : F|$. Then*

$$\sum_{i=1}^{m} e(Q_i|P)f(Q_i|P) = n.$$

Proof. We consider only the case $F = \mathbb{Q}$. Apply the norm to the equality $pO_L = \prod Q_i^{e_i}$. Then by 3.4.2, 3.4.4

$$p^n = N(pO_L) = \prod N(Q_i)^{e_i} = \prod p^{f(Q_i|P)e(Q_i|P)}.$$

3.5.8. Example. One can describe in certain situations how a prime ideal (p) factorizes in finite extensions of $\mathbb{Q}$, provided the factorization of the monic irreducible polynomial of an integral generator (if it exists) modulo p is known.

Let the ring of integers O_F of an algebraic number field F be generated by one element α: $O_F = \mathbb{Z}[\alpha]$, and $f(X) \in \mathbb{Z}[X]$ be the monic irreducible polynomial of α over $\mathbb{Q}$.

Let $f_i(X) \in \mathbb{Z}[X]$ be monic polynomials such that

$$\overline{f}(X) = \prod_{i=1}^{m} \overline{f_i}(X)^{e_i} \in \mathbb{F}_p[X]$$

is the factorization of $\overline{f}(X)$ where $\overline{f_i}(X)$ is an irreducible polynomial over $\mathbb{F}_p$. Since $O_F \simeq \mathbb{Z}[X]/(f(X))$, we have

$$O_F/(p) \simeq \mathbb{Z}[X]/(p, f(X)) \simeq \mathbb{F}_p[X]/(\overline{f}(X)),$$

and

$$O_F/(p, f_i(\alpha)) \simeq \mathbb{Z}[X]/(p, f(X), f_i(X)) \simeq \mathbb{F}_p[X]/(\overline{f_i}(X)).$$

Putting $P_i = (p, f_i(\alpha))$ we see that O_F/P_i is isomorphic to the field $\mathbb{F}_p[X]/(\overline{f_i}(X))$, hence P_i is a maximal ideal of O_F dividing (p). We also deduce that

$$N(P_i) = p^{|\mathbb{F}_p[X]/(\overline{f_i}(X)):\mathbb{F}_p|} = p^{\deg \overline{f_i}}.$$

Now $\prod P_i^{e_i} = \prod (p, f_i(\alpha))^{e_i} \subset pO_F$, since $\prod f_i(\alpha)^{e_i} - f(\alpha) \in pO_F$. We also get $N(\prod P_i^{e_i}) = p^{\sum e_i \deg \overline{f_i}} = p^n = N(pO_F)$. Therefore from 3.5.7 we deduce that $(p) = \prod_{i=1}^{m} P_i^{e_i}$ is the factorization of (p).

So we have proved

Theorem. *Let the ring of integers O_F of an algebraic number field F be generated by one element α: $O_F = \mathbb{Z}[\alpha]$, and $f(X) \in \mathbb{Z}[X]$ be the monic irreducible polynomial of α over $\mathbb{Q}$. Let $f_i(X) \in \mathbb{Z}[X]$ be irreducible polynomials such that*

$$\overline{f}(X) = \prod_{i=1}^{m} \overline{f_i}(X)^{e_i} \in \mathbb{F}_p[X]$$

is the factorization of $\overline{f}(X)$ where $\overline{f_i}(X)$ is an irreducible polynomial over $\mathbb{F}_p$.

Then in O_F

$$(p) = \prod_{i=1}^{m} P_i^{e_i}$$

where $P_i = (p, f_i(\alpha))$ is a maximal ideal of O_F with norm $p^{\deg \overline{f_i}}$.

Definition–Example. Let $F = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ with a square free integer d.

Let p be a prime in $\mathbb{Z}$ and let $pO_L = \prod_{i=1}^{m} Q_i^{e_i}$. Then there are three cases:

(i) $m = 2$, $e_1 = e_2 = 1$, $f(Q_i|P) = 1$. Then $pO_L = Q_1Q_2$, $Q_1 \neq Q_2$. We say that p *splits in* L.

(ii) $m = 1$, $e_1 = 2$, $f(Q_1|P) = 1$. Then $pO_L = Q_1^2$. We say that p *ramifies in* L.

(iii) $m = 1$, $e_1 = 1$, $f(Q_1|P) = 2$. Then $pO_L = Q_1$. We say that p *remains prime in* L.

Using the previous theorem we see that p remains prime in O_F iff $\overline{f}$ is irreducible over $\mathbb{F}_p$; p splits ($pO_F = P_1 \dots P_m$) iff $\overline{f}$ is separable and reducible, and p ramifies ($pO_F = P^e$) iff $\overline{f}$ is a positive power of an irreducible polynomial over $\mathbb{F}_p$.

3.5.9. In particular, if $F = \mathbb{Q}(\sqrt{d})$ then one can take $\sqrt{d}$ for $d \not\equiv 1 \mod 4$ and $(1 + \sqrt{d})/2$ for $d \equiv 1 \mod 4$ as α. Then $f(X) = X^2 - d$ and $f(X) = X^2 - X + (1-d)/4$ resp.

We have $X^2 - X + (1-d)/4 = 1/4(Y^2 - d)$ where $Y = 2X - 1$, so if p is odd (so the image of 2 is invertible in $\mathbb{F}_p$), the factorization of $f(X)$ corresponds to the factorization of $X^2 - d$ independently of what d is. The factorization of $X^2 - d$ certainly depends on whether d is a quadratic residue modulo p, or not.

For $p = 2$ $\overline{f}(X) = (X - \overline{d})^2 \in \mathbb{F}_2[X]$ and $\overline{f}(X) = X^2 + X + \overline{(1-d)/4} \in \mathbb{F}_2[X]$ resp.

Thus, we get

Theorem. *If p is odd prime, then*

p splits in $L = \mathbb{Q}(\sqrt{d})$ iff d is a quadratic residue mod p.

p ramifies in L iff d is divisible by p.

p remains prime in L iff d is a quadratic non-residue mod p.

If $p = 2$ *then*
if $d \equiv 1 \mod 8$*, then 2 splits in* $\mathbb{Q}(\sqrt{d})$*,*
if $d \not\equiv 1 \mod 4$ *then 2 ramifies in* $\mathbb{Q}(\sqrt{d})$*;*
if $d \equiv 1 \mod 4, d \not\equiv 1 \mod 8$ *then 2 remains prime in* $\mathbb{Q}(\sqrt{d})$.

3.5.10. Let p be an odd prime. Recall from 2.4.2 that the ring of integers of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ is generated by ζ_p. Its irreducible monic polynomial is $f(X) = X^{p-1} + \dots + 1 = (X^p - 1)/(X - 1)$. Since $X^p - 1 \equiv (X - 1)^p \mod p$ we deduce that $(f(X), p) = ((X - 1)^{p-1}, p)$. Therefore by 3.5.8 $p = (\zeta_p - 1)^{p-1}$ ramifies in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. For any other prime l one can show that the polynomial $f(X)$ modulo l is the product of distinct irreducible polynomials over $\mathbb{F}_l$. Thus, no other prime ramifies in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

3.6. Finiteness of the ideal class group

In this subsection O_F is the ring of integers of a number field F.

3.6.1. Definition. For two non-zero ideals I and J of O_F define the equivalence relation $I \sim J$ if there are non-zero $a, b \in O_F$ such that $aI = bJ$. Classes of equivalence are called *ideal classes*. Define the product of two classes with representatives I and J as the class containing IJ. Then the class of O_F (consisting of all nonzero principal ideals) is the indentity element. By 3.3.3 for every non-zero I there is a non-zero J such that IJ is a principal ideal, i.e. every ideal class is invertible. Thus ideal classes form an abelian group which is called the *ideal class group* C_F of the number field F.

The ideal class group shows how far from PID the ring O_F is. Note that C_F consists of one element iff O_F is a PID iff O_F is a UFD.

3.6.2. Proposition. *There is a positive real number* c *such that every non-zero ideal* I *of* O_F *contains a non-zero element* a *with*

$$|N_{F/\mathbb{Q}}(a)| \leqslant cN(I).$$

Proof. Let $n = |F : \mathbb{Q}|$. According to 2.3.7 there is a basis $a_1, \dots, a_n$ of the $\mathbb{Z}$-module O_F which is also a basis of the $\mathbb{Q}$-vector space F. Let $\sigma_1, \dots, \sigma_n$ be all distinct $\mathbb{Q}$-homomorphisms of F into $\mathbb{C}$. Put

$$c = \prod_{i=1}^{n} \Big(\sum_{j=1}^{n} |\sigma_i a_j| \Big).$$

Then $c > 0$.

For a non-zero ideal I let m be the positive integer satisfying the inequality $m^n \leqslant N(I) < (m+1)^n$. In particular, $|O_F : I| < (m+1)^n$. Consider $(m+1)^n$ elements $\sum_{j=1}^n m_j a_j$ with $0 \leqslant m_j \leqslant m$, $m_j \in \mathbb{Z}$. There are two of them which have the same image in O_F/I. Their difference $0 \neq a = \sum_{j=1}^n n_j a_j$ belongs to I and satisfies $|n_j| \leqslant m$.

Now

$$|N_{F/\mathbb{Q}}(a)| = \prod_{i=1}^n |\sigma_i a| = \prod_{i=1}^n |\sum_{j=1}^n n_j \sigma_i a_j| \leqslant \prod_{i=1}^n \Bigl(\sum_{j=1}^n |n_j||\sigma_i a_j|\Bigr) \leqslant m^n c \leqslant cN(I).$$

3.6.3. Corollary. *Every ideal class of O_F contains an ideal J with $N(J) \leqslant c$.*

Proof. Given ideal class, consider an ideal I of the inverse ideal class. Let $a \in I$ be as in the theorem. By 3.3.3 there is an ideal J such that $IJ = aO_F$, so $(I)(J) = (aO_F) = 1$ in C_F. Then J belongs to the given ideal class. Using 3.4.1 and 3.4.4 we deduce that $N(I)N(J) = N(IJ) = N(aO_F) = |N_{F/\mathbb{Q}}(a)| \leqslant cN(I)$. Thus, $N(J) \leqslant c$.

3.6.4. Theorem. *The ideal class group C_F is finite. The number $|C_F|$ is called the class number of F.*

Proof. By 3.5.4 and 3.5.2 for each prime p there are finitely many maximal ideals P lying over (p), and $N(P) = p^m$ for $m \geqslant 1$. Hence there are finitely many ideals $\prod P_i^{e_i}$ satisfying $N(\prod P_i^{e_i}) \leqslant c$.

Example. The class number of $\mathbb{Q}(\sqrt{-19})$ is 1, i.e. every ideal of the ring of integers of $\mathbb{Q}(\sqrt{-19})$ is principal.

Indeed, by 2.3.8 we can take $a_1 = 1$, $a_2 = (1+\sqrt{-19})/2$ as an integral basis of the ring of integers of $\mathbb{Q}(\sqrt{-19})$. Then

$$c = \bigl(1 + |(1+\sqrt{-19})/2|\bigr)\bigl(1 + |(1-\sqrt{-19})/2|\bigr) = 10.4\ldots .$$

So every ideal class of $O_{\mathbb{Q}(\sqrt{-19})}$ contains an ideal J with $N(J) \leqslant 10$. Let $J = \prod P_i^{e_i}$ be the factorization of J, then $N(P_i) \leqslant 10$ for every i.

By Corollary 3.5.4 we know that $N(P_i)$ is a positive power of a prime integer, say p_i. From 3.5.2 we know that P_i is a prime divisor of the ideal (p_i) of $O_{\mathbb{Q}(\sqrt{-19})}$. So we need to look at prime integer numbers not greater than 7 and their prime ideal divisors as potential candidates for non-principal ideals. Now prime number 3 has the property that -19 is a quadratic non-residue modulo them, so by Theorem 3.5.9 it remains prime in $O_{\mathbb{Q}(\sqrt{-19})}$.

Odd prime numbers 5, 7 have the property that -19 is a quadratic residue module them, so by Theorem 3.5.9 they split in $O_{\mathbb{Q}(\sqrt{-19})}$. It is easy to check that

$$5 = \bigl((1+\sqrt{-19})/2\bigr)\bigl((1-\sqrt{-19})/2\bigr),$$
$$7 = \bigl((3+\sqrt{-19})/2\bigr)\bigl((3-\sqrt{-19})/2\bigr)..$$

Each of ideals generated by a factor on the right hand side is prime by 3.4.5, since its norm is a prime number. So prime ideal factors of $(5), (7)$ are principal ideals.

Finally, 2 remains prime in $O_{\mathbb{Q}(\sqrt{-19})}$, as follows from 3.5.9.

Thus, $O_{\mathbb{Q}(\sqrt{-19})}$ is a principal ideal domain.

Remark. The bound given by c is not good in practical applications. A more refined estimation is given by Minkowski's Theorem 3.6.6.

3.6.5. Definition. Let F be of degree n over $\mathbb{Q}$. Let $\sigma_1, \dots, \sigma_n$ be all $\mathbb{Q}$-homomorphisms of F into $\mathbb{C}$. Let

$$\tau: \mathbb{C} \to \mathbb{C}$$

be the complex conjugation. Then $\tau \circ \sigma_i$ is a $\mathbb{Q}$-homomorphism of F into $\mathbb{C}$, so it is equal to certain σ_j. Note that $\sigma_i = \tau \circ \sigma_i$ iff $\sigma_i(F) \subset \mathbb{R}$. Let r_1 be the number of $\mathbb{Q}$-homomorphisms of this type, say, after renumeration, $\sigma_1, \dots, \sigma_{r_1}$. For every $i > r_1$ we have $\tau \circ \sigma_j \neq \sigma_j$, so we can form couples $(\sigma_j, \tau \circ \sigma_j)$. Then $n - r_1$ is an even number $2r_2$, and $r_1 + 2r_2 = n$.

Renumerate the σ_j's so that $\sigma_{i+r_2} = \tau \circ \sigma_i$ for $r_1 + 1 \leqslant i \leqslant r_1 + r_2$. Define the *canonical embedding* of F by

$$\sigma: a \to (\sigma_1(a), \dots, \sigma_{r_1+r_2}(a)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \qquad a \in F.$$

The field F is isomorphic to its image $\sigma(F) \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The image $\sigma(F)$ is called the geometric image of F and it can be partially studied by geometric tools.

3.6.6. Minkowski's Bound Theorem. *Let F be an algebraic number field of degree n with parameters r_1, r_2. Then every class of C_F contains an ideal I such that its norm $N(I)$ satisfies the inequality*

$$N(I) \leqslant (4/\pi)^{r_2} n! \sqrt{|d_F|}/n^n$$

where d_F is the discriminant of F.

Proof. Use the geometric image of F and some geometric combinatorial considerations. In particular, one uses Minkowski's Lattice Point Theorem:

Let L be a free $\mathbb{Z}$-module of rank n in an n-dimensional Euclidean vector space V over $\mathbb{R}$ (then L is called a complete lattice in V). Denote by $\mathrm{Vol}\,(L)$ the volume of the set

$$\{a_1 e_1 + \dots + a_n e_n : 0 \leqslant a_i \leqslant 1\},$$

where $e_1, \dots, e_n$ is a basis of L. Notice that $\mathrm{Vol}\,(L)$ does not depend on the choice of basis.

Let X be a centrally symmetric convex subset of V. Suppose that $\mathrm{Vol}\,(X) > 2^n \mathrm{Vol}\,(L)$. Then X contains at least one nonzero point of L.

3.6.7. Examples. 1. Let $F = \mathbb{Q}(\sqrt{5})$. Then $r_1 = 2,\ r_2 = 0,\ n = 2,\ |d_F| = 5$.

$$(4/\pi)^{r_2} n! \sqrt{|d_F|}/n^n = 2!\sqrt{5}/2^2 = 1.1...,$$

so $N(I) = 1$ and therefore $I = O_F$. Thus, every ideal of O_F is principal and $C_F = \{1\}$.

2. Let $F = \mathbb{Q}(\sqrt{-5})$. Then $r_1 = 0,\ r_2 = 1,\ n = 2,\ |d_F| = 20,\ (2/\pi)\sqrt{|20|} < 3$. Hence, similar to Example in 3.6.4 we only need to look at prime numbers 2 (< 3) and prime ideal divisors of the ideal (2) as potential candidates for non-principal ideals.

From 3.3.8 we know that $(2) = (2, 1+\sqrt{-5})^2$ and $2 = N(2, 1+\sqrt{-5})$. So the ideal $(2, 1+\sqrt{-5})$ is maximal by 3.4.5.

The ideal $(2, 1+\sqrt{-5})$ is not principal: Indeed, if $(2, 1+\sqrt{-5}) = aO_L$ then $2 = N(2, 1+\sqrt{-5}) = N(aO_L) = |N_{L/\mathbb{Q}}(a)|$. If $a = c + d\sqrt{-5}$ with $c, d \in \mathbb{Z}$ we deduce that $c^2 + 5d^2 = \pm 2$, a contradiction.

We conclude that $C_{\mathbb{Q}(\sqrt{-5})}$ is a cyclic group of order 2.

3. Let $F = \mathbb{Q}(\sqrt{14})$. Then $r_1 = 2,\ r_2 = 0,\ n = 2,\ |d_F| = 56$ and $(1/2)\sqrt{56} = 3.7... < 4$. So we only need to inspect prime ideal divisors of (2) and of (3).

Now $2 = (4+\sqrt{14})(4-\sqrt{14})$, so $(2) = (4+\sqrt{14})(4-\sqrt{14})$. Since $N(4\pm\sqrt{14}) = 2$, 3.4.5 implies that the principal ideals $(4+\sqrt{14}),\ (4-\sqrt{14})$ are prime.

14 is quadratic non-residue modulo 3, so by Theorem 3.5.9 we deduce that 3 remains prime in O_F. Thus, every ideal of the ring of integers of $\mathbb{Q}(\sqrt{14})$ is principal, $C_{\mathbb{Q}(\sqrt{14})} = \{1\}$.

4. It is known that for negative square-free d the only quadratic fields $\mathbb{Q}(\sqrt{d})$ with class number 1 are the following:

$$\mathbb{Q}(\sqrt{-1}),\quad \mathbb{Q}(\sqrt{-2}),\quad \mathbb{Q}(\sqrt{-3}),\quad \mathbb{Q}(\sqrt{-7}),\quad \mathbb{Q}(\sqrt{-11}),$$
$$\mathbb{Q}(\sqrt{-19}),\quad \mathbb{Q}(\sqrt{-43}),\quad \mathbb{Q}(\sqrt{-67}),\quad \mathbb{Q}(\sqrt{-163}).$$

For $d > 0$ there are many more quadratic fields with class number 1. Gauss conjectured that there are infinitely many such fields, but this is still unproved.

3.6.8. Now we can state one of the greatest achivements of Kummer.

Kummer's Theorem. *Let p be an odd prime. Let $F = \mathbb{Q}(\zeta_p)$ be the pth cyclotomic field.*

If p doesn't divide $|C_F|$,
or, equivalently, p does not divide numerators of (rational) Bernoulli numbers $B_2, B_4, \dots, B_{p-3}$ given by

$$\frac{t}{e^t - 1} = \sum_{i=0}^{\infty} \frac{B_i}{i!} t^i,$$

then the Fermat equation

$$X^p + Y^p = Z^p$$

does not have positive integer solutions.

Among primes < 100 only 37, 59 and 67 don't satisfy the condition that p does not divide $|C_F|$, so Kummer's theorem implies that for any other prime number smaller 100 the Fermat equation does not have positive integer solutions.

3.7. Units of rings of algebraic numbers

3.7.1. Definition. A subgroup Y of $\mathbb{R}^n$ is called *discrete* if for every bounded closed subset Z of $\mathbb{R}^n$ the intersection $Y \cap Z$ is finite.

Example: points of $\mathbb{R}^n$ with integer coordinates form a discrete subgroup.

3.7.2. Proposition. *Let Y be a discrete subgroup of $\mathbb{R}^n$. Then there are m linearly independent over $\mathbb{R}$ vectors $y_1, \dots y_m \in Y$ such that $y_1, \dots, y_m$ is a basis of the $\mathbb{Z}$-module Y.*

Proof. Let $x_1, \dots, x_m$ be a set of linearly independent elements in Y over $\mathbb{R}$ with the maximal m. Denote

$$L = \{x \in \mathbb{R}^n : x = \sum_{i=1}^{m} c_i x_i : 0 \leqslant c_i \leqslant 1\}.$$

The set L is bounded and closed, so $L \cap Y$ is finite. For $y \in Y$ write $y = \sum_{i=1}^m b_i x_i$ with $b_i \in \mathbb{R}$. Define

$$z = y - \sum [b_i] x_i = \sum (b_i - [b_i]) x_i \in L \cap Y.$$

Hence the group Y is generated by the finite set $L \cap Y$ and $\{x_i\}$, and Y is finitely generated as a $\mathbb{Z}$-module.

Since the torsion of Y is trivial, the main theorem on the structure of finitely generated modules over principal ideal domains implies the assertion of the proposition.

3.7.3. Dirichlet's Unit Theorem. *Let F be a number field of degree n, $r_1 + 2r_2 = n$. Let O_F be its ring of integers and U be the group of units of O_F. Then U is the direct product of a finite cyclic group T consisting of all roots of unity in F and a free abelian group U_1 of rank $r_1 + r_2 - 1$:*

$$U \simeq T \times U_1 \simeq T \times \mathbb{Z}^{r_1 + r_2 - 1}.$$

A basis of the free abelian group U_1 is called a fundamental system of units in O_F.

Proof. Consider the canonical embedding σ of F into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Define

$$f\colon O_F \setminus \{0\} \to \mathbb{R}^{r_1+r_2},$$
$$f(x) = \bigl(\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1}(x)|, \log(|\sigma_{r_1+1}(x)|^2), \dots, \log(|\sigma_{r_1+r_2}(x)|^2)\bigr).$$

The map f induces a homomorphism $g\colon U \to \mathbb{R}^{r_1+r_2}$.

We now show that $g(U)$ is a discrete group. Let $u \in g^{-1}(Z)$ and Z be a bounded set. Then there is c such that $|\sigma_i(u)| \leqslant c$ for all i. The coefficients of the characteristic polynomial $g_u(X) = \prod_{i=1}^n (X - \sigma_i(u))$ of u over F being functions of $\sigma_i(u)$ are integers bounded by $\max(c^n, nc^{n-1}, \dots)$, so the number of different characteristic polynomials of $g^{-1}(Z)$ is finite, and so is $g^{-1}(Z)$.

Every finite subgroup of the multiplicative group of a field is cyclic by 1.2.4. Hence the kernel of g, being the preimage of 0, is a cyclic finite group. On the other hand, every root of unity belongs to the kernel of g, since $mg(z) = g(z^m) = g(1) = 0$ implies $g(z) = 0$ for the vector $g(z)$. We conclude that the kernel of g consists of all roots of unity T in F.

Since for $u \in U$ the norm $N_{F/\mathbb{Q}}(u) = \prod \sigma_i(u)$, as the product of units, is a unit in $\mathbb{Z}$, it is equal to ± 1. Then $\prod |\sigma_i(u)| = 1$ and $\log|\sigma_1(u)| + \dots + \log|\sigma_{r_1}(u)| + \log(|\sigma_{r_1+1}(u)|^2) + \dots + \log(|\sigma_{r_1+r_2}(u)|^2) = 0$. We deduce that the image $g(U)$ is contained in the hyperplane $H \subset \mathbb{R}^{r_1+r_2}$ defined by the equation $y_1 + \dots + y_{r_1+r_2} = 0$. Since $g^{-1}(Z)$ is finite for every bounded set Z, the intersection $g(U) \cap Z$ is finite. Hence by 3.7.2 $g(U)$ has a $\mathbb{Z}$-basis $\{y_i\}$ consisting of $m \leqslant r_1 + r_2 - 1$ linearly independent vectors over $\mathbb{Z}$. Denote by U_1 the subgroup of U generated by z_i such that $g(z_i) = y_i$; it is a free abelian group, since there are no nontrivial relations among y_i. From the main theorem on group homomorphisms we deduce that $U/T \simeq g(U)$ and hence $U = TU_1$. Since U_1 has no nontrivial torsion, $T \cap U_1 = \{1\}$. Then U as a $\mathbb{Z}$-module is the direct product of the free abelian group U_1 of rank m and the cyclic group T of roots of unity.

It remains to show that $m = r_1 + r_2 - 1$, i.e. $g(U)$ contains $r_1 + r_2 - 1$ linearly independent vectors. Put $l = r_1 + r_2$. As an application of Minkowski's geometric method one can show that

for every integer k between 1 and l there is $c > 0$ such that for every non-zero $a \in O_F \setminus \{0\}$ with $g(a) = (\alpha_1, \dots, \alpha_l)$ there is a non-zero $b = h_k(a) \in O_F \setminus \{0\}$ such that

$$|N_{F/\mathbb{Q}}(b)| \leqslant c \quad \text{and } g(b) = (\beta_1, \dots, \beta_l) \text{ with } \beta_i < \alpha_i \text{ for } i \neq k\,.$$

(for the proof see Marcus, Number Fields, p.144–145)

Fix k. Start with $a_1 = a$ and construct the sequence $a_j = h_k(a_{j-1}) \in O_F$ for $j \geqslant 2$. Since $N(a_j O_F) = |N_{F/\mathbb{Q}}(a_j)| \leqslant c$, in the same way as in the proof of 3.6.4 we deduce that there are only finitely many distinct ideals $a_j O_F$. So $a_j O_F = a_q O_F$ for some $j < q \leqslant l$. Then $u_k = a_q a_j^{-1}$ is a unit and satisfies the property: the ith coordinate of $g(u_k) = f(a_q) - f(a_j) = (\alpha_1^{(k)}, \dots, \alpha_l^{(k)})$ is negative for $i \neq k$. Then $\alpha_k^{(k)}$ is positive, since $\sum_i \alpha_i^{(k)} = 0$.

This way we get l units $u_1, \dots, u_l$. We claim that there are $l-1$ linearly independent vectors among the images $g(u_i)$. To verify the claim it suffices to check that the first $l-1$ columns of the matrix $(\alpha_i^{(k)})$ are linearly independent.

If there were not, then there would be a non-zero vector $(t_1, \dots, t_{l-1})$ such that $\sum_{i=1}^{l-1} t_i\alpha_i^{(k)} = 0$ for all $1 \leqslant k \leqslant l$. Without loss of generality one can assume that there is i_0 between 1 and $l-1$ such that $t_{i_0} = 1$ and $t_i \leqslant 1$ for $i \neq i_0$, $1 \leqslant i \leqslant l-1$. Then $t_{i_0}\alpha_{i_0}^{(i_0)} = \alpha_{i_0}^{(i_0)}$ and for $i \neq i_0$ $t_i\alpha_i^{(i_0)} \geqslant \alpha_i^{(i_0)}$ since $t_i \leqslant 1$ and $\alpha_i^{(i_0)} < 0$. Now we would get

$$0 = \sum_{i=1}^{l-1} t_i\alpha_i^{(i_0)} \geqslant \sum_{k=1}^{l-1} \alpha_i^{(i_0)} > \sum_{i=1}^{l} \alpha_i^{(i_0)} = 0,$$

a contradiction.

Thus, $m = r_1 + r_2 - 1$.

3.7.4. Example. Let $F = \mathbb{Q}(\sqrt{d})$ with a square free non-zero integer d.

If $d > 0$, then the group of roots of 1 in F is $\{\pm 1\}$, since $F \subset \mathbb{R}$ and there are only two roots of unity in $\mathbb{R}$.

Let O_F be the ring of integers of F. We have $n = 2$ and $r_1 = 2, r_2 = 0$ if $d > 0$; $r_1 = 0, r_2 = 1$ if $d < 0$. If $d < 0$, then

$$U(O_F) = T$$

is a finite cyclic group consisting of all roots of unity in F. It has order 4 for $d = -1$, 6 for $d = -3$, and one can show it has order 2 for all other negative square free integers.

If $d > 0$, $U(O_F)$ is the direct product of $\langle \pm 1 \rangle$ and the infinite group generated by a unit u (fundamental unit of O_F):

$$U(O_F) \simeq \langle \pm 1 \rangle \times \langle u \rangle = \{\pm u^k : k \in \mathbb{Z}\}.$$

Here is an algorithm how to find a fundamental unit if $d \not\equiv 1 \mod 4$ (there is a similar algorithm for an arbitrary square free positive d):

Let b be the minimal positive integer such that either $db^2 - 1$ or $db^2 + 1$ is a square of a positive integer, say, a. Then $N_{F/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$, so $a + b\sqrt{d} > 1$ is a unit of O_F.

Let $u_0 = e + f\sqrt{d}$ be a fundamental unit. Changing the sign of e, f if necessary, we can assume that e, f are positive. Due to the definition of u_0 there is an integer k such that $a + b\sqrt{d} = \pm u_0^k$. The sign is $+$, since the left hand side is positive; $k > 0$, since $u_0 \geqslant 1$ and the left hand side is > 1. From $a + b\sqrt{d} = (e + f\sqrt{d})^k$ we deduce that if $k > 1$ then $b = f +$ some positive integer $> f$, a contradiction. Thus, $k = 1$ and $a + b\sqrt{d} > 1$ is a fundamental unit of O_F.

For example, $1+\sqrt{2}$ is a fundamental unit of $\mathbb{Q}(\sqrt{2})$ and $2+\sqrt{3}$ is a fundamental unit of $\mathbb{Q}(\sqrt{3})$.

3.7.5. Now suppose that $d > 0$, and for simplicity, $d \not\equiv 1 \mod 4$. We already know that if an element $u = a + b\sqrt{d}$ of O_F is a unit, then its norm $N_{F/\mathbb{Q}}(u) = a^2 - db^2$ is ± 1. On the other hand, if $a^2 - db^2 = \pm 1$, then $\pm u^{-1} = a - b\sqrt{d}$ is in O_F, so u is a unit. Thus, $u = a + b\sqrt{d}$ is a unit iff $a^2 - db^2 = \pm 1$.

Let $u_0 = e + f\sqrt{d}$ be a fundamental unit.

From the previous we deduce that all integer solutions (a, b) of the equation

$$X^2 - dY^2 = \pm 1$$

satisfy $a + b\sqrt{d} = \pm(e + f\sqrt{d})^m$ for some integer m, which gives formulas for a and b as functions of e, f, m.

4. p-adic numbers

4.1.1. p-adic valuation and p-adic norm. Fix a prime p.

For a non-zero integer m let

$$k = v_p(m)$$

be the maximal integer such that p^k divides m, i.e. k is the power of p in the factorization of m. Then $v_p(m_1 m_2) = v_p(m_1) + v_p(m_2)$.

Extend v_p to rational numbers putting $v_p(0) := \infty$ and

$$v_p(m/n) = v_p(m) - v_p(n),$$

this does not depend on the choice of a fractional representation: if $m/n = m'/n'$ then $mn' = m'n$, hence $v_p(m) + v_p(n') = v_p(m') + v_p(n)$ and $v_p(m) - v_p(n) = v_p(m') - v_p(n')$.

Thus we get the p-adic valuation $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$. For non-zero rational numbers $a = m/n, b = m'/n'$ we get

$$\begin{aligned} v_p(ab) &= v_p(mm'/(nn')) = v_p(mm') - v_p(nn') \\ &= v_p(m) + v_p(m') - v_p(n) - v_p(n') \\ &= v_p(m) - v_p(n) + v_p(m') - v_p(n') \\ &= v_p(m/n) + v_p(m'/n') \\ &= v_p(a) + v_p(b). \end{aligned}$$

Thus v_p is a homomorphism from $\mathbb{Q}^\times$ to $\mathbb{Z}$.

4.1.2. p-adic norm. Define the *p-adic norm* of a rational number α by

$$|\alpha|_p = p^{-v_p(\alpha)}, \quad |0|_p = 0.$$

Then

$$|\alpha\beta|_p = |\alpha|_p |\beta|_p.$$

If $\alpha = m/n$ with integer m, n relatively prime to p, then $v_p(m) = v_p(n) = 0$ and $|\alpha|_p = 1$. In particular, $|-1|_p = |1|_p = 1$ and so $|-\alpha|_p = |\alpha|_p$ for every rational α.

4.1.3. Ultrametric inequality. For two integers m, n let $k = \min(v_p(m), v_p(n))$, so both m and n are divisible by p^k. Hence $m + n$ is divisible by p^k, thus

$$v_p(m+n) \geqslant \min(v_p(m), v_p(m)).$$

For two nonzero rational numbers $\alpha = m/n,\ \beta = m'/n'$

$$\begin{aligned} v_p(\alpha+\beta) &= v_p(mn'+m'n) - v_p(nn') \\ &\geqslant \min(v_p(m)+v_p(n'), v_p(m')+v_p(n)) - v_p(n) - v_p(n') \\ &\geqslant \min(v_p(m)-v_p(n), v_p(m')-v_p(n')) \\ &= \min(v_p(\alpha), v_p(\beta)). \end{aligned}$$

Hence for all rational α, β we get

$$v_p(\alpha+\beta) \geqslant \min(v_p(\alpha), v_p(\beta)).$$

This implies

$$|\alpha+\beta|_p \leqslant \max(|\alpha|_p, |\beta|_p).$$

This inequality is called *an ultrametric inequality*.

In particular, since $\max(|\alpha|_p, |\beta|_p) \leqslant |\alpha|_p + |\beta|_p$, we obtain

$$|\alpha+\beta|_p \leqslant |\alpha|_p + |\beta|_p,$$

so $|\ |_p$ is a metric (p-adic metric) on the set of rational numbers $\mathbb{Q}$ and

$$d_p(\alpha, \beta) = |\alpha - \beta|_p$$

gives *the p-adic distance* between rational α, β.

4.1.4. All norms on $\mathbb{Q}$. In general, for a field F a norm $|\ |: F \to \mathbb{R}_{\geqslant 0}$ is a map which sends 0 to 0, which is a homomorphism from $F^\times$ to $\mathbb{R}_{>0}^\times$ and which satisfies the triangle inequality: $|\alpha+\beta| \leqslant |\alpha| + |\beta|$. In particular,

$$|1| = 1, 1 = |1| = |(-1)(-1)| = |-1|^2,$$

so $|-1| = 1$, and hence

$$|-a| = |-1||a| = |a|.$$

A norm is called nontivial if there is a nonzero $a \in F$ such that $|a| \neq 1$.

In addition to p-adic norms on $\mathbb{Q}$ we get the usual absolute value on $\mathbb{Q}$ which we will denote by $|\ |_\infty$.

A complete description of norms on $\mathbb{Q}$ is supplied by the following result.

Theorem (Ostrowski). *A nontrivial norm $|\ |$ on $\mathbb{Q}$ is either a power of the absolute value $|\ |_\infty^c$ with positive real c, or is a power of the p-adic norm $|\ |_p^c$ for some prime p with positive real c.*

Proof. For an integer $a > 1$ and an integer $b > 0$ write

$$b = b_n a^n + b_{n-1} a^{n-1} + \cdots + b_0$$

with $0 \leqslant b_i < a, a^n \leqslant b$. Then

$$|b| \leqslant (|b_n| + |b_{n-1}| + \cdots + |b_0|) \max(1, |a|^n)$$

and

$$|b| \leqslant (\log_a b + 1)\, d \max(1, |a|^{\log_a b}),$$

with $d = \max(|0|, |1|, \ldots, |a-1|)$.

Substituting b^s instead of b in the last inequality, we get

$$|b^s| \leqslant (s \log_a b + 1)\, d \max(1, |a|^{s \log_a b}),$$

hence

$$|b| \leqslant (s \log_a b + 1)^{1/s} d^{1/s} \max(1, |a|^{\log_a b}).$$

When $s \to +\infty$ we deduce

$$|b| \leqslant \max(1, |a|^{\log_a b}).$$

There are two cases to consider.

(1) Suppose there is an integer b such that $|b| > 1$. We can assume b is positive. Then

$$1 < |b| \leqslant \max(1, |a|^{\log_a b}),$$

and so $|a| > 1$, $|b| \leqslant |a|^{\log_a b}$ for every integer $a > 1$. Swapping a and b we get $|a| \leqslant |b|^{\log_b a}$, thus,

$$|a| = |b|^{\log_b a}$$

for every integer a and hence for every rational a.

Choose $c > 0$ such that $|b| = |b|_\infty^c$ then we obtain $|a| = |a|_\infty^c$ for every rational a.

(2) Suppose that $|a| \leqslant 1$ for all integer a. Since $|\ |$ is nontrivial, let a_0 be the minimal positive integer such that $|a_0| < 1$. If $a_0 = a_1 a_2$ with positive integers a_1, a_2, then $|a_1|\,|a_2| < 1$ and either $a_1 = 1$ or $a_2 = 1$. This means that $a_0 = p$ is a prime. If $q \notin p\mathbb{Z}$, then $pp_1 + qq_1 = 1$ with some integers p_1, q_1 and hence $1 = |1| \leqslant |p|\,|p_1| + |q|\,|q_1| \leqslant |p| + |q|$. Writing q^s instead of q we get $|q|^s \geqslant 1 - |p| > 0$ and $|q| \geqslant (1 - |p|)^{1/s}$. The right hand side tends to 1 when s tends to infinity. So we obtain $|q| = 1$ for every q prime to p. Therefore, $|\alpha| = |p|^{v_p(\alpha)}$, and $|\ |$ is a power of the p-adic norm.

4.1.5. Lemma (reciprocity law for all $|\ |_p$). *For every nonzero rational α*

$$\prod_{i \text{ prime or } \infty} |\alpha|_i = 1.$$

Proof. Due to the multiplicative property of the norms and factorization of integers it is sufficient to consider the case of $\alpha = p$ a prime number, then $|p|_p = p^{-1}$, $|p|_\infty = p$ and $|p|_i = 1$ for all other i.

4.2. The field of p-adic numbers $\mathbb{Q}_p$

4.2.1. The definition. Similarly to the definition of real numbers as the completion of $\mathbb{Q}$ with respect to the absolute value $|\ |_\infty$ define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic norm $|\ |_p$. So $\mathbb{Q}_p$ consists of equivalences classes of all fundamental sequences (with respect to the p-adic norm) (a_n) of rational numbers a_n: two fundamental sequences (a_n), (b_n) are equivalent if and only if $|a_n - b_n|_p$ tends to 0.

The field $\mathbb{Q}_p$ is called the field of p-adic numbers and its elements are called p-adic numbers.

4.2.2. p-adic series presentation of p-adic numbers. As an analogue of the decimal presentation of real numbers every element α of $\mathbb{Q}_p$ has a series representation: it can be written as an infinite convergent (with respect to the p-adic norm) series

$$\sum_{i=n}^{\infty} a_i p^i$$

with coefficients $a_i \in \{0, 1, \dots, p-1\}$ and $a_n \neq 0$.

4.2.3. The p-adic norm and p-adic distance. We have an extension of the p-adic norm from $\mathbb{Q}$ to $\mathbb{Q}_p$ by continuity: if $\alpha \in \mathbb{Q}_p$ is the limit of a fundamental sequence (a_n) of rational numbers, then $|\alpha|_p := \lim |a_n|_p$. Since two fundamental sequences (a_n), (b_n) are equivalent if and only if $|a_n - b_n|_p$ tends to 0, the p-adic norm of α is well defined.

If we use the series representation $\alpha = \sum_{i=n}^{\infty} a_i p^i$ with coefficients $a_i \in \{0, 1, \dots, p-1\}$ and $a_n \neq 0$, then $|\alpha|_p = p^{-n}$.

The p-adic norm on $\mathbb{Q}_p$ satisfies the ultrametric inequality: let $\alpha = \lim a_n, \beta = \lim b_n$, (a_n), (b_n) are fundamental sequences of rational numbers, then $\alpha + \beta = \lim(a_n + b_n)$. Suppose that $|\alpha|_p \leqslant |\beta|_p$, then $|a_n|_p \leqslant |b_n|_p$ for all sufficiently large n, and so

$$|\alpha + \beta|_p = \lim |a_n + b_n|_p \leqslant \lim \max(|a_n|_p, |b_n|_p) = \lim |b_n|_p = |\beta|_p = \max(|\alpha|_p, |\beta|_p).$$

For α, β such that $|\alpha|_p < |\beta|_p$ we obtain $\beta = \gamma + \alpha$ where $\gamma = \beta - \alpha$. By the ultrametric inequality $|\beta|_p \leqslant \max(|\gamma|_p, |\alpha|_p)$, so $|\beta|_p \leqslant |\gamma|_p$ and by the ultrametric inequality $|\gamma|_p \leqslant \max(|\alpha|_p, |-\beta|_p) = \max(|\alpha|_p, |\beta|_p) = |\beta|_p$. Thus if $|\alpha|_p < |\beta|_p$ then $|\alpha - \beta|_p = |\beta|_p$.

Using the p-adic distance d_p we have shown that for every triangle with vertices in $0, \alpha, \beta$ if the p-adic length of its side connecting 0 and α is smaller than the p-adic length of its side connecting 0 and β then the p-adic length of the third side connecting α and β equals to the former. Thus, in every triangle two sides are of the same p-adic length!

4.2.4. The ring of p-adic integers $\mathbb{Z}_p$. Define the set $\mathbb{Z}_p$ of p-adic integers as those p-adic numbers whose p-adic norm does not exceed 1, i.e. whose p-adic series representation has $n_0 \geqslant 0$. For two elements $\alpha, \beta \in \mathbb{Z}_p$ we get $|\alpha\beta|_p \geqslant 0, |\alpha \pm \beta|_p \geqslant 0$. Hence $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

The units $\mathbb{Z}_p^\times$ of the ring $\mathbb{Z}_p$ are those p-adic numbers u whose p-adic norm is 1.

Every nonzero p-adic number α can be uniquely written as $p^{v_p(\alpha)}u$ with $u \in \mathbb{Z}_p^\times$. Thus

$$\mathbb{Q}_p^\times \simeq \langle p \rangle \times \mathbb{Z}_p^\times$$

where $\langle p \rangle$ is the infinite cyclic group generated by p.

Let I be a non-zero ideal of $\mathbb{Z}_p$. Let $n = \min\{v_p(\alpha) : \alpha \in I\}$. Then $p^n u$ belongs to I for some unit u, and hence p^n belongs to I, so $p^n\mathbb{Z}_p \subset I \subset p^n\mathbb{Z}_p$, i.e. $I = p^n\mathbb{Z}_p$. Thus $\mathbb{Z}_p$ is a principal ideal domain.

4.2.5. Note that $\mathbb{Z}_p$ is the closed ball of radius 1 in the p-adic norm.

Let α be its internal point, so $|\alpha|_p < 1$. Then for every β on the boundary of the open ball, i.e. $|\beta|_p = 1$ we obtain, applying the previous calculation $|\alpha - \beta|_p = |\beta|_p = 1$. Thus, the p-adic distance from α to every point on the boundary of the ball is 1, i.e. *every internal point of a p-adic ball is its centre!*

5. On class fi eld theory

To describe some very basic things about it, we first need to go through a very useful notion of the projective limit of algebraic objects.

5.1.1. Projective limits of groups/rings. Let A_n, $n \geqslant 1$ be a set of groups/rings, with group operation, in the case of groups, written additively. Suppose there are group/ring homomorphisms $\varphi_{nm}\colon A_n \to A_m$ for all $n \geqslant m$ such that

$\varphi_{nn} = \mathrm{id}_{A_n}$,

$\varphi_{nr} = \varphi_{mr} \circ \varphi_{nm}$ for all $n \geqslant m \geqslant r$.

The *projective limit* $\varprojlim A_n$ of (A_n, φ_{nm}) is the set

$$\{(a_n) : \quad a_n \in A_n, \quad \varphi_{nm}(a_n) = a_m \quad \text{for all } n \geqslant m\}$$

with the group/ring operation(s) $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n)(b_n) = (a_n b_n)$

For every m one has a group/ring homomorphism $\varphi_n\colon \varprojlim A_n \to A_m, (a_n) \mapsto a_m$.

5.1.2. Examples.

1. If $A_n = A$ for all n and $\varphi_{nm} = \mathrm{id}$ then $\varprojlim A_n = A$.

2. If $A_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\varphi_{nm}(a + p^n\mathbb{Z}) = a + p^m\mathbb{Z}$ then $(a_n) \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ means $p^{\min(n,m)} | (a_n - a_m)$ for all n, m.

The sequence (a_n) as above is a fundamental sequence with respect to the p-adic norm, and thus determines a p-adic number $a = \lim a_n \in \mathbb{Z}_p$. For its description, denote by r_m the integer between 0 and $p^m - 1$ such that $r_m \equiv a_m \mod p^m$. Then $r_m \equiv a_n \mod p^m$ for $n \geqslant m$ and $r_n \equiv r_m \mod p^m$ for $n \geqslant m$. Denote $c_0 = r_0$ and $c_m = (r_m / - r_{m-1})p^{-m+1}$, so $c_m \in \{0, 1, \dots, p-1\}$. Then $a = \sum_{m \geqslant 0} c_m p^m = \lim r_m \in \mathbb{Z}_p$.

We have a group and ring homomorphism

$$f \colon \varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p, \quad (a_n) \to a = \lim a_n \in \mathbb{Z}_p.$$

It is surjective: if $a = \sum_{m \geqslant 0} c_m p^m$ then define r_m by the inverse procedure to the above, then a is the image of $(r_n) \in \varprojlim \mathbb{Z}/p^n$; and its kernel is trivial, since $a = 0$ implies that for every k p^k divides a_n for all sufficiently large n, and so p^k divides a_k.

Thus,

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p.$$

This can be used as another (algebraic) definition of the ring of p-adic integers.

In particular, we a surjective homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ whose kernel equals to $p^n\mathbb{Z}_p$.

From the above we immediately deduce that if $A_n = (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\varphi_{nm}(a+p^n\mathbb{Z}) = a + p^m\mathbb{Z}$, $(a, p) = 1$, then similarly we have a homomorphism

$$f \colon \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \to \mathbb{Z}_p^\times, \quad (a_n) \to \lim r_m \in \mathbb{Z}_p^\times$$

(note that $(r_m, p) = 1$ and hence $\lim r_m \notin p\mathbb{Z}_p$). Thus, there is an isomorphism

$$\varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

3. One can extend the definition of the projective limit to the case when the maps φ_{nm} are defined for some specific pairs (n, m) and not necessarily all $n \geqslant m$.

Let $A_n = \mathbb{Z}/n\mathbb{Z}$ and let $\varphi_{nm} \colon A_n \to A_m$ be defined only if $m | n$ and then $\varphi_{nm}(a + n\mathbb{Z}) = a + m\mathbb{Z}$. Define, similarly to the above definition of the projective limit the projective limit $\varprojlim A_n$.

By the Chinese remainder theorem

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z}$$

where $n = p_1^{k_1} \dots p_r^{k_r}$ is the factorization of n. The maps φ_{nm} induce the maps already defined in 2 on $\mathbb{Z}/p^r\mathbb{Z}$, and we deduce

$$\varprojlim \mathbb{Z}/n\mathbb{Z} = \varprojlim \mathbb{Z}/2^r\mathbb{Z} \times \varprojlim \mathbb{Z}/3^r\mathbb{Z} \times \dots \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots = \prod \mathbb{Z}_p.$$

The group $\varprojlim \mathbb{Z}/n\mathbb{Z}$ is denoted $\widehat{\mathbb{Z}}$ and is called the procyclic group (topologically it is generated by its unity 1). This group is uncountable. We have a surjective homomorphism $\widehat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ whose kernel is $n\widehat{\mathbb{Z}}$.

Similarly we have

$$\widehat{\mathbb{Z}}^\times = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \varprojlim (\mathbb{Z}/2^r\mathbb{Z})^\times \times \varprojlim (\mathbb{Z}/3^r\mathbb{Z})^\times \times \cdots \simeq \prod \mathbb{Z}_p^\times.$$

5.2.1. Infinite Galois theory. As described in 1.3

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z},$$

where $q = p^n$ and the isomorphism is given by $\phi_n \mapsto 1 + m\mathbb{Z}$. The algebraic closure $\mathbb{F}_q^a$ of $\mathbb{F}_q$ is the compositum of all $\mathbb{F}_{q^m}$. From the point of view of infinite Galois theory and it is natural to define the infinite Galois group $\mathrm{Gal}(\mathbb{F}_q^a/\mathbb{F}_q)$ as the projective limit $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ with respect to the natural surjective homomorphisms $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, $r|m$. This corresponds to φ_{mr} defined in Example 4 above.

Hence we get

$$\mathrm{Gal}(\mathbb{F}_q^a/\mathbb{F}_q) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

Similarly, using 2.4.3 for the maximal cyclotomic extension $\mathbb{Q}^{\mathrm{cycl}}$, the composite of all finite cyclotomic extensions $\mathbb{Q}(\zeta_m)$ of $\mathbb{Q}$, we have

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{cycl}}/\mathbb{Q}) \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \simeq \widehat{\mathbb{Z}}^\times.$$

The main theorem of extended (to infinite extensions) Galois theory (one has to add a new notion of closed subgroup for an appropriate extension of the finite Galois theory), can be stated as follows:

Let L/F be a (possibly infinite) Galois extension, i.e. L is the compositum of splitting fields of separable polynomials over F. Denote $G = \mathrm{Gal}(L/F) = \varprojlim \mathrm{Gal}(E/F)$ where E/F runs through all finite Galois subextensions in L/F. Call a subgroup H of G closed if $H = \varprojlim \mathrm{Gal}(E/K)$ where K runs through a subfamily of finite subextensions in E/F, and the projective maps $\mathrm{Gal}(E''/K'') \to \mathrm{Gal}(E'/K')$ are induced by $\mathrm{Gal}(E''/F) \to \mathrm{Gal}(E'/F)$.

There is a one-to-one correspondence $(H \mapsto L^H)$ between closed subgroups H of G and fields M, $F \subset M \subset L$, the inverse map is given by $M \mapsto H = \varprojlim \mathrm{Gal}(E/K)$ where $K = E \cap M$. We have $\mathrm{Gal}(L/M) = H$.

Normal closed subgroups H of G correspond to Galois extensions M/F and $\mathrm{Gal}(M/F) \simeq G/H$.

5.3.1. We have already seen the importance of cyclotomic fields in Kummer's theorem 3.6.8.

Another very important property of cyclotomic fields is given by the following theorem

Theorem (Kronecker–Weber). *Every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$. Therefore the maximal abelian extension $\mathbb{Q}^{\text{ab}}$ of $\mathbb{Q}$ coincides with the cyclotomic field $\mathbb{Q}^{\text{cycl}}$ which is the compositum of all cyclotomic fields $\mathbb{Q}(\zeta_n)$.*

According to 2.4.3 the Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. So the infinite group $\text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q})$ is isomorphic to the limit of $(\mathbb{Z}/n\mathbb{Z})^\times$ which by 5.1.2 coincides with the group of units of $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

The isomorphism

$$\Upsilon\colon \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q})$$

can be described as follows: if $a \in \widehat{\mathbb{Z}}^\times$ is congruent to m modulo n via

$$\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z},$$

then $\Upsilon(a)(\zeta_n) = \zeta_n^m$.

Using 5.1.2 we have an isomorphism

$$\Psi\colon \prod \mathbb{Z}_p^\times \xrightarrow{\sim} \widehat{\mathbb{Z}}^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}).$$

On the left hand side we have an object $\widehat{\mathbb{Z}}^\times$ which is defined at the ground level of $\mathbb{Q}$, on the right hand side we have an object which incorporates information about all finite abelian extensions of $\mathbb{Q}$.

The restriction of the isomorphism to quadratic extensions of $\mathbb{Q}$ is related with the Gauss quadratic reciprocity law, see below.

Abelian class field theory generalizes the Kronecker–Weber theorem for an algebraic number field K to give a reciprocity homomorphism which relates an object (idele class group) defined at level of K and the Galois group of the maximal abelian extension of K over K.

5.3.2. Ideles. Recall (see 4.2.4) that $\mathbb{Q}_p^\times \simeq \langle p \rangle \times \mathbb{Z}_p^\times$, $\quad a \mapsto (n, u)$ where $n = v_p(a)$ and $u = ap^{-n}$,
v_p is the p-adic valuation.

Denote $\mathbb{Q}_\infty = \mathbb{R}$ and include ∞ in the set of "primes" of $\mathbb{Z}$. Form the so called *restricted product*

$$I_\mathbb{Q} = \prod{}' \mathbb{Q}_p^\times = \{(a_\infty, a_2, a_3, \dots) : a_p \in \mathbb{Q}_p^\times\}$$

of $\mathbb{R}^\times = \mathbb{Q}_\infty^\times$, $\mathbb{Q}_2^\times, \mathbb{Q}_3^\times, \dots$ such that almost all components a_p are p-adic units. Elements of $I_\mathbb{Q}$ are called *ideles over* $\mathbb{Q}$.

Define a homomorphism

$$f\colon I_{\mathbb{Q}} = \prod{}' \mathbb{Q}_p^\times \to \mathbb{Q}^\times \times \mathbb{R}_+^\times \times \prod \mathbb{Z}_p^\times,$$
$$(a_\infty, a_2, a_3, \dots) \mapsto (a, a_\infty a^{-1}, a_2 a^{-1}, a_3 a^{-1}, \dots)$$

where $a = \operatorname{sgn}(a_\infty) \prod p^{v_p(a_p)} \in \mathbb{Q}^\times$ and $\operatorname{sgn}(a)$ is the sign of a.

It is easy to verify that f is an isomorphism.

5.3.3. Define a homomorphism

$$\Phi_{\mathbb{Q}}\colon \prod{}' \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

by the following local-global formula:

$$\Phi_{\mathbb{Q}}(a_\infty, a_2, a_3, \dots) = \prod \Phi_{\mathbb{Q}_p}(a_p).$$

Here the *local reciprocity map* $\Phi_{\mathbb{Q}_p}$ is described as follows: if $a_p = p^n u$ where $n = v_p(a)$, then for a q^m th primitive root ζ of unity with prime q

$$\Phi_{\mathbb{Q}_p}(a_p)(\zeta) = \begin{cases} \zeta^{p^n}, & \text{if } p \neq q \\ \zeta^{u^{-1}}, & \text{if } p = q. \end{cases}$$

In particular, if $p \neq q$, then $\Phi_{\mathbb{Q}_p}(p)$ sends ζ to ζ^p, similar to the pth Frobenius automorphism defined in 1.3. So one can say that the reciprocity map sends prime p to the pth Frobenius automorphism.

For $p = \infty$ put

$$\Phi_{\mathbb{Q}_\infty}(a_\infty)(\zeta) = \zeta^{\operatorname{sgn}(a_\infty)}.$$

The homomorphism $\Phi_{\mathbb{Q}}$ is called the *reciprocity map*.

Theorem (class field theory over $\mathbb{Q}$).

1. Reciprocity Law: for a non-zero rational number a one has

$$\Phi_{\mathbb{Q}}(a, a, a, \dots) = 1.$$

2. For units $u_p \in \mathbb{Z}_p^\times$ one has

$$\Phi_{\mathbb{Q}}(1, u_2, u_3, \dots) = \Psi(u_2, u_3, \dots)^{-1}.$$

3. Using f define

$$g\colon I_{\mathbb{Q}} \to \mathbb{Q}^\times \times \mathbb{R}_+^\times \times \prod \mathbb{Z}_p^\times \to \prod \mathbb{Z}_p^\times,$$

$(a, b, u_2, u_3, \dots) \mapsto (u_2, u_3, \dots)$. *Then*

$$\Phi_{\mathbb{Q}}(\alpha)^{-1} = \Psi \circ g(\alpha).$$

4. The kernel of the reciprocity map $\Phi_{\mathbb{Q}}$ equals to $g^{-1}(1, 1, 1, \dots) =$ the product of the diagonal image of $\mathbb{Q}^\times$ in $I_{\mathbb{Q}}$ and of the image of $\mathbb{R}_+^\times$ in $I_{\mathbb{Q}}$ with respect to the *homomorphism* $\alpha \mapsto (\alpha, 1, 1, \dots)$. *It induces an isomorphism*

$$I_{\mathbb{Q}}/\mathbb{Q}^{\times}\mathbb{R}_{+}^{\times} \simeq \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

Proof. To verify the first property, due to the multiplicativity of $\Phi_{\mathbb{Q}}$ it is sufficient to show that for a primitive q^m th root ζ of unity

$$\Phi_{\mathbb{Q}}(p, p, \dots)(\zeta) = \zeta \quad \text{for all positive prime numbers } p$$
$$\Phi_{\mathbb{Q}}(-1, -1, \dots)(\zeta) = \zeta.$$

From the definition of $\Phi_{\mathbb{Q}}$ we deduce that

$$\Phi_{\mathbb{Q}_l}(p)(\zeta) = \begin{cases} \zeta, & \text{if } l \neq q, l \neq p \\ \zeta^p, & \text{if } l \neq q, l = p \\ \zeta^{p^{-1}}, & \text{if } l = q, l \neq p \\ \zeta, & \text{if } l = q = p. \end{cases}$$

So $(\prod_l \Phi_{\mathbb{Q}_l}(p))(\zeta) = \zeta$ for $q \neq p$ and for $q = p$. Similarly one checks the second assertion.

The second property is easy: due to multiplicativity it suffices to show that

$$\Psi(1, \dots, u_p, 1, \dots)^{-1} = \Phi_{\mathbb{Q}}(1, \dots, u_p, 1, \dots)$$

and this follows immediately from the definition of Ψ, $\Phi_{\mathbb{Q}}$.

The third property follows from the definition of f and the first and second properties. The fourth property follows from the third.

From this theorem one can deduce Gauss quadratic reciprocity law.

5.3.4. For an algebraic number field F one can define, in a similar way, the idele group I_F as a restricted product of the multiplicative groups $F_P^{\times}$ of completions F_P of F with respect to non-zero prime ideals P of the ring of integers of F, and of real or complex completions of F with respect to real and complex imbeddings of F into $\mathbb{C}$.

Except the case of $\mathbb{Q}$ and imaginary quadratic fields one does not have an explicit description of the maximal abelian extension as in Kronecker–Weber theorem 4.2.3. So one needs to directly define a reciprocity map

$$\Phi_F \colon I_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

and study its properties. This global reciprocity map is defined as the product of composites of local reciprocity maps $F_P^{\times} \to \mathrm{Gal}({F_P}^{\mathrm{ab}}/F_P)$ and homomorphisms $\mathrm{Gal}({F_P}^{\mathrm{ab}}/F_P) \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$.

The analog of the reciprocity law is that the kernel of Φ_F contains the image of $F^{\times}$ in I_F.

Part of class field theory associates to every open subgroups N in $I_F/F^\times$ its class field L – the unique finite abelian extension of F such that $N_{L/F}(I_L)F^\times = N$.

It also contains information on arithmetical properties of the behavior of prime numbers in finite abelian extensions as a generalization of Theorem 3.5.9 and Gauss quadratic reciprocity law.