1. Commutative algebra.

In this first section we recall some basic facts from commutative algebra. All rings are supposed to be commutative and have a unit element 1.

Proposition 1.1. *Let R be a ring.*
(i) If R is not the zero ring, it admits a maximal ideal.
(ii) An element $x \in R$ is a unit if and only if it is not contained in any maximal ideal of R.

Proof. *(i)* Consider the set Ω of all ideals $I \subset R$ that are not equal to R itself. Then Ω is partially ordered by inclusion. Every chain $\{I_\alpha : \alpha \in A\}$ has the upper bound $\cup_{\alpha\in A} I_\alpha$. It is also contained in Ω since it does not contain 1. By Zorn's Lemma there is therefore an element $\mathfrak{m} \in \Omega$ that is maximal for the inclusion relation. This means precisely that it is a maximal ideal of R.
(ii) If the ring $R/(x)$ is the zero-ring, then $1 \in (x)$ and x is a unit. If not, then part *(i)* implies that it possesses a maximal ideal. This ideal is of the form $\mathfrak{m}/(x)$ for some maximal R-ideal $\mathfrak{m}$ containing x.

Proposition 1.2. *Let R be a ring. Then the nilradical*

$$\mathrm{Nil}(R) = \{z \in R : z^n = 0 \text{ for some } n \geq 1\}$$

of R is equal to the intersection of all prime ideals of R.

Proof. It is clear that $\mathrm{Nil}(R) \subset \mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R$. Conversely, let $z \notin \mathrm{Nil}(R)$ and consider

$$\Omega = \{I \subset R : z^n \notin I \text{ for any } n \geq 1\}.$$

Since $\{0\} \in \Omega$, this is a non-empty set, partially ordered by inclusion. Since every chain has an upper bound in Ω, Zorn's Lemma applies and there is an ideal $I \subset \Omega$ that is maximal with respect to the inclusion. We claim that I is prime. Indeed, if not, then let $x, y \notin I$ while $xy \in I$. Since $I + (x)$ and $I + (y)$ are strictly larger than I, they contain each a power of z. But then so does I since it contains $(I + (x))(I + (y))$. Contradiction. Therefore I is prime. Since $z \notin I$, the proof of the proposition is complete.

Proposition 1.3. *(Chinese Remainder Theorem). Let R be a ring and let $I, J \subset R$ be two ideals for which $I + J = R$. Then the natural map*

$$R/IJ \quad \longrightarrow \quad R/I \times R/J$$

given by $(x \pmod{IJ}) \mapsto (x \pmod{I}, x \pmod{J})$ is a well-defined isomorphism of R-algebras.

Proof. The map is a well-defined R-algebra homomorphism. Let $\lambda \in I$ and $\mu \in J$ such that $\lambda + \mu = 1$. Let $x, y \in R$. Since the element $z = \mu x + \lambda y \in R$ has the property

that $z \equiv \mu x = (1-\lambda)x \equiv x \pmod{I}$ and $z \equiv \lambda y = (1-\mu)y \equiv y \pmod{J}$, the image of $(z \pmod{IJ})$ is $(x \pmod{I}, x \pmod{J})$. It follows that the map is surjective.

The kernel of the map $R \longrightarrow R/I \times R/J$ given by $x \mapsto (x \pmod{I}, y \pmod{J})$ is equal to $I \cap J$. We have that $IJ \subset I \cap J$. To see that equality holds, let $x \in I \cap J$. Then $x = x(\lambda + \mu)$ is also contained in IJ. This proves the proposition.

Definitions. Let R be a ring. A module M is said to be generated by a subset $S \subset M$, if any $m \in M$ is of the form $\lambda_1 m_1 + \ldots + \lambda_t m_t$ for some elements $m_1, \ldots, m_t \in S$ and $\lambda_1, \ldots, \lambda_t \in R$. We write $M = \sum_{m \in S} mR$. If S can be taken finite, then M is said to be *finitely generated*. If M can be generated by one element m, it is denoted by mR. In particular, the principal ideal generated by $x \in R$ is denoted by xR.

An R-module is called *free*, if it is of the form $\oplus_{s \in \Sigma} R$ for some index set Σ. A finitely generated free module is of the form R^n for some $n \geq 0$. A *projective* R-module is a direct summand of a free module. Free modules are themselves projective. Since a free module P has the property that every exact sequence of the form

$$0 \quad \longrightarrow \quad N \quad \longrightarrow \quad M \quad \longrightarrow \quad P \quad \longrightarrow \quad 0$$

is *split*, the same is true when P is merely projective.

An element m in an R-module M is called *torsion* if there is a non-zero $\lambda \in R$ for which $\lambda m = 0$. An R-module all whose elements are torsion is called a torsion module. An R-module none of whose non-zero elements are torsion is called *torsion-free*. Since free modules are torsion-free, so are projective modules.

Definition. Let R be a domain with quotient field F. The *rank* of an R-module M is defined as $\text{rank}(M) = \dim_F(M \otimes_R F)$. If M is finitely generated, we have that $\text{rank}(M) = \dim_F \text{Hom}_R(M, F)$. Ranks are additive. If N is a submodule or quotient module of M, then $\text{rank}(N) \leq \text{rank}(M)$.

Definition. A *Noetherian* ring is a ring all of whose ideals are finitely generated.

Proposition 1.4. *Let R be a ring. The following are equivalent.*

(i) R is Noetherian.

(ii) Every chain of R-ideals $I_1 \subset I_2 \subset \ldots$ stabilizes.

(iii) Every non-empty of ideals Ω possesses an element that is maximal for the inclusion ordering.

Proof. Let $I_1 \subset I_2 \subset \ldots$ be a chain of ideals of R. The union is finitely generated and a finite set of generators is contained in I_n for some $n \geq 1$. Clearly $I_k = I_n$ for all $k \geq n$ so that the chain stabilizes. This shows that *(i)* implies *(ii)*. Let Ω be a non-empty collection of R-ideals. If it does not contain a maximal element, then we can choose a infinite chain

$$I_1 \underset{\neq}{\subset} I_2 \underset{\neq}{\subset} I_3 \quad \ldots,$$

contradicting *(ii)*. Therefore *(ii)* implies *(iii)*. Finally, let I be an R-ideal and consider the set of ideals $\{J \subset I : J \text{ is finitely generated}\}$. If *(iii)* holds, there is a maximal element $J_0 \in \Omega$. Then $J_0 = I$ so that I itself is finitely generated. Indeed, if not, then pick $x \in I - J_0$ and consider the ideal generated by J_0 and x. It is an element of Ω that is strictly larger than J_0. Contradiction. Therefore *(i)* holds.

This proves the proposition.

Proposition 1.5. *Let R be a Noetherian ring. Then*

(i) For any ideal $I \subset R$, the quotient ring R/I is Noetherian.

(ii) Let M be a finitely generated R-module. Then any submodule $N \subset M$ is also finitely generated.

Proof. *(i)* Indeed, any ideal of R/I is of the form J/I where $J \subset R$ is an ideal containing I. Since R is Noetherian, J is finitely generated. The same generators generate the R/I ideal J modulo I.

(ii) We proceed with induction with respect to the number of generators of M. If M is generated by one element, then $M \cong R/I$ for some ideal I and we are done by *(i)*. If M is generated by $m_1, \ldots, m_t$ for some $t \geq 2$, then we have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N \cap Rm_1 & \longrightarrow & N & \longrightarrow & N/(N \cap Rm_1) & \longrightarrow & 0 \\ & & \downarrow \subset & & \downarrow \subset & & \downarrow \subset & & \\ 0 & \longrightarrow & Rm_1 & \longrightarrow & M & \longrightarrow & M/Rm_1 & \longrightarrow & 0 \end{array}$$

Since R is Noetherian, the module $N \cap Rm_1$ admits finitely many generators. By induction, the submodule $N/(N \cap Rm_1)$ of M/Rm_1 is also finitely generated. The set of generators of $N \cap Rm_1$ together with any lift of a finite set of generators of $N/(N \cap Rm_1)$, generate N. This proves the proposition.

Proposition 1.6. *(Hilbert Basissatz) Let R be a Noetherian ring. Then the polynomial ring $R[X]$ is also Noetherian.*

Proof. Let $I \subset R[X]$ be an ideal. For $n \geq 1$ consider the R-ideals

$$J_n = \{\text{leading coefficients of } f \in I \text{ with } \deg f \leq n\}$$

We have that

$$J_1 \subset J_2 \subset J_3 \subset \ldots$$

Since R is Noetherian, this sequence stabilizes at J_{n_0}, say. Consider the R-module $M = \{f \in I : \deg f \leq n_0\}$. Since M is a submodule of the finitely generated free R-module of *all* polynomials of degree n_0, Prop. 1.5 implies that it is itself finitely generated over R. Let $f_1, \ldots, f_t$ be generators. Note that their leading coefficients $a_1, \ldots, a_t$ generate J_{n_0}.

We claim that $f_1, \ldots, f_t$ generate the $R[X]$-ideal I. Indeed, let $\varphi(X) \in I$. If $\deg \varphi \leq n_0$, then $\varphi \in M$ and φ is even an R-linear (rather than $R[X]$-linear) combination of $f_1, \ldots, f_t$. If $\deg \varphi = n > n_0$, then the leading coefficient a of φ is contained in J_n and hence in J_{n_0}. This means that $a = \lambda_1 a_1 + \ldots + \lambda_t a_t$ for certain $\lambda_1, \ldots, \lambda_t \in R$. Consider now the polynomial $\psi(X) = \varphi(X) - \sum_{i=1}^{t} \lambda_i X^{n - \deg f_i} f_i(X)$. Then $\psi \in I$ and its degree is smaller than n because its n-th degree coefficient is equal to $a - \sum_{i=1}^{t} \lambda_i a_i = 0$.

The proof of the proposition is now completed with respect to induction of the degree of φ.

Corollary 1.7. *For any $n \geq 0$ and any ideal I of $\mathbf{Z}[X_1, \ldots, X_n]$ the ring $\mathbf{Z}[X_1, \ldots, X_n]/I$ is Noetherian. For any field K, any $n \geq 0$ and and any ideal $J \subset K[X_1, \ldots, X_n]$, the ring $K[X_1, \ldots, X_n]/J$ is Noetherian.*

Proof. This follows from Proposition 1.5 and Theorem 1.6.

Definition. Let R be a ring and let M be an R-module. Then M is called *faithful* if the natural homomorphism $R \longrightarrow \mathrm{End}(M)$ that maps $x \in R$ to the multiplication by x map, is injective.

Definition. Let $R \subset S$ be an inclusion of rings. An element $x \in S$ is called *integral* over R if there exists a monic polynomial $f \in R[X]$ with $f(x) = 0$.

Proposition 1.8. *Let $R \subset S$ be an inclusion of rings and let $x \in S$. The following are equivalent.*
(i) x is integral over R.
(ii) The subring $R[x]$ of S is finitely generated as an R-module.
(iii) There exists a finitely generated faithful R-submodule $M \subset S$ for which $xM \subset M$.

Proof. If x is zero of a *monic* polynomial in $R[X]$ of degree n, the ring $R[x]$ is generated as an R-module by the elements $1, x, \ldots, x^{n-1}$. This shows that *(i)* implies *(ii)*. Since $R[x]$ contains 1, it is a faithful R-module. Therefore *(ii)* implies *(iii)*. To show that *(iii)* implies *(i)*, let $e_1, e_2, \ldots, e_t$ denote generators of M as an R-module. Since $xM = \{xm : m \in M\}$ is contained in M, there exist for every $i = 1, 2, \ldots, t$ coefficients $\lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{it} \in R$ such that

$$xe_i = \sum_{j=1}^{t} \lambda_{ij} e_j.$$

It follows that $\det(\lambda_{ij} - x\delta_{ij})e_i = 0$ for all i. Here δ_{ij} denotes the Kronecker δ-function: $\delta_{ij} = 1$ when $i = j$ and is 0 otherwise. As a consequence $\det(\lambda_{ij} - x\delta_{ij})$ kills every element of M. Since M is faithful it follows that $\det(\lambda_{ij} - x\delta_{ij})$ is zero and hence that the monic polynomial $\det(\lambda_{ij} - X\delta_{ij}) \in R[X]$ has x as a zero. This proves the proposition.

Corollary 1.9. *Let $R \subset S$ be an inclusion of rings. The elements in S that are integral over R form a subring of S that contains R.*

Proof. Since any $a \in R$ is zero of the polynomial $X - a \in R[X]$, the last statement is clear. We need to show that for any two integral elements $x, y \in S$, both sum and product are integral as well. The subrings $R[x]$ and $R[y]$ are generated as R-modules by $1, x, \ldots, x^{n-1}$ and $1, y, \ldots, y^{m-1}$ respectively. It follows that the subring $R[x, y]$ is generated as an R-module by the monomials $x^i y^j$ with $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$. Since $x + y$ and xy are contained in $R[x, y]$, the result now follows from the previous proposition.

Definition. A domain R is called *integrally closed* or *normal* if every element in its quotient field that is integral over R, is already contained in R.

Proposition 1.10. *Principal ideal domains are integrally closed.*

Proof. Any element x in its quotient field is of the form $x = u/v$ with coprime $u, v \in R$, i.e. with u, v such that $uR + vR = R$. Suppose $f(X) = X^n + \ldots + a_1 X + a_0 \in R[X]$ has x as a zero. Then

$$u^n + \ldots + a_1 u v^{n-1} + a_0 v^n = 0.$$

If v is *not* a unit, then its is contained in some maximal ideal $\mathfrak{m} = \pi R$ of R. It follows that v^n and hence v are in πR. This contradicts that fact that $uR + vR = R$. therefore v is a unit and x is integral, as required.

Definition. The *Krull dimension* $\dim R$ of a domain R is defined as the supremum of the $n \geq 0$ for which there exists a chain of prime ideals

$$(0) = \mathfrak{p}_0 \underset{\neq}{\subset} \mathfrak{p}_1 \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} \mathfrak{p}_n \underset{\neq}{\subset} R$$

of R.

Proposition 1.11. *Let R be a domain. Then*
(i) $\dim R = 0$ *if and only if R is a field.*
(ii) $\dim R \leq 1$ *if R is a principal ideal domain.*

Proof. If R is a field, the only prime ideal is its zero ideal. Conversely, a domain that does not contain any non-zero prime ideals is a field. This follows from Prop. 1.1. This proves *(i)*. To prove *(ii)*, let R be a principal ideal domain and let $\mathfrak{p} = aR$ be a non-zero prime ideal of R. We want to show it is a maximal ideal. Let $\mathfrak{m} = bR$ be a maximal ideal containing a. Then $a = \lambda b$ for some $\lambda \in R$. If $\lambda \in \mathfrak{p}$, we have that $\lambda = \mu a$ for some $\mu \in R$ and hence $a = \lambda b = \mu a b$ and hence $\mu b = 1$. However, this is impossible, because b is not a unit. Therefore $\lambda \notin \mathfrak{p}$. Since $a = \lambda b \in \mathfrak{p}$, this implies that $b \in \mathfrak{p}$ and hence $\mathfrak{m} = \mathfrak{p}$ as required.

Exercises

1.1 Let R be a ring. Show that for every R-module M there exists a free R-module F and a surjective R-homomorphism $F \twoheadrightarrow M$. Does there always exist a free R-module F and an *injective* R-homomorphism $M \hookrightarrow F$?

1.2 If possible, give an example of an exact sequence of finite abelian groups

$$0 \longrightarrow N \longrightarrow (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/8\mathbf{Z}) \longrightarrow M \longrightarrow 0.$$

with
(i) $M \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ and $N \cong \mathbf{Z}/4\mathbf{Z}$;
(ii) $M \cong \mathbf{Z}/4\mathbf{Z}$ and $N \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$;
(iii) $M \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ and $N \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$;
(iv) $M \cong \mathbf{Z}/4\mathbf{Z}$ and $N \cong \mathbf{Z}/4\mathbf{Z}$.

1.3 Show that the dimension of the polynomial ring $\mathbf{R}[X_1, \ldots, X_n]$ is at least n. Show that the dimension of the polynomial ring $\mathbf{Z}[X_1, \ldots, X_n]$ is at least $n + 1$.

1.4 Let R be a ring. Show that $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Q}/\mathbf{Z}$ and $\oplus_{n \geq 1} \mathbf{Z}/n\mathbf{Z}$ are faithful $\mathbf{Z}$-modules. Give an example of a $\mathbf{Z}$-module that is not faithful.

1.5 Let R be a domain with quotient field F. The *integral closure* of R is the subring R' of F that consists of all $x \in F$ that are integral over R. Show that R' is integrally closed.

1.6 Let $n \in \mathbf{Z}_{>0}$; consider the ring $R = \mathbf{Z}[X]/(X^2, nX)$.

(i) Determine the unit group R^*.

(ii) Let $a, b \in \mathbf{Z}$. Show that the R-ideal aXR is contained in bXR if and only if $\gcd(b, n)$ divides $\gcd(a, n)$.

(iii) Find $n \in \mathbf{Z}_{>0}$ and $a, b \in \mathbf{Z}$ for which the ideals aXR and bXR of R are equal, while there does not exist a unit $u \in R^*$ with $uaX = bX$.

1.7 Let R be a ring and let M, N be R-modules.

(i) Show that the abelian group $\mathrm{Hom}_R(M, N)$ of R-homomorphisms has the structure of an R-module given by $(\lambda f)(m) = \lambda f(m)$ (for $\lambda \in R$, $m \in M$ and $f \in \mathrm{Hom}_R(M, N)$).

(ii) Let $f : M \longrightarrow N$ be an R-homomorphism. and let P be a third R-module. Show that the map $f_P : \mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, N)$ given by $f_P(\varphi) = f \cdot \varphi$ is a group homorphism.

(iii) Suppose that

$$0 \quad \longrightarrow \quad L \quad \xrightarrow{f} \quad M \quad \xrightarrow{g} \quad N \quad \longrightarrow \quad 0.$$

is an exact sequence of R-modules. Show that the induced sequence

$$0 \quad \longrightarrow \quad \mathrm{Hom}_R(P, L) \quad \xrightarrow{f_P} \quad \mathrm{Hom}_R(P, M) \quad \xrightarrow{g_P} \quad \mathrm{Hom}_R(P, N) \quad \longrightarrow \quad 0$$

is *left-exact* (i.e., exact except perhaps at $\mathrm{Hom}_R(P, N)$).

(iv) Show that the sequence of part *(iii)* is exact if P is projective.

(v) Let $R = \mathbf{Z}$ and $P = \mathbf{Z}/2\mathbf{Z}$. Give an example of a short exact sequence $0 \to L \to M \to N \to 0$ of abelian groups, for which the sequence

$$0 \longrightarrow \mathrm{Hom}_R(\mathbf{Z}/2\mathbf{Z}, L) \quad \xrightarrow{f_{\mathbf{Z}/2\mathbf{Z}}} \quad \mathrm{Hom}_R(\mathbf{Z}/2\mathbf{Z}, M) \quad \xrightarrow{g_{\mathbf{Z}/2\mathbf{Z}}} \quad \mathrm{Hom}_R(\mathbf{Z}/2\mathbf{Z}, N) \longrightarrow 0$$

is not exact.

2. Dedekind rings.

Rings of integers of algebraic number fields are Noetherian integrally closed domains of Krull dimension 1. Rings having these properties are called Dedekind rings. In this section we discuss their basic properties.

Definition. A ring R is called a *Dedekind ring* if it is a Noetherian, integrally closed domain of Krull dimension ≤ 1.

Proposition 2.1. *Prinicipal ideal domains are Dedekind domain.*

Proof. Principal ideal domains are clearly Noetherian. It follows therefore from Propositions 1.10 and 1.11 that they are Dedekind rings.

Theorem 2.2. *Let R be a Dedekind domain. For every two non-zero R-ideals $I \subset J$, there exists a unique R-ideal J' so that $JJ' = I$.*

Proof. The unicity of J' follows from the existence: pick a non-zero $x \in J$. Then there is an ideal J'' for which $JJ'' = xR$. If there were two ideals J'_1 and J'_2 with $I = JJ'_1 = JJ'_2$, then multiplying by J'' gives that $xJ'_1 = xJ'_2$ and hence $J'_1 = J'_2$.
Claim. Every non-zero R-ideal contains a product of non-zero prime ideals.
Proof. Suppose not. Let I be a maximal element in the non-empty partially ordered set Ω of ideals for which the statement is false. Then I is certainly not itself a prime ideal. Therefore there are x, y not in I with $xy \in I$. The strictly larger ideals $I + xR$ and $I + yR$ each contain a product of non-zero prime ideals. Since I contains the product of $I + xR$ and $I + yR$, so does I. Contradiction.

Suppose $I \subset J$ are R-ideals for which the statement of the theorem does not hold. Since R is Noetherian, we may by Prop, 1.4 *(iii)* assume that J is *maximal* with respect to this property, i.e. that for every strictly larger J and any ideal $I \subset J$, the statement of the theorem is true. Let y be non-zero element of J. By the claim, the principal ideal yR contains a product of non-zero prime ideals

$$\prod_{i=1}^{s} \mathfrak{p}_i \quad \subset \quad yR,$$

which we assume has a minimal number of factors $s \geq 1$. The ideal yR is contained in a maximal ideal $\mathfrak{m}$. Then $\mathfrak{p}_1 \subset \mathfrak{m}$, say. Since R has dimension ≤ 1, it follows that $\mathfrak{m} = \mathfrak{p}_1$. Since the number of factors in the product is minimal, we have that

$$\prod_{i=2}^{s} \mathfrak{p}_i \quad \not\subset \quad yR.$$

Let $x \in \prod_{i=2}^{s} \mathfrak{p}_i - yR$. Note that this means that the fraction $\frac{x}{y}$ is not contained in R. However, $\frac{x}{y}J \subset R$ because $xJ \subset x\mathfrak{p}_1 \subset \prod_{i=1}^{s} \subset yR$. This implies that the R-ideal $J + \frac{x}{y}J$ *strictly* contains J. Indeed, if not we would have that $\frac{x}{y}J \subset J$ so that $\frac{x}{y}$ would be integral over R and hence be contained in R.

Since

$$I \quad \subset \quad J \quad \underset{\neq}{\subset} \quad J + \tfrac{x}{y}J,$$

there exists by the maximality of J an ideal J' so that $I = J'(J + \frac{x}{y}J)$. Consider now $J'' = J' + \frac{x}{y}J'$. Then $J''J = (J' + \frac{x}{y}J')J = I$. In particular, $J''J \subset J$ so that every $x \in J''$ is integral and hence $J'' \subset R$. This proves the theorem.

Corollary 2.3. *Let R be a Dedekind domain. Then every non-zero ideal is a product of prime ideals. Up to permutation of the prime ideals, this factorization of I is unique.*

Proof. Let I be a non-zero ideal of R. If $I \neq R$, it is contained in some maximal ideal $\mathfrak{p}$. By the Theorem, there is an R-ideal I_1 so that $I = \mathfrak{p}I_1$. The ideal I_1 strictly contains I. Repeat this with I_1 instead of I. Since R is Noetherian, this process must stop at some ideal I_n. Then $I_n = R$. Indeed, if we had that $I_n = \mathfrak{p}I_{n+1} = \mathfrak{p}I_n$ for some prime $\mathfrak{p}$, then $\mathfrak{p} = R$ by the unicity statement of Theorem 2.2. This shows the existence of a prime factorization.

If we have two prime factorizations, then any prime $\mathfrak{p}$ occurring in one factorization must occur also in the other. Pick $0 \neq x \in \mathfrak{p}$ and let $J \subset R$ be the ideal for which $J\mathfrak{p} = xR$. After multiplying the factorizations by J, we can divide by x and are left with two factorizations with fewer factors. This process eventually stops, at which point we conclude that the factorizations were equal as required.

Definition. Let R be a Dedekind domain with quotient field F. For every non-zero R-ideal J and every non-zero prime ideal of R we put $\mathrm{ord}_{\mathfrak{p}}(J) = a_{\mathfrak{p}}$, where the $a_{\mathfrak{p}} \in \mathbf{Z}_{\geq 0}$ is the exponent that occurs in the prime factorization of the ideal J:

$$J = \prod_{\mathfrak{q}} \mathfrak{q}^{a_{\mathfrak{q}}}.$$

A *fractional R-ideal* is a subset I of F for which there exist $x \in O_F$ so that $xI = \{xy : y \in I\}$ is a non-zero ideal of R. For any non-zero prime ideal $\mathfrak{p}$ of R we put

$$\mathrm{ord}_{\mathfrak{p}}(I) = \mathrm{ord}_{\mathfrak{p}}(xI) - \mathrm{ord}_{\mathfrak{p}}(xR).$$

The product of two fractional ideals I and J is the submodule of F generated by elements of the form xy with $x \in I$ and $y \in J$. By Corollary 2.3, the fractional ideals form a group isomorphic to $\oplus_{\mathfrak{p}}\mathbf{Z}$. For any $x \in F^*$, the *principal fractional ideal generated by x* is the set $xR = \{xy : y \in R\}$. For $x \in F^*$ and any non-zero prime ideal $\mathfrak{p}$ of R we put

$$\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(xR).$$

This is a homomorphism from F^* to $\mathbf{Z}$. An element $x \in F^*$ is contained in R if and only if $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ for all prime ideals $\mathfrak{p}$. It is contained in the unit group R^* if and only if $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for all prime ideals $\mathfrak{p}$. Putting all these homomorphisms together, we obtain therefore an exact sequence

$$0 \quad \longrightarrow \quad R^* \quad \longrightarrow \quad F^* \quad \longrightarrow \quad \bigoplus_{\mathfrak{p}} \mathbf{Z} \quad \longrightarrow \quad Cl(R) \quad \longrightarrow \quad 0,$$

which we use to define the *class group* $Cl(R)$ of R.

Two ideals $I, J \subset R$ have the same image in $Cl(R)$ if and only if there are non-zero $x, y \in R$ so that $xI = yJ$. Since any R-homomorphism $I \longrightarrow J$ is given by multiplication by an element in F^*, this happens if and only if I and J are isomorphic R-modules. Therefore the map

$$\{\text{non-zero } R\text{-ideals up to } R\text{-isomorphism}\} \quad \stackrel{\cong}{\longrightarrow} \quad Cl(R)$$

that send an ideal to its class, is a bijection.

Proposition 2.4. *Let R be a Dedekind ring. Then the following are equivalent.*
(i) The class group $Cl(R)$ is trivial.
(ii) R is a principal ideal domain.
(iii) R is a unique factorization domain.

Proof. For any ring *(ii)* implies *(iii)*. To show that *(i)* implies *(ii)*, let $I \subset R$ be a non-zero ideal. Let $I = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$ be its factorization into a product of non-zero prime ideals of R. Since $Cl(R)$ is trivial, there is an element $x \in F^*$ for which $\mathrm{ord}_{\mathfrak{p}}(x) = a_{\mathfrak{p}}$. The implies that $x \in R$ and that $I = xR$ so that I is principal. Finally, to show that *(iii)* implies *(i)*, it suffices to show that every non-zero prime of R is principal. This implies that every vector $(a_{\mathfrak{p}}) \in \oplus_{\mathfrak{p}} \mathbf{Z}$ is the image of a suitable element in F^*. Let therefore $\mathfrak{p}$ be a non-zero prime and let $0 \neq x \in \mathfrak{p}$. Since x is a product of irreducible elements, it follows that $\mathfrak{p}$ contains an irreducible element π. But then $\pi R \subset \mathfrak{p}$ are two non-zero prime ideals of R. Since R has dimension 1, they are therefore equal.

This proves the proposition.

Lemma 2.5. *Let R be a Dedekind ring and let $I \subset R$ be a non-zero ideal. Then R/I is a principal ideal ring. A local Dedekind ring is a discrete valuation domain.*

Definition. The ideals of R/I are of the form J/I where $J \subset R$ is an ideal containing I. Every such J is a product of prime ideals $\mathfrak{p}$. It suffices to show that each such prime is of the form $\mathfrak{p} = I + xR$ for some $x \in R$. By the Chinese Remainder Theorem, there exists an element $x \in \mathfrak{p} - \mathfrak{p}^2$ which is congruent to 1 modulo the remaining primes that occur in the factorization of J. Then $I + xR \subset \mathfrak{p}$. By Theorem 2.2 there exists therefore an ideal $J' \subset R$ with $J'\mathfrak{p} = I + xR$. Any prime occuring in the prime factorization of J' occurs in the prime factorization of I and of xR. Therefore only $\mathfrak{p}$ can occur. However, since $I + xRnot \subset \mathfrak{p}^2$, the prime $\mathfrak{p}$ does not occur either. Therefore J' is the unit ideal and $\mathfrak{p} = I + xR$ as required.

If R is a local Dedekind ring with maximal ideal $\mathfrak{m}$, then $R/\mathfrak{m}^2$ is a principal ideal ring. Let $\pi \in R$ be a generator of $\mathfrak{m}/\mathfrak{m}^2$. Then $\pi R = \mathfrak{m}$ is the unique factorization into prime ideals of the ideal πR. It follows that R is a discrete valuation ring, the valuation $F^* \longrightarrow \mathbf{Z}$ being given by $x \mapsto \mathrm{ord}_{\mathfrak{m}}(x)$.

This proves the lemma.

Proposition 2.6. *Let R be a Dedekind ring and let $I, J \subset R$ be two non-zero ideals. Then*

$$I \oplus J \quad \cong \quad R \oplus IJ, \qquad \text{as } R\text{-modules.}$$

Proof. If $I + J = R$, we have that $IJ = I \cap J$ and the result follows from the following split-exact sequence

$$0 \quad \longrightarrow \quad IJ \quad \longrightarrow \quad I \oplus J \quad \longrightarrow \quad R \quad \longrightarrow \quad 0.$$

To get the statement in general, it suffices to show that for any two R-ideals I, J there exists an ideal $J' \subset R$ in the same ideal class as J that is coprime to I. Pick a non-zero element $x \in J$. By Theorem 2.2 there exists an ideal $J_1 \subset R$ with $JJ_1 = xR$. Then $IJ_1 \subset J_1$, so by Prop. 2.5 there exists $y \in J_1$ so that $IJ_1 + yR = J_1$. Multiplying this relation by the ideal J we get

$$IJ_1J + yJ = J_1J.$$

since $yJ \subset J_1J = xR$, we have that $yJ = xJ'$ for some ideal $J' \subset R$. In particular, J and J' are in the same ideal class of R. Replacing yJ by xJ' and JJ_1 by xR in the formula leads to the equality $xI + xJ' = xR$, which after division by x gives the required result.

Corollary 2.7. *Every ideal of a Dedekind ring R is projective.*

Proof. Let $I \subset R$ be an ideal. If $I = 0$, everything is clear. If not, pick $0 \neq x \in I$. By Theorem 2.2 there is an ideal $J \subset R$ with $IJ = xR$. The proposition implies that

$$I \oplus J \quad \cong \quad R \oplus xR \quad \cong \quad R^2,$$

showing that I is projective as required.

Lemma 2.8. *Let R be a Dedekind ring. Let M be a torsion-free R-module. Then* $\operatorname{rank}(M) = 1$ *if and only if M is isomorphic to a non-zero R-ideal.*

Proof. For any non-zero ideal $I \subset R$ we have that $\operatorname{Hom}_R(I, F) \cong F$, the isomorphism being given by $f \mapsto f(x)/x$ where $x \in I$ is any non-zero element. On the other hand, if M is a torsion free R-module for which $\operatorname{Hom}_R(M, F) \cong F$ is 1-dimensional, then we can find an R-linear $f : M \longrightarrow F$ whose image is a non-zero ideal J in R. Since J is projective, the sequence $0 \to \ker f \to M \to J \to 0$ splits. This implies that $\ker f$ has rank 0. Since M is torsion-free, it follows that $\ker f$ is zero and hence that $M \cong J$ as required.

Theorem 2.9. *Let R be a Dedekind domain. Suppose that M is a direct product of R-ideals and that $N \subset M$ is a submodule. Then*

(i) the submodule N is also isomorphic to a product of R-ideals.

(ii) There exist $n \geq 0$ and elements $e_i \in M$ and R-ideals $J_i \subset I_i$ for $i = 1, \ldots, n$ so that

$$\begin{aligned} M &= I_1e_1 \oplus \cdots \oplus I_ne_n, \\ N &= J_1e_1 \oplus \cdots \oplus J_ne_n. \end{aligned}$$

Proof. If $N \neq 0$, then there is a non-torsion element $x \in N$ and hence an isomorphism $xR \longrightarrow R$. This isomorphism extends to a morphism of N and even of M to R. We denote it by φ. The images $\varphi(M)$ and $\varphi(N)$ are non-zero ideals I and J of R. Let $K \subset M$ denote the kernel of φ. We have the following commutative diagram with split-exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K \cap N & \longrightarrow & N & \xrightarrow{\varphi} & J & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \subset} & & \downarrow{\scriptstyle \subset} & & \downarrow{\scriptstyle \subset} & & \\ 0 & \longrightarrow & K & \longrightarrow & M & \xrightarrow{\varphi} & I & \longrightarrow & 0 \end{array}$$

(i) We proceed with induction with respect to the rank of N. If the rank of N is 0, then N, being torsion free, is itself 0 and there is nothing to prove. If $\text{rank}(N) \geq 1$, then the above applies. Since the rank of J is 1, the rank of $K \cap N$ is strictly smaller than $\text{rank}(N)$ and we are done, since the sequence splits.
(ii) This part is proved with induction with respect to the rank of M. If $\text{rank}(M) = 1$, then M is isomorphic to an ideal of R and everything is clear. If $\text{rank}(M) > 1$, then the above applies. By part *(i)* the module K is isomorphic to a product of R-ideals. Since $\text{rank}(J) = 1$ the result now follows by induction.

Corollary 2.10. *Let R be a Dedekind ring. Then any finitely generated R-module is a direct product of a torsion module T and a projective module P. Moreover, there are R-ideals $I_1, \ldots, I_s$ so that*

$$T \quad \cong \quad (R/I_1) \times \cdots (R/I_s),$$

and for some $r \geq 0$ and some ideal $I \subset R$ we have that

$$P \quad \cong \quad R^r \times I$$

Proof. Let M be a finitely generated R-module and choose a surjective R-morphism $R^n \longrightarrow M$. Let N be the kernel. Then $M \cong R^n/N$ and it follows from Theorem 2.9 that M is isomorphic to $I_1/J_1 \oplus \cdots \oplus I_s/J_s$ for certain ideals $J_i \subset I_i$ (for $i = 1, \ldots, s$). The summands that have $J_i = 0$ is isomorphic to a sum of ideals of R. By Prop. 2.6, this sum is either zero or is isomorphic to $R^r \oplus I$ for some $r \geq 0$ and some ideal I. For the summands for which $J_i \neq 0$ part, we have by Prop. 2.5 that $I_i = J_i + xR$ for some $x \in R$. This implies that $I_i/J_i \cong (J_i + xR)/J_i \cong xR/J$ where $J = xR \cap J_i$.

Corollary 2.11. *Let R be a Dedekind ring. Then any finitely generated R-module is projective if and only if it is torsion-free.*

Corollary 2.12. *Let R be a principal ideal domain and let M be a finitely generated R-module. Then*
(i) M is free if and only if it is projective and if and only if it is torsion-free.
(ii) There exist elements $a_1, a_2, \ldots, a_t \in R$ so that M is isomorphic to the R-module

$$R/a_1R \times \ldots \times R/a_tR.$$

Proof. If M is free, it is projective and hence torsion-free. Conversely, if M is torsion-free it is projective. By Prop. 2.4 it is therefore free. This proves *(i)*. Part *(ii)* is a consequence of the fact that all R-ideals are principal.

Proposition 2.13. *(Gauss' Lemma) Let R be a Dedekind ring with quotient field F. Suppose that $f \in R[X]$ is a product of two monic polynomials $g, h \in F[X]$. Then g and h are contained in $R[X]$.*

Proof. Suppose that $f = g \cdot h$ with monic polynomials $g, h \in F[X]$ and let $\mathfrak{p}$ be a prime ideal. We claim that all coefficients of g and h are integral at $\mathfrak{p}$. Indeed, suppose not. Let

$i \geq 0$ be the smallest power so that $\mathfrak{p}^i g \subset R[X]$ and let $j \geq 0$ be the smallest power so that $\mathfrak{p}^i h \subset R[X]$. Let $a \in \mathfrak{p} - \mathfrak{p}^2$ and consider the relation

$$a^{i+j} f = (a^i g) \cdot (a^j h).$$

By assumption $i + j \geq 1$. This implies that the left hand side is zero in the ring $(R/\mathfrak{p})[X]$. On the other hand, the polynomial $a^i g \not\equiv 0 \pmod{\mathfrak{p}}$. Indeed, if $i = 0$ this follows from the fact that g is monic and if $i > 0$ there is by definition of i a coefficient b of g for which $\mathrm{ord}_{\mathfrak{p}}(b) = -i$. This implies that the coefficient $a^i b$ of $a^i g$ has its $\mathrm{ord}_{\mathfrak{p}}$ equal to zero and is therefore not zero modulo $\mathfrak{p}$. Similarly, $a^j h \not\equiv 0 \pmod{\mathfrak{p}}$. This contradicts the fact that $(R/\mathfrak{p})[X]$ is a domain. This proves the proposition.

Exercises.

2.1 Let $R = \mathbf{Z}$, let $M = \mathbf{Z}^2$ and $N = \begin{pmatrix} 2 \\ 5 \end{pmatrix}\mathbf{Z} + \begin{pmatrix} 7 \\ 2 \end{pmatrix}\mathbf{Z}$. Find a basis for M as in Theorem 2.8. Do the same for $N' = \begin{pmatrix} 4 \\ 8 \end{pmatrix}\mathbf{Z} + \begin{pmatrix} 6 \\ 12 \end{pmatrix}\mathbf{Z}$.

2.2 (Jordan Normal Form). Let A be an $n \times n$-matrix with complex coefficients. Prove that there exists an invertible matrix B so that BAB^{-1} has a 'block form' with each block of the shape

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & & \cdots & \lambda & 1 \\ 0 & 0 & & \cdots & 0 & \lambda \end{pmatrix}$$

for some $\lambda \in \mathbf{C}$. (Sugg. Take $R = \mathbf{C}[X]$ and provide $\mathbf{C}^n$ with the structure of a $\mathbf{C}[X]$-module by defining $X \cdot v = Av$ for every $v \in \mathbf{C}^n$. Then apply Cor. 2.12 and the Chinese Remainder Theorem).

2.3 Let R be a Dedekind ring and let $I_1, \ldots, I_r, J_1, \ldots, J_s$ be non-zero R-ideals. Show that the R-modules $I_1 \times \ldots \times I_r$ and $J_1 \times \ldots \times J_s$ are isomorphic if and only if $r = s$ and the ideal classes of the products $I_1 \cdot \ldots \cdot I_r$ and $J_1 \cdot \ldots \cdot J_s$ are equal.

2.4 Let $d \in \mathbf{Z}$ be squarefree. We define the *Norm* of an element $x \in \mathbf{Q}(\sqrt{d})$ by $N(x) = a^2 - db^2$. Here $a, b \in \mathbf{Q}$ are taken so that $x = a + b\sqrt{d}$. Show that the norm map is multiplicative: $N(xy) = N(x)N(y)$ for all $x, y \in \mathbf{Q}(\sqrt{d}$.

2.5 Let $R = \mathbf{Z}[\sqrt{-6}]$.

(i) Show that $10 = 2 \cdot 5$ and $10 = (2+\sqrt{-6})(2-\sqrt{-6})$ are two factorizations of $10 \in \mathbf{Z}[\sqrt{-6}]$ that are essentially distinct in the sense that the factorizations cannot be transformed into one another by multiplying the factors by units.

(ii) Find the factorizations of the principal ideals (2), (5), $(2 + \sqrt{-6})$ and $(2 - \sqrt{-6})$ into a product of prime ideals of $R = \mathbf{Z}[\sqrt{-6}]$.

2.6 Let R be a domain and let $N : R - \{0\} \longrightarrow \mathbf{R}_{>0}$ be a multiplicative function. The ring R is called *Euclidean* with respect to the map N if for every $x, y \in R$ with $y \neq 0$, there exist $q, r \in R$ with $y = qx + r$ and either $r = 0$ or $N(r) < N(y)$.

(i) Show that a Euclidean domain is a PID.
(ii) Show that the ring $\mathbf{Z}$ is Euclidean with respect to the map $N(n) = |n|$.
(iii) Let K be a field. Show that the polynomial ring $K[X]$ is Euclidean with respect to the map $N(f) = e^{\deg f}$.
(iv) Show that the ring of integers $\mathbf{Z}[i]$ of Gauss is Euclidean with respect to the map $N(a+bi) = a^2 + b^2$ (where $a, b \in \mathbf{Z}$).

2.7. Let R be a domain with quotient field F. Suppose that R is equipped with a multiplicative function $N : R - \{0\} \longrightarrow \mathbf{R}_{>0}$. Show that N can be extended to a a homomorphism $F^* \longrightarrow \mathbf{R}_{>0}$. Show that R is Euclidean if and only if for every $x \in F$, either $x \in R$ or there exists an element $x \in R$ with $N(x - y) < 1$.

3. Finite free algebras.

In this section we discuss finite free algebras over a base ring R.

Definition. Let R be a ring. A *finite free R-algebra* is an R-algebra that is finitely generated and free as an R-module.

Examples of finite free algebras are R-algebras of the form $R[X]/(\varphi(X))$ where $\varphi(X) \in R[X]$ is a monic polynomial. If R is a field, any finite extension of R is automatically a finite free R-algebra.

Definition. Let R be a ring and let A be a finite free R-algebra. For any $a \in A$, multplication by a is an R-linear map. With respect to an R-basis of A, it can be described by a the square matrix M with entries in R. We define the *norm* of a by $N(a) = \det(A)$ and the *trace* of a by $\mathrm{Tr}(a) = \mathrm{Trace}(A)$. The *characteristic polynomial* $f^a_{\mathrm{char}}(X)$ of a is defined as the characteristic polynomial $\det(X \cdot \mathrm{id} - M)$ of M.

Definition. The *discriminant* of a finite free R-algebra is defined by

$$\Delta(A/R) = \det(\mathrm{Tr}(\omega_i \omega_j))$$

where $\omega_1, \ldots, \omega_n$ is any R-basis for A. Changing the basis, changes $\Delta(A/R)$ by the square of the determinant of the base change matrix M. Therefore $\Delta(A/R)$ is an element of R that is well defined up to multiplication by squares of units of R.

Proposition 3.1. *Let R be a ring and $\varphi(X) \in R[X]$ be a monic polynomial. Then the discriminant of $A = R[X]/(\varphi(X))$ is equal to the discriminant of φ. In other words, if $\lambda_1, \ldots, \lambda_n$ denote the zeroes of φ, then $\Delta(A/R) = \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j)^2$.*

Proof. We use the R-basis $\omega_1, \ldots, \omega_n = 1, X, \ldots, X^{n-1}$ of A. The multiplication by X matrix A has an almost diagonal form and one easily computes that its characteristic polynomial is equal to φ. Counting multiplicities, let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of A. Then $\mathrm{Tr}(A^k) = \lambda_1^k + \ldots + \lambda_n^k$ and

$$\begin{pmatrix} \mathrm{Tr}(\omega_1^2) & \cdots & \mathrm{Tr}(\omega_n \omega_1) \\ \mathrm{Tr}(\omega_1 \omega_2) & \cdots & \mathrm{Tr}(\omega_n \omega_2) \\ \vdots & & \vdots \\ \mathrm{Tr}(\omega_1 \omega_n) & \cdots & \mathrm{Tr}(\omega_n^2) \end{pmatrix} = M^t M, \qquad \text{where } M = \begin{pmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_n \\ \vdots & & \vdots \\ \lambda_1^{n-1} & \cdots & \lambda_n^{n-1} \end{pmatrix}$$

The determinant of the Vandermonde matrix M is equal to $\prod_{1\leq i<j\leq n}(\lambda_i - \lambda_j)$ and the result follows.

Definition. For *any* R-algebra A, its module of *Kähler differentials* $\Omega^1_{A/R}$ is the A-module generated by symbols da for $a \in A$ modulo the A-submodule generated by the relations $d\lambda$ for $\lambda \in R$ and $d(a+b) - da - db$ and $d(ab) - adb - bda$ for $a, b \in A$

Example. Let R be a ring and $\varphi(X) \in R[X]$ be a monic polynomial and let $A = R[X]/(\varphi(X))$. Then the module of Kähler differentials $\Omega^1_{A/R}$ is given by $AdX/\varphi'(X)dX$. It is isomorphic to the A-mdoule $R[X]/(\varphi(X), \varphi'(X))$.

Definition. Let F be a field. A polynomial $f \in F[X]$ is called *separable* if it has no double zeroes in $\overline{F}$ or, equivalently, if $\gcd(f, f') = 1$. The field F is called *perfect* if every irreducible polynomial $f \in F[X]$ is separable.

Proposition 3.2. *(Theorem of the primitive element). Let F be a perfect field. Then every finite field extension K of F is of the form $F(\gamma)$ for some so-called primitive element $\gamma \in K$.*

Proof. If F is finite, we let γ denote a generator of the multiplicative group L^*. Then we have that $L = F(\gamma)$. If F is infinite, we proceed by induction with respect to $[L : F]$. It suffices to show that any field of the form $F(\alpha, \beta)$ with $\alpha, \beta \in F$ is also of the form $F(\gamma)$ for some $\gamma \in L$. Let $f, g \in F[X]$ be the minimum polynomials of α and β respectively. Since F is separable, both f and g have distinct zeroes. Let $\lambda \in F^*$ be distinct from all numbers

$$\frac{\alpha - \alpha'}{\beta - \beta'}$$

where $\alpha' \neq \alpha$ denotes a zero of f and $\beta' \neq \beta$ a zero of g. Consider $\gamma = \alpha + \lambda\beta$. It is distinct from $\alpha' + \lambda\beta'$ for all choices of α' and β'. This implies that the polynomials $f(\gamma - \lambda T)$ and $g(T)$ have only the zero β in common. Since both polynomials are contained in the ring $F(\gamma)[T]$, this implies that $\beta \in F(\gamma)$. It follows that $\alpha \in F(\gamma)$ as well and the proposition follows.

Theorem 3.3. *Let F be a field and let A be a finite F-algebra. Then A is isomorphic to a product of local F-algebras with nilpotent maximal ideals.*

Proof. Suppose that $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ are distinct maximal ideals of A. Then, if $\mathfrak{m}$ is yet another maximal ideal, we have that $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t \not\subset \mathfrak{m}$ because the product $\mathfrak{m}_1 \cdots \mathfrak{m}_t$ is not contained in $\mathfrak{m}$. It follows that $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t \cap \mathfrak{m}$ is strictly smaller than $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t$. Since the F-dimension of A is finite, this process must eventually stop. This shows that A admits only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ say. Since all prime ideals of A are maximal, Lemma 3.1. implies that the product $\mathfrak{m}_1, \cdots, \mathfrak{m}_t$ is nilpotent. Let $n \geq 1$ be an exponent for which $(\mathfrak{m}_1 \cdots \mathfrak{m}_t)^n = 0$. Since $\mathfrak{m}_1 + \mathfrak{m}_2 \cdots \mathfrak{m}_t = A$, we also have that $\mathfrak{m}_1^n + (\mathfrak{m}_2 \cdots \mathfrak{m}_t)^n = A$. The Chinese Remainder Theorem provides us then with an isomorphism of A-algebras

$$A \cong A/\mathfrak{m}_1^n \times A/(\mathfrak{m}_2 \cdots \mathfrak{m}_t)^n.$$

The F-algebra $A/\mathfrak{m}_1^n$ is local and its maximal ideal $\mathfrak{m}_1/\mathfrak{m}_1^n$ is nilpotent. The result now follows by induction with respect to the F-dimension of A.

Definition. An *étale* R-algebra is an algebra that satisfies any of the conditions of the following theorem.

Theorem 3.4. *Let F be a perfect field and let A be a finite F-algebra. Then the following are equivalent.*

(i) The discriminant $\Delta(A/F)$ is not zero;
(ii) The trace map $A \longrightarrow F$ is non-degenerate;
(iii) A is isomorphic to a product of finite field extensions of F;
(iv) The module of Kähler differentials $\Omega^1_{A/F}$ vanishes;
(v) A is reduced, i.e., its nilradical is zero.

Proof. We write A as a product of local F-algebras A_i with nilpotent maximal ideals $\mathfrak{m}_i$. We show: *(iii)* $\rightarrow$ *(ii)* $\rightarrow$ *(i)* $\rightarrow$*(iii)* and then *(iii)* $\rightarrow$ *(iv)* $\rightarrow$ *(v)* $\rightarrow$*(iii)*.

To show that *(iii)* implies *(ii)*, it suffices to show that the trace map $A_i \longrightarrow F$ is non-degenerate for each of the local factors A_i. Since by assumption, each A_i is a field, it suffices to show that for a finite field extension $F \subset L$, the trace map $L \longrightarrow F$ is not identically zero. Let $x \in L$ and let $f \in F[X]$ denote its characteristic polynomial. Let $n = [L : F]$. The zeroes $\lambda_1 \ldots, \lambda_n$ of $f(T)$ are the eigenvalues, with multiplicities, of the matrix A that corresponds to the of the multiplication by a map. We have the following identity in the power series ring $F[[T]]$:

$$\frac{T^{n-1} f'(1/T)}{T^n f(1/T)} = \sum_{i=1}^{n} \frac{1}{1 - \lambda_i T} = \sum_{k=1}^{\infty} \mathrm{Tr}(A^k) T^k.$$

Suppose that the trace map is zero. Then the right hand side is zero. Since $T^n f(1/T)$ is a unit in the ring $F[[T]]$, it follows that $f'(T) = 0$. When we take for $x \in L$ a *primitive* element, the polynomial f is equal to the minimum polynomial of x. Since F is perfect, this contradicts the fact that $f' = 0$..

To show that *(ii)* implies *(i)*, we let $\omega_1, \ldots, \omega_n$ denote an F-basis of A. If the discriminant of A is zero, there is a non-trivial F-linear relation between the columns of the matrix $(\mathrm{Tr}(\omega_i \omega_j))_{ij}$. This implies that there is an F-linear combination $a = \lambda_1 \omega_1 + \ldots + \lambda_n \omega_n$ of the ω_i that is not zero, but has the property that $\mathrm{Tr}(ab) = 0$ for all $b \in A$ as required.

To see that *(i)* implies *(iii)*, we assume that A is not a product of fields. Then there is a non-zero nilpotent element $a \in A$, which we can take as an element in an F-basis of A. Since mutiples of a are also nilpotent and nilpotent elements have trace zero, this leads to a zero column in the matrix $(\mathrm{Tr}(\omega_i \omega_j))_{ij}$ and hence $\Delta(A/F) = 0$.

To show that *(iii)* implies *(iv)* it suffices to prove that $\Omega^1_{L/F} = 0$ when $F \subset L$ is a finite field extension. Since F is perfect, $L \cong F[X]/(\varphi(X)$ for some irreducible polynomial $\varphi(X)$. The Kähler differentials are then equal to $K[X]/(\varphi, \varphi')$ which vanishes, because φ has no double zeroes.

To show that *(iv)* implies *(v)*, we assume that A is not reduced and show that $\Omega^1_{A/F}$ does not vanish. Since for any surjective F-algebra homomorphism $A \twoheadrightarrow B$ the natural map $\Omega^1_{A/F} \longrightarrow \Omega^1_{B/F}$ is also surjective, it suffices to construct a suitable quotient algebra B. We first project A on any of its local factors A_i that contains non-zero nilpotent elements. Then we take the quotient by $\mathfrak{m}_i^2$. The maximal ideal $\mathfrak{m}$ of the resulting local F-algebra B

satisfies $\mathfrak{m}^2 = 0$. Let $L = A/\mathfrak{m}$ be the residue field of A'. Since F is perfect, we have that $L = K(x)$ for some primitive element $x \in L$. Let $f \in K[X]$ denote the minimum polynomial of x. Let $a \in B$ be some lift of x to B. Then $f(a) \equiv 0 \pmod{\mathfrak{m}}$ and $f'(a) \not\equiv \pmod{\mathfrak{m}}$. Let $a' = a - f(a)/f'(a)$. Since $\mathfrak{m}^2 = 0$, we have that $f(a)^2 = 0$ and hence that

$$f(a') = f\left(a - \frac{f(a)}{f'(a)}\right) = f(a) - \frac{f(a)}{f'(a)} f'(a) = 0.$$

It follows that the natural map from B to its residue field L admits a section and hence that B is isomorphic to the F-algebra $L[X_1, \ldots, X_m]/J$ for a certain ideal J satisfying $(X_1, \ldots, X_m)^2 \subset J \subset (X_1, \ldots, X_m)$. It follows that

$$\Omega^1_{B/F} = \bigoplus_{i=1}^{n} B dX_i / \langle dg : g \in J \rangle \cong \bigoplus_{i=1}^{n} L dX_i / \langle \sum_{i=1}^{n} \frac{\partial g}{\partial X_i}(0) dX_i : g \in J \rangle \cong (X_1, \ldots, X_n)/J.$$

Since J is strictly contained in the ideal $(X_1, \ldots, X_n)$, this does not vanish and we are done.

Finally, the fact that that *(v)* implies *(iii)* follows at once from the fact that A is isomorphic to a product of local F-algebras with nilpotent maximal ideals.

Exercises.

3.1 Let $\alpha = \zeta_5 + \zeta_5^{-1} \in \mathbf{Q}(\zeta_5)$ where ζ_5 denotes a primitive 5th root of unity. Calculate the characteristic polynomial of $\alpha \in \mathbf{Q}(\zeta_5)$.

3.2 Let F be a number field of degree n and let $x \in F$. Show that for $q \in \mathbf{Q} \subset F$ one has that

$$\begin{aligned} \mathrm{Tr}(qx) &= q\mathrm{Tr}(x), \\ \mathrm{Tr}(q) &= nq, \\ \mathrm{N}(q) &= q^n. \end{aligned}$$

Show that the map $\mathrm{Tr} : F \longrightarrow \mathbf{Q}$ is surjective. Show that the norm $\mathrm{N} : F^* \longrightarrow \mathbf{Q}^*$ is, in general, not surjective.

3.3 Let α be a zero of the polynomial $X^3 - X + 1$. Put $A = \mathbf{Z}[\alpha]$. Show that $\Delta(A/\mathbf{Z}) = -23$.

3.4 Let $1 \neq d \in \mathbf{Z}$ be squarefree and put $F = \mathbf{Q}(\sqrt{d})$. Show that

$$O_F = \begin{cases} \mathbf{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod 4; \\ \mathbf{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

3.5 Let F be a number field of degree n and let $\alpha \in F$. Show that for $q \in \mathbf{Q}$ one has that $N(q - \alpha) = f^{\alpha}_{\mathrm{char}}(q)$. Show that for $q, r \in \mathbf{Q}$ one has that $N(q - r\alpha) = r^n f^{\alpha}_{\mathrm{char}}(q/r)$.

3.6 Let A be a finite algebra over a field F. Suppose that A is a field. Show that for every $a \in A$, the characteristic polynomial $f^{a}_{\mathrm{char}} \in F[X]$ is a power of the minimal polynomial of a.

3.7 Let A and B be finite free R-algebras.

(i) Show that $A \times B$ is also a finite free R-algebra.

(ii) Show that $\Delta((A \times B)/R) = \Delta(A/R)\Delta(B/R)$.

(iii) Show that the characteristic polynomial of $(a, b) \in A \times B$ is equal to the product of the characteristic polynomials of $a \in A$ and $b \in B$.

3.8 Prove that $\mathrm{Disc}(T^n - a) = n^n a^{n-1}$. Compute $\mathrm{Disc}(T^2 + bT + c)$ and $\mathrm{Disc}(T^3 + bT + c)$.

3.9 (*Newton's formulas*) Let K be a field and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. We define the *symmetric functions* s_k of the α_i by

$$\prod_{i=1}^{n}(T - \alpha_i) = T^n - s_1 T^{n-1} + s_2 T^{n-2} + \ldots + (-1)^n s_n.$$

We extend the definition by putting $s_k = 0$ whenever $k > n$. We define the *power sums* p_k by

$$p_k = \sum_{i=1}^{n} \alpha_i^k \qquad \text{for } k \geq 0.$$

Show that for every $k \geq 1$ one has that

$$(-1)^k k s_k = p_k - p_{k-1}s_1 + p_{k-2}s_2 - p_{k-3}s_3 + \ldots.$$

In particular

$$\begin{aligned} s_1 &= p_1 \\ -2s_2 &= p_2 - p_1 s_1 \\ 3s_3 &= p_3 - p_2 s_1 + p_1 s_2 \\ -4s_4 &= p_4 - p_3 s_1 + p_2 s_2 - p_1 s_3 \\ 5s_5 &= \ldots \end{aligned}$$

(Hint: Take the logarithmic derivative of $\prod_{i=1}^{n}(1 - \alpha_i T)$.)

3.10 Let $f(X) \in \mathbf{Z}[X]$ be an irreducible polynomial of degree n and let $F = \mathbf{Q}(\alpha)$. Show that

$$\Delta(\mathbf{Z}[\alpha]/\mathbf{Z}) = \det((p_{i+j-2})_{1 \leq i,j \leq n}).$$

Here p_k denotes the power sum $\alpha_1^k + \ldots + \alpha_n^k$ of the zeroes $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are the zeroes of $f(X)$.

3.10 Show that the polynomial $T^5 + T^3 - 2T + 1 \in \mathbf{Z}[T]$ is irreducible. Compute its discriminant.

4. Lattices.

In this section we discuss the basic properties of lattices.

Definition. A (*Euclidean*) *lattice* is a free abelian group L of finite rank together with a scalar product $\langle -, - \rangle$ on the vector space $\mathbf{R} \otimes_{\mathbf{Z}} L$. Two lattices L and L' are called *isometric* if there is a $\mathbf{Z}$-linear bijection $A : L \longrightarrow L'$ compatible with the scalar products: $\langle A(\mathbf{v}), A(\mathbf{w}) \rangle' = \langle \mathbf{v}, \mathbf{w} \rangle$ for all $\mathbf{v}, \mathbf{w} \in L$.

Here all scalar products are supposed to be positive definite. Since for every scalar product the underlying vector space admits an orthonormal basis, every lattice is isomorphic to a lattice of the form

$$L = \mathbf{Z} \begin{pmatrix} a_{11} \\ \vdots \\ a_{1n} \end{pmatrix} + \ldots + \mathbf{Z} \begin{pmatrix} a_{n1} \\ \vdots \\ a_{nn} \end{pmatrix}$$

equipped with the usual scalar product on $\mathbf{R}^n$. It follows that the lattices of rank n are parametrized by the points of the symmetric space $\mathrm{GL}_2(\mathbf{R})/\mathrm{O}_n(\mathbf{R})$. For example, for $n = 1$ this is $\mathbf{R}^*/\{\pm 1\} \cong \mathbf{R}^*_{>0}$ with $t \in \mathbf{R}^*_{>0}$ corresponding to the lattice $t\mathbf{Z} \subset \mathbf{R}$.

Definition. The *covolume* $\mathrm{covol}(L)$ of a lattice L is the volume of V/L. Here $V = L \otimes_{\mathbf{Z}} \mathbf{R}$. Alternatively, it is the volume of a fundamental domain: if $L = \oplus_{i=1}^n \mathbf{Z}\mathbf{e}_i$, then $\mathrm{covol}(L) = \mathrm{vol}\,(\oplus_{i=1}^n [0,1]\mathbf{e}_i)$.

The covolume of a lattice $L \subset \mathbf{R}^n$ of the form

$$L = \mathbf{Z} \begin{pmatrix} a_{11} \\ \vdots \\ a_{1n} \end{pmatrix} + \ldots + \mathbf{Z} \begin{pmatrix} a_{n1} \\ \vdots \\ a_{nn} \end{pmatrix}$$

is equal to the absolute value of $\det(a_{ij})$. Here $\mathbf{R}^n$ is equipped with its usual scalar product.

Proposition 4.1. *Let V be a real vector space equipped with scalar product and let $L \subset V$ be an additive subgroup. The following are equivalent:*

(i) L is a lattice;
(ii) L is discrete and cocompact;
(iii) L contains a basis of V and $L \subset B$ is finite for every bounded subset $B \subset V$.

Proof. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be a $\mathbf{Z}$-basis of L. Since for every $x \in L$, the intersection of L and the open set $\oplus_{i=1}^n (-1/2, 1/2)\mathbf{e}_i$ is equal to $\{x\}$, the group L is discrete. The canonical map $\oplus_{i=1}^n [0,1]\mathbf{e}_i \twoheadrightarrow V/L$ is continuous and surjective. This shows that V/L is compact. This shows that *(i)* implies *(ii)*. To see that *(ii)* implies *(iii)*, let W be the subspace of V generated by L. Then there is a continuous surjective map $V/L \twoheadrightarrow V/W$. This shows that the vector space V/W is compact. Therefore it is zero and L contains a basis. If for some bounded set B, the intersection $B \cap L$ were infinite, then L would not be discrete.

Finally we show that *(iii)* implies *(i)*. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n \in L$ be a basis of V. The intersection of the L with the bounded set $B = \oplus_{i=1}^n [0,1]\mathbf{e}_i$ is finite. Then L is a finite union:

$$L \quad = \quad \bigcup_{x \in B \cap L} (x + \oplus_{i=1}^n \mathbf{Z}\mathbf{e}_i)$$

It follows that the index $m = [L : \oplus_{i=1} \mathbf{Z}\mathbf{e}_i]$ is finite. This implies that $mL \subset \oplus_{i=1} \mathbf{Z}\mathbf{e}_i$. Therefore L, being a subgroup of finite index of a free group of rank n, is itself free of rank n as required. This follows from Cor. 2.12 applied to the principal ideal domain $\mathbf{Z}$.

Theorem 4.2. *(Minkowski's Convex Body Theorem) Let L be a lattice and let $B \subset V = L \otimes_{\mathbf{Z}} \mathbf{R}$ be a bounded symmetric convex set containing 0. If the volume of B exceeds $2^n \mathrm{covol}(L)$, then there is a non-zero vector in $B \cap L$.*

Proof. Consider the combined map

$$B \quad \hookrightarrow \quad V \quad \twoheadrightarrow \quad V/2L.$$

It preserves distances. Since $\mathrm{vol}(B)$ is strictly larger than $\mathrm{vol}(V/2L) = 2^n \mathrm{covol}(L)$, the map cannot be injective. There are therefore two distinct elements $b_1, b_2 \in B$ that map to the same element in $V/2L$. In other words, $x = \frac{1}{2}(b_1 + (-b_2)) \in L$. Since $b_1 \neq b_2$, the vector x is not zero. Since B is symmetric, the vector $-b_2$ is contained in B and since B is convex, it contains x. Therefore x is a non-zero vector contained in $B \cap L$. This proves the theorem.

Definition. Let L be a lattice and put $V = L \otimes_{\mathbf{Z}} \mathbf{R}$. The *dual* or $\mathbf{Z}$*-dual* $L^\vee$ of L is given by

$$L^\vee = \{v \in V : \ \langle v, w \rangle \in \mathbf{Z} \text{ for all } w \in L\}.$$

When $V = \mathbf{R}^n$ and L is generated by the columns of an invertible matrix (a_{ij}) as above, then the functionals $f_i : L \longrightarrow \mathbf{Z}$ defined by $f_i(\mathbf{w}) = \langle \mathbf{b}_i, w \rangle$ where $\mathbf{b}_i$ denotes the i-th row of the inverse of the matrix(a_{ij}) are clearly a $\mathbf{Z}$-basis for $\mathrm{Hom}(L, \mathbf{Z})$. This shows that $L^\vee$ is the lattice generated by the *columns* of the matrix ${}^t(a_{ij})^{-1}$ in $\mathbf{R}^n$. The covolume of $L^\vee$ is equal to the absolute value of the determinant of the matrix ${}^t(a_{ij})^{-1}$, which in turn is equal to $\mathrm{covol}(L)^{-1}$.

Theorem 4.3. *(Poisson summation formula) Let L be a lattice and let $L^\vee$ denote its $\mathbf{Z}$-dual. Then*

$$\sum_{x \in L} e^{-\pi \|x\|^2} \quad = \quad \frac{1}{\mathrm{covol}(L)} \sum_{x \in L^\vee} e^{-\pi \|x\|^2}.$$

In order to prove this theorem, we consider the *Schwartz* space of rapidly decreasing functions.

$$\mathcal{S} = \{f : \mathbf{R}^n \longrightarrow \mathbf{C} : \begin{array}{l}\text{for every polynomial } g \in \mathbf{C}[X_1, \ldots, X_n] \text{ and every (higher)} \\ \text{partial derivative } \partial f \text{ of } f, \text{ the function } g \cdot \partial f \text{ is bounded}\end{array}\}$$

The *Fourier transform* $\hat{f}$ of a function $f \in \mathcal{S}$ is defined by

$$\hat{f}(x) = \int_{\mathbf{R}^n} f(t) e^{-2\pi i \langle x, t \rangle} dt.$$

Here $x = (x_1, \ldots, x_n)$ and $t = (t_1, \ldots, t_n)$. Similarly 'dt' indicates $dt_1 \cdots dt_n$.

Lemma 4.4. *If $f \in \mathcal{S}$ then also $\hat{f} \in \mathcal{S}$.*

Proof. Let $f \in \mathcal{S}$. Then it satisfies

$$f(x_1, \ldots, x_n) \leq \frac{C}{(1+x_1^2)\cdots(1+x_n^2)}$$

for some constant C that depends on f. Therefore $|\hat{f}| \leq \int_{\mathbf{R}^n} |f| dx_1 \ldots dx_n$ is bounded. We need to show that not only $\hat{f}$, but that any function $g \cdot \partial \hat{f}$ with $g \in \mathbf{C}[X_1, \ldots, X_n]$ and any (high) partial derivative of f is bounded.

We have that

$$\frac{\partial \hat{f}}{\partial x_1} = \int_{\mathbf{R}^n} f(t) e^{-2\pi i x \cdot t} dt = \int_{\mathbf{R}^n} (-2\pi i t_1) f(t) e^{-2\pi i x \cdot t} dt.$$

Since the function $(-2\pi i t_1) f(t)$ is contained in $\mathcal{S}$, the integral is bounded. It follows inductively that all higher derivatives of $\hat{f}$ are contained in $\mathcal{S}$. In a similar way, integrating by parts gives that

$$\int_{\mathbf{R}^n} \frac{\partial f}{\partial t_1} e^{-2\pi i x \cdot t} dt = 0 - \int_{\mathbf{R}^n} f \cdot (-2\pi i x_1) e^{-2\pi i x \cdot t} dt = 2\pi i x_1 f.$$

This shows that $x_1 \hat{f} \in \mathcal{S}$. Similarly and inductively, $g \cdot \hat{f} \in \mathcal{S}$ for every polynomial $g \in \mathbf{C}[X_1, \ldots, X_n]$.

This proves the lemma.

Lemma 4.5. *The function $\mathbf{R}^n \longrightarrow \mathbf{C}$ given by $x \mapsto e^{-\pi \|x\|^2}$ has a Fourier transform equal to itself.*

Proof. We want to show that

$$\int_{\mathbf{R}^n} e^{-2\pi i \langle x, t \rangle} e^{-\pi \|t\|^2} dt = e^{-\pi \|x\|^2}.$$

Proof. Since both sides can be written as products of expressions that depend only on one variable, it suffices to deal with the case of one variable: we need to show that

$$\int_{-\infty}^{\infty} e^{-2\pi i x t - \pi t^2} dt = e^{-\pi x^2}.$$

We integrate the function $e^{-\pi z^2}$ of a complex variable z over the contour in $\mathbf{C}$ given by $-A \to A \to A + ix \to -A + ix \to -A$ and let A tend to infinity. The integrals over the vertical segments tend to zero. The integral from $-A$ to A tends to $\int_{-\infty}^{\infty} e^{-\pi t^2} dt = 1$. Therefore the integral from $A + ix$ to $-A + ix$ tends to

$$\int_{-\infty}^{\infty} e^{-(t+ix)^2} dt = 1.$$

This proves the lemma.

Theorem 4.6. *Let f be a function in the Schwartz space $\mathcal{S}$ of rapidly decreasing functions $\mathbf{R}^n \longrightarrow \mathbf{C}$. Then*

$$\sum_{x \in \mathbf{Z}^n} f(x) = \sum_{x \in \mathbf{Z}^n} \hat{f}(x).$$

Proof. Consider the function

$$g(x) = \sum_{m \in \mathbf{Z}^n} f(m + x).$$

Since the sum converges absolutely and uniformly, this is a well-defined function on the torus $\mathbf{T}^n = \mathbf{R}^n/\mathbf{Z}^n$. For $k \in \mathbf{Z}^n$ we define its Fourier coefficient c_k by

$$c_k = \int_{\mathbf{T}^n} g(x) e^{-2\pi i k x} dx.$$

Since for every $d > 0$ there is a constant $C(d, g) > 0$ for which $|c_k| \leq C(g, d)/\|k\|^d$, we have that

$$\left| \sum_{\|k\| > N} c_k e^{2\pi i k x} \right| \leq C(d, g) \sum_{\|k\| > N} \frac{1}{\|k\|^d} = O(\frac{1}{N^{d-1}}),$$

and we conclude that the Fourier series $\sum_{k \in \mathbf{Z}^n} c_k e^{2\pi i k x}$ converges uniformly and hence pointwise to $g(x)$. In particular,

$$\sum_{m \in \mathbf{Z}^n} f(m) = g(0) = \sum_{k \in \mathbf{Z}^n} c_k.$$

Moreover,

$$\begin{aligned} c_k &= \int_{\mathbf{T}^n} \sum_{m \in \mathbf{Z}^n} f(m + x) e^{-2\pi i \langle k, x \rangle} dx, \\ &= \int_{\mathbf{T}^n} \sum_{m \in \mathbf{Z}^n} f(m + x) e^{-2\pi i \langle k, x + m \rangle} dx, \\ &= \int_{\mathbf{R}^n} f(x) e^{-2\pi i \langle k, x \rangle} dx, \\ &= \hat{f}(k). \end{aligned}$$

This proves the theorem.

Proof of Theorem 4.3. We may assume that $V = L \otimes_{\mathbf{Z}} \mathbf{R}$ is just $\mathbf{R}^n$ with its usual scalar product and that $L = A(\mathbf{Z})$ for some matrix $A \in \mathrm{GL}_n(\mathbf{R})$. In this way the $\mathbf{Z}$-dual lattice $L^\vee$ is equal to ${}^tA^{-1}(\mathbf{Z})$. The left hand side of the Poisson summation formula is equal to

$$\sum_{x \in L} e^{-\pi \|x\|^2} = \sum_{k \in \mathbf{Z}^n} e^{-\pi \|A(x)\|^2}.$$

The function $f(x) = e^{-\pi\|A(x)\|^2}$ is in the Schwartz space $\mathcal{S}$ and by Lemma 4.5 its Fourier transform is equal to

$$\begin{aligned}\hat{f}(t) &= \int_\infty^\infty e^{-2\pi i\langle x,t\rangle} e^{-\pi\|A(x)\|^2} dx,\\ &= \frac{1}{|\det(A)|}\int_\infty^\infty e^{-2\pi i\langle A^{-1}(x),t\rangle} e^{-\pi\|x\|^2} dx,\\ &= \frac{1}{|\det(A)|}\int_\infty^\infty e^{-2\pi i\langle x,{}^tA^{-1}(t)\rangle} e^{-\pi\|x\|^2} dx,\\ &= \frac{1}{|\det(A)|} e^{-\pi\|{}^tA^{-1}(x)\|^2}.\end{aligned}$$

It follows that

$$\sum_{k\in\mathbf{Z}^n} e^{-\pi\|A(x)\|^2} = \frac{1}{|\det(A)|}\sum_{x\in L^\vee} e^{-\pi\|x\|^2}$$

and the result follows.

Exercises.

4.1 Let $L' \subset L$ be two lattices in $\mathbf{R}^n$. Show that $\mathrm{covol}(L) = [L : L']\mathrm{covol}(L)$.

4.2 Let

$$L = \{\begin{pmatrix} x\\ y\\ z\end{pmatrix} \in \mathbf{Z}^3 : x + y + z \equiv 0 \pmod 7\}.$$

Show that $L \subset \mathbf{R}^3$ is a lattice and compute its covolume.

4.3 Let $L \subset \mathbf{R}^n$ be a lattice. Let A be an invertible $n \times n$-matrix. Show that $A(L)$ is a lattice. Show that $\mathrm{covol}(A(L)) = |\det(A)|\mathrm{covol}(L)$. Let $m \in \mathbf{R}_{>0}$; show that $\mathrm{covol}(mL) = m^n\mathrm{covol}(L)$.

4.4 Identify the quaternions $\mathbf{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbf{R}\}$ with $\mathbf{R}^4$ via $a + bi + cj + dk \leftrightarrow (a, b, c, d)$. What is the covolume of the ring of Hurwitz integers

$$\mathbf{Z}[i, j, k, \frac{1 + i + j + k}{2}]$$

in $\mathbf{H} \cong \mathbf{R}^4$?

4.5 Let F be a number field. Suppose $R \subset F$ is a subring with the property that its image in $F \otimes \mathbf{R}$ is a lattice. Show that $R \subset O_F$.

4.6 *(Euclidean complex quadratic rings.)* Let F be an imaginary quadratic number field. We embed F in $\mathbf{C}$.

(i) Show that O_F is Euclidean for the norm if and only if the disks with radius 1 and centers in O_F cover $\mathbf{C}$.

(ii) Show that O_F is Euclidean for the norm if and only if $\Delta_F = -3, -4, -7, -8$ or -11.

4.7 Show that the symmetric space is $\mathrm{GL}_2(\mathbf{R})/O_2(\mathbf{R})$ homeomorphic to $\mathbf{R}^*_{>0} \times \mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R})$. Show that the map $\mathrm{SL}_2(\mathbf{R})/\mathrm{SO}_2(\mathbf{R}) \longrightarrow \mathbf{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$ given by

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix} \quad \mapsto \quad \frac{ai + b}{ci + d}$$

is a homeomorphism.

5. Number fields.

In this section we 'generalize' the three rings $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$ to an arbitrary number field F.

Definition. Let F be a number field of degree n over $\mathbf{Q}$. The algebra $F_{\mathbf{R}}$ is defined by

$$F_{\mathbf{R}} = F \otimes_{\mathbf{Q}} \mathbf{R}.$$

In more explicit terms, writing $F = \mathbf{Q}(\alpha)$ with $f(X) \in \mathbf{Q}[X]$ the minimum polynomial of α, we have that $F = \mathbf{Q}[X]/(f(X))$ and hence that $F_{\mathbf{R}} = \mathbf{R}[X]/(f(X))$.

Since irreducible polynomials in $\mathbf{Q}[X]$ don't have double zeroes, the Chinese Remainder theorem implies that the $\mathbf{R}$-algebra is isomorphic to a product of copies of $\mathbf{R}$ and $\mathbf{C}$. In these terms the natural map $F \longrightarrow F_{\mathbf{R}}$ can be described as follows. Since a field homomorphism $\sigma : F \longrightarrow \mathbf{C}$ is entirely determined by the zero z in $\mathbf{C}$ of $f(X)$ for which $\sigma(\alpha) = z$, there are exactly n distinct embeddings

$$\sigma : F \longrightarrow \mathbf{C}.$$

Since $f(X) \in \mathbf{R}[X]$, the ring homomorphism $\overline{\sigma}$ given by $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ is an embedding, whenever σ is. If $z = \sigma(\alpha) \in \mathbf{R}$, we have that $\overline{\sigma} = \sigma$. The σ corresponding to $z \notin \mathbf{R}$ come in complex conjugate pairs.

Definition. An *infinite prime* of a number field F is an embedding $\sigma : F \hookrightarrow \mathbf{C}$ considered up to complex conjugation. An infinite prime σ is called *real* if $\sigma(F) \subset \mathbf{R}$ and *complex* if $\sigma(F) \not\subset \mathbf{R}$. The number of real and complex infinite primes is denoted by r_1 and r_2 respectively.

We have that $r_1 + 2r_2 = n = [F : \mathbf{Q}]$. The $\mathbf{R}$-algebra morphism

$$F_{\mathbf{R}} = \mathbf{R}[X]/(f(X)) \quad \stackrel{\cong}{\longrightarrow} \prod_{\sigma} F_{\sigma}$$

given by mapping $X \mapsto (\sigma(\alpha))$ is an isomorphism. Here F_{σ} denotes $\mathbf{R}$ or $\mathbf{C}$ depending on whether σ is real or complex. The product runs over the infinite primes $\sigma : F \hookrightarrow \mathbf{C}$.

Lemma 5.1. *Let F be a number field and let $x \in F$. Then*

$$f^x_{\mathrm{char}}(T) = \prod_{\text{all } \sigma} (T - \sigma(x))$$

and hence $N(x) = \prod_{\text{all } \sigma} \sigma(x)$ and $\mathrm{Tr}(x) = \sum_{\text{all } \sigma} \sigma(x)$. Here "all σ" means that the sum is extended over all embeddings $F \hookrightarrow \mathbf{C}$, not merely up to complex conjugation. In terms of infinite primes σ one has that $N(x) = \prod_{\sigma} \sigma(x)^{\deg(\sigma)}$ and that $\mathrm{Tr}(x) = \sum_{\sigma} \deg(\sigma)\sigma(x)$

Proof. The characteristic polynomial of x viewed as element of the $\mathbf{Q}$-algebra F is the same as the one of x viewed as element of the $\mathbf{R}$-algebra $F_{\mathbf{R}}$. We compute the characteristic polynomial by writing $F_{\mathbf{R}}$ as a product of copies of $\mathbf{R}$ and $\mathbf{C}$. In this way the element $x \in F$ is identified with the vector $(\sigma(x))$ where σ runs over the embeddings $\sigma : F \hookrightarrow \mathbf{C}$ up to

complex conjugation. Since the characteristic polynomial of x is equal to the product of the characteristic polynomials of the various $\sigma(x)$, we may proceed coordinate by coordinate. For the real coordinates the characteristic polynomial is simply $T - \sigma(x)$. For complex coordinates, we use the $\mathbf{R}$-basis $\{1, i\}$ of $\mathbf{C}$ and it is the characteristic polynomial of the 2-by-2 matrix

$$\begin{pmatrix} \operatorname{Re}\sigma(x) & -\operatorname{Im}\sigma(x) \\ \operatorname{Im}\sigma(x) & \operatorname{Re}\sigma(x) \end{pmatrix},$$

which is $(T - \sigma(x))(T - \overline{\sigma(x)})$. Taking the product now gives the result.

Definition. Any étale $\mathbf{R}$-algebra A admits a *canonical involution* and a canonical scalar product as follows. Writing A as a product of copies of $\mathbf{R}$ and $\mathbf{C}$, the involution is given by complex conjugation on each coordinate. This involution is functorial. It is a functor on the category of étale $\mathbf{R}$-algebras. We denote it by $a \mapsto \overline{a}$ and in terms of it we define a scalar product by

$$\langle a, b \rangle = \operatorname{Tr}(a\overline{b}), \qquad \text{for } a, b \in A.$$

Definition. Let F be a number field. Its *ring of integers* O_F is the integral closure of $\mathbf{Z}$ in F:

$$O_F = \{x \in F : x \text{ is integral over } \mathbf{Z}\}.$$

By Cor. 1.9 the ring O_F is a subring of F. We view it as a subring of the algebra $F_{\mathbf{R}}$ through the natural map $F \longrightarrow F_{\mathbf{R}}$.

Definition. Let F be a number field. The *discriminant* Δ_F of F is the discriminant $\Delta(O_F)$ of the $\mathbf{Z}$-algebra O_F.

Lemma 5.2. *Let F be a number field. Let $x \in F$. The following are equaivalent.*
(i) the element x is contained in O_F;
(ii) the minimum polynomial of x is in $\mathbf{Z}[X]$;
(iii) the characteristic polynomial of x is in $\mathbf{Z}[X]$.

Proof. Gauss's Lemma (Prop. 2.13 with $R = \mathbf{Z}$) shows that *(i)* implies *(ii)*. Part *(iii)* follows from *(ii)* because f^x_{char} is a power of f^x_{min} by Exer. 3.2. Finally, it is trivial that *(iii)* implies *(i)*.

Proposition 5.3. *The ring O_F is a lattice in $F_{\mathbf{R}}$. Its covolume is equal to $\sqrt{|\Delta_F|}$.*

Proof. Suppose $\omega_1, \ldots, \omega_n$ is a basis for F as a $\mathbf{Q}$-vector space. Then it is also a basis for $F_{\mathbf{R}}$ as a $\mathbf{R}$-vector space. Multiplying the ω_i by a large integer M does not change these properties. However, we can choose M in such a way that all $M\omega_i$ are integral. This shows that O_F contains an $\mathbf{R}$-basis for $F_{\mathbf{R}}$.

Let $\mu > 0$ and consider the bounded subset $B = \{x \in F_{\mathbf{R}} : \|x\| < \mu\}$ of $F_{\mathbf{R}}$. Suppose that x is contained in $O_F \cap B$. Then $\operatorname{Tr}(x\overline{x}) < \mu^2$ and hence $\sigma(x) < \mu$ for every embedding $\sigma : F \hookrightarrow \mathbf{C}$. It follows then from Lemma 5.1 that the coefficients of the characteristic polynomial of x are bounded by $\binom{2n}{n}\mu^n$. By Lemma 5.2 all these coefficients are in $\mathbf{Z}$. Therefore there are only finitely many possibilities for f^x_{char} and hence for x. It follows that $O_F \cap B$ is finite.

The criterion of Prop. 4.1 implies then that O_F is a lattice in $F_{\mathbf{R}}$. Its covolume is the absolute value of the discriminant of the matrix

Corollary 5.4. *Let F be a number field of degree n. Then there are elements $\omega_1, \ldots, \omega_n \in F$ so that*

$$\begin{array}{rl} O_F & = \mathbf{Z}\omega_1 \oplus \cdots \oplus \mathbf{Z}\omega_n, \\ \subset\big\downarrow & \\ F & = \mathbf{Q}\omega_1 \oplus \cdots \oplus \mathbf{Q}\omega_n, \\ \subset\big\downarrow & \\ F_{\mathbf{R}} & = \mathbf{R}\omega_1 \oplus \cdots \oplus \mathbf{R}\omega_n. \end{array}$$

Definition. *Let F be a number field and let $I \subset O_F$ be a non-zero ideal. The norm $N(I)$ of I is defined as $N(I) = [O_F : I]$.*

The following proposition shows that $N(I)$ is a well defined natural number.

Proposition 5.5. *Let F be a number field. Then*
(i) for any non-zero ideal $I \subset O_F$ the index of I in O_F is finite;
(ii) any non-zero ideal $I \subset O_F$ is a lattice in $F_{\mathbf{R}}$. Its covolume is given by

$$\mathrm{covol}(I) = N(I)|\Delta_F|^{1/2}.$$

(iii) There are only finitely many O_F-ideals $I \subset O_F$ of bounded norm.

Proof. *(i)* Let $0 \neq x \in I$. Then the constant term a_0 of its minimum polynomial f is not zero. It is contained in I because $a_0 = a_0 - f(x)$ is a multiple of x. Therefore $a_0 O_F \subset I$. Since $O_F/a_0O_F \cong \mathbf{Z}/(a_0) \times \ldots \times \mathbf{Z}/(a_0)$ is finite, so is O_F/I.
(ii) Since $I \subset O_F$, it is a discrete subgroup of $F_{\mathbf{R}}$. Since I contains a group of the form a_0O_F, it contains an F-basis. It follows that $I \subset F_{\mathbf{R}}$ is a lattice. By Exercise 4.2 its covolume is equal to covolume(O_F) times $[O_F : I]$. The result now follows from Prop. 5.3.
(iii) Any ideal $I \subset O_F$ of index m contains mO_F. Since O_F/mO_F is a finite group, there are only finitely many ideals of index m.

This proves the proposition

Theorem 5.6. *Let F be a number field. Then the ring of integers O_F is a Dedekind ring.*

Proof. Since $\mathbf{Z}$ is Noetherian and since O_F is a free abelian group of rank n, any ideal $I \subset O_F$ is finitely generated group. So it is certainly also finitely generted as an O_F-module. Therefore O_F is Noetherian. Any non-zero prime ideal of O_F has finite index. Therefore it is maximal. This shows that the Krull dimension of O_F is 1. Finally, O_F is the integral closure of $\mathbf{Z}$ in F. By Exerc.1.5 it is therefore a normal ring.

This proves the theorem.

Proposition 5.7. *Let F be a number field.*
(i) For any non-zero $x \in O_F$ we have that $|N(x)| = N((x))$;
(ii) $N(IJ) = N(I)N(J)$ for any two non-zero ideals $I, J \subset O_F$.

Proof. *(i)* We prove that $|N(x)|N(I) = N(xI)$ for any non-zero O_F-ideal I. Let $\omega_1, \ldots, \omega_n$ be a $\mathbf{Z}$-basis for O_F, let $\sum_j b_{ij}\omega_j$ (for $i = 1, \ldots, n$) be a $\mathbf{Z}$-basis for I and let A be the matrix of the multiplication my x map with respect to the basis $\omega_1, \ldots, \omega_n$. Then $N(I) = |\det(A)|$ and $N(xI) = |\det(AB)|$. Since $N(x) = \det(A)$, the result follows.
(ii) We use the fact that O_F is a Dedekind ring. By the proof of Prop. 2.6, there are non-zero $x, y \in O_F$ and there is an ideal $J' \subset O_F$ that is *coprime to* I so that $xJ = yJ'$. By the Chinese Remainder Theorem we have that $O_F/IJ' \cong (O_F/I) \times (O_F/J')$ so that $N(IJ') = N(I)N(J')$. Therefore

$$\begin{aligned} |N(x)|N(IJ) = N(xIJ) = N(yIJ') = |N(y)|N(I)N(J') = \\ = N(I)N(yJ') = N(I)N(xJ) = |N(x)|N(I)N(J), \end{aligned}$$

as required.

Exercises.

5.1 Let F be a number field.
(i) Let $\alpha \in F$. Show that there exist an integer $0 \neq m \in \mathbf{Z}$ such that $m\alpha \in O_F$.
(ii) Show that for every number field F there exists an *integral* element $\alpha \in O_F$ such that $F = \mathbf{Q}(\alpha)$.
(iii) Show that the field of fractions of O_F is F.
(iv) Let $F \subset K$ be an extension of number fields. Show that $O_K \cap F = O_F$.

5.2 Let F be a number field. Show that every ideal $I \neq 0$ of O_F contains a non-zero integer $m \in \mathbf{Z}$.

5.3 Let F be a number field and let $\alpha \in O_F$. Show that $N(\alpha) = \pm 1$ if and only if α is a unit of the ring O_F.

5.4 Let F be a number field. Let r_1 and r_2 denote the number of real and complex infinite primes respectively. Show that the sign of Δ_F is $(-1)^{r_2}$.

5.5 Let A be an étale $\mathbf{R}$-algebra. Show that $\mathrm{Tr}(a\bar{b})$ defines a scalar product on A: show that it is symmetric, bilinear and positive definite.

5.6 Let F be a number field. Show that $\overline{L} = \{\overline{x} : x \in L\} \subset F_{\mathbf{R}}$ is a lattice if and only L is. Moreover, L and $\overline{L}$ have the same covolume.

5.7 Let F be a number field.
(i) Show that $\|x\| = \|\overline{x}\|$ for all $x \in F_{\mathbf{R}}$.
(ii) For $x = (x_\sigma) \in F_{\mathbf{R}}$ we let $|x| \in F_{\mathbf{R}}$ the element whose σ-th component is equal to $|x_\sigma|$. Show that $\|x\| = \||x|\|$.
(iii) Let $\varphi : F_{\mathbf{R}} \longrightarrow F_{\mathbf{R}}$ be $F_{\mathbf{R}}$-linear. Show that φ is given by multiplication by some element $x \in F_{\mathbf{R}}$.
(iv) Let $x \in F_{\mathbf{R}}$. Show that the multiplication by x map preserves the canonical scalar product if and only if $|x| = 1$.

5.8*(Stickelberger 1923) Let F be a number field of degree n. Let $\{\omega_1, \omega_2, \ldots, \omega_n\}$ be a $\mathbf{Z}$-basis for the ring of integers of F. Let $\sigma_i : F \hookrightarrow \mathbf{C}$ denote the n distinct embeddings of F into $\mathbf{C}$.

By A_n we denote the normal subgroup of *even* permutations of the symmetric group S_n. We define $\Delta^+ = \sum_{\tau \in A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$ and $\Delta^- = \sum_{\tau \in S_n - A_n} \prod_{i=1}^n \phi_i(\omega_{\tau(i)})$. Prove, using Galois theory, that $\Delta^+ + \Delta^-$ e $\Delta^+\Delta^-$ are in $\mathbf{Z}$. Conclude that $\Delta_F = (\Delta^+ + \Delta^-)^2 - 4\Delta^+\Delta^- \equiv 0$ or $1 \pmod 4$.

6. Rings of integers.

In this section we explain how to compute the ring of integers O_F of a number field F. Once we have a presentation of O_F as a $\mathbf{Z}$-algebra, we show how to compute explicit generators for the prime ideals of O_F.

Suppose that F is a number field F given as $\mathbf{Q}(\alpha)$ for some element $\alpha \in F$. Suppose in addition that $\alpha \in O_F$. This is not a real restriction since $M\alpha$ is integral for an appropriate choice of a non-zero integer M. Since $\mathbf{Z}[\alpha]$ contains a $\mathbf{Q}$-basis for F and is contained in O_F, it is a lattice and has the same rank as O_F. Therefore the index $[O_F : \mathbf{Z}[\alpha]]$ is finite.

Rather than sticking to $\mathbf{Z}[\alpha]$, we consider more generally a subring $R \subset O_F$ of finite index $[O_F : R]$. In the applications, R is explicitly given and we want to either decide that $R = O_F$ or, if it isn't, construct generators for O_F. This is done inductively. The ring R is called *maximal* at a prime number p, if p does *not* divide $[O_F : R]$.

We first make a useful observation.

Lemma 6.1. *Let F be a number field and let R be a subring of O_F of finite index. If R is not maximal at a prime p, then p^2 divides $\Delta(R/\mathbf{Z})$. In particular, if $\Delta(R/\mathbf{Z})$ is square-free, we have that $R = O_F$.*

Proof. The lemma follows from the fact that $\Delta(R/\mathbf{Z}) = [O_F : R]^2 \Delta(O_F/\mathbf{Z})$.

Let R and p be as above and put $N = \{t \in R : t^m \in pR \text{ for some } m \geq 1\}$. Since N is a finitely generated R-ideal, we actually have $N^m \subset pR$ for some m. Consider the following two subrings of O_F:

$$R' = \{t \in O_F : tN \subset N\} \qquad \text{and} \qquad R'' = \{t \in O_F : pt \in R\}.$$

We have $R'' \subset \frac{1}{p}R$. Since p is in N, every $t \in R'$ has the property that pt is in $N \subset R$. It follows that $R \subset R' \subset R'' \subset O_F$.

Proposition 6.2. *In the above notation, if $R = R'$, then $R = R''$.*

Proof. Let $x \in R''$ and let $y \in N$. We claim that $(xy)^{mn} \in pR$ where $n = [F : \mathbf{Q}]$ and m satisfies $N^m \subset pR$. Indeed, we have $y^m \in pR$. It follows that $xy^m \in R$ and hence $y^{m(k+1)}x^k = y^m(xy^m)^k \in pR$ for all $k \geq 0$. Since x is integral, it satisfies a monic relation of the form $x^n + \ldots + a_1 x + a_0 = 0$ with $a_i \in \mathbf{Z} \subset R$. This implies that

$$y^{mn}x^k \in pR, \qquad \text{for } \textit{all } k \geq 1.$$

In particular, we have $(xy)^{mn} \in pR$ as claimed.

To show that $R'' \subset R$, we pick $x \in R''$ and show

$$xN^{k+1} \subset N \quad \Longrightarrow \quad xN^k \subset N \qquad \text{for any } k \geq 1.$$

Since $xN^{m+1} \subset xpN \subset N$, it follows then inductively that $xN \subset N$. Therefore x is in R' which is equal to R by assumption.

So, let $x \in R''$ and suppose that $xN^{k+1} \subset N$ for some $k \geq 1$. Let $y \in N^k$. For any $z \in N$ we have $xyz \in xN^kN \subset N$. This shows that $xyN \subset N$ and hence $xy \in R' = R$. Since we have $(xy)^{nm} \in pR$, this implies $xy \in N$ as required.

This proves the proposition.

Corollary 6.3. *In the notation of Proposition 6.2, we have $R = R'$ if and only if the homomorphism*

$$m : R/pR \quad \longrightarrow \quad \mathrm{End}(N/pN)$$

given by $x \mapsto m_x$, where m_x is the multiplication by x map, is injective. Moreover, if the map is injective, then R is maximal at p. If it isn't, then for any $x \in R$ for which $x \pmod{pR}$ is contained in $\ker h$, we have that

$$R \quad \underset{\neq}{\subset} \quad R[\frac{x}{p}] \quad \subset \quad R' \quad \subset \quad O_F.$$

Proof. Suppose that m is injective and let $x \in R'$. Then $xN \subset N$ and hence $xpN \subset pN$. Since $x \in R' \subset R''$, the element xp is contained in R. It follows that xp is in the kernel of m. Since m is injective, we have that $px = px'$ for some $x' \in R$. It follows that $x = x' \in R$ showing that $R = R'$.

By Proposition 6.2 we have $R = R' = R''$. This implies that $[O_F : R]$ is prime to p, so that R is maximal at p

In the other direction, suppose that $R = R'$ and let $x \in R$ with m_x the zero-map. Then $xN \subset pN$. This implies that $\frac{x}{p}N \subset N$. Since N is finitely generated, this implies that $\frac{x}{p} \in O_F$. By definition, $\frac{x}{p}$ is contained in $R' = R$. In other words, $x = px'$ for some $x' \in R$. This shows that $x \pmod{pR}$ is zero and that m is injective.

This argument also shows that $\frac{x}{p} \in O_F$ for every $x \in R$ in the kernel of m. Therefore the subring $R[\frac{1}{p}]$ of O_F is strictly larger than R, as required

This leads to the following algorithm. Let $F = \mathbf{Q}(\alpha)$ be a number field with $\alpha \in O_F$. We put $R = \mathbf{Z}[\alpha]$ and make a list of the primes p for which p^2 divides $\Delta(R/\mathbf{Z})$. By Lemma 6.1 the ring R is maximal at all other primes. For each prime p in the list we compute the nilradical of the finite ring R/pR and check whether the map m of Cor. 6.3 is injective. This involves only linear algebra over $\mathbf{F}_p$. When m is injective, we know that R is maximal at p and we are done with p. If m is not injective, we pick $x \in R$ with $x \not\equiv 0 \pmod{p}$ but $m(x) = 0$ and replace R by the strictly larger ring $R[\frac{x}{p}]$. If the discriminant of this new ring is not divisible by p^2 we are once again done with p. If not we repeat this procedure.

Since each time the ring R 'becomes' strictly larger, the algorithm terminates. At the end we have $R = O_F$.

Corollary 6.4. *Let $F = \mathbf{Q}(\alpha)$ be a number field and let p be a prime. Suppose that $\alpha \in O_F$ and that the minimum polynomial of α is an Eisenstein polynomial with respect to p. Then p does not divide the index $[O_F : \mathbf{Z}[\alpha]]$*

Proof. Put $R = \mathbf{Z}[\alpha]$. Since the minimum polynomial $f(X)$ of α is Eisenstein, the ring R/pR is isomorphic to $(\mathbf{Z}/p\mathbf{Z})[X]/(X^n)$. Here $n = [F : \mathbf{Q}]$. The ideal N of Prop. 6.2 is therefore equal to $(\alpha, p) \subset R$. We check that the map m of Cor. 6.3 is injective. Let $x \in R$ be in the kernel of m. Then $x = g(\alpha)$ for some polynomial $g(X) \in \mathbf{Z}[X]$ of degree at most $n-1$ and $g(\alpha)N \subset pN$. This implies that

$$g(X)X = p^2 h_1(X) + pXh_2(X) + f(X)h_3(X)$$

for certain polynomials $h_1, h_2, h_3 \in \mathbf{Z}[X]$. Putting $X = 0$, we see that $f(0)h_3(0) \equiv 0 \pmod{p^2}$. Since f is Eisenstein, this implies that p divides $h_3(0)$. Now take the equation modulo p. This leads to the congruence $g(X)X \equiv X^n h_3(X) \pmod{p}$. The degree of the polymonial on the left is at most n while the degree of the polynomial on the right is at least $n+1$. This shows that $g(X) \equiv 0 \pmod{p}$ and hence that $x \in pR$ and that m is injective.

The result now follows from Cor. 6.3.

Example. Consider $F = \mathbf{Q}(\sqrt[3]{17})$ and put $R = \mathbf{Z}[\sqrt[3]{17}]$. Then $R \subset O_F$ has finite index. A $\mathbf{Z}$-basis for R is given by $\{1, \sqrt[3]{17}, (\sqrt[3]{17})^2]\}$ and the discriminant of R is equal to the determinant of the matrix of traces

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3 \cdot 17 \\ 0 & 3 \cdot 17 & 0 \end{pmatrix} = -3^3 \cdot 17^2.$$

Therefore R is maximal at all primes p except possibly $p = 3$ and 17. Since the minimum polynomial $X^3 - 17$ of $\sqrt[3]{17}$ is Eisenstein with respect to the prime 17, Cor. 6.4 implies that R is maximal at 17. In order to study the prime $p = 3$, we compute the nilradical of the ring $R/3R \cong \mathbf{Z}[X]/(X^3 - 17)$. Since $X^3 - 17 \equiv (X+1)^3 \pmod{3}$, the nilradical of $R/3R$ is generated by $X+1$ and the R-ideal N of Cor. 6.3 is equal to $(3, \alpha)$ where $\alpha = \sqrt[3]{17} + 1$. Note that $\alpha^3 - 3\alpha^2 + 3\alpha - 18 = (\alpha - 1)^3 - 17 = 0$

A $\mathbf{Z}$-basis for R is given by $\{1, \alpha, \alpha^2\}$ and a $\mathbf{Z}$-basis for N by $\{3, \alpha, \alpha^2\}$. Next we study kernel of the homomorphism

$$m : R/3R \quad \longrightarrow \quad \mathrm{End}(N/3N)$$

that maps $x \in R$ to the multiplication by x map. Suppose that $a, b, c \in \mathbf{Z}$ and $x = a + b\alpha + c\alpha^2 \in R$. We multiply the three $\mathbf{F}_3$-basis vectors of $N/3N$ by x. We have that $x \cdot 3 = 3a + 3b\alpha + 3c\alpha^2 \equiv a \cdot 3 \pmod{3N}$. Since $\alpha^3 \equiv 0 \pmod{3N}$, we have that $x \cdot \alpha = a \cdot \alpha + b \cdot \alpha^2$ and $x \cdot \alpha^2 = a \cdot \alpha^2$. Therefore the matrix that describes the multplication by x map with respect to the basis $\{3, \alpha, \alpha^2\}$ is given by

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ b & a & 0 \end{pmatrix}.$$

It follows that $\ker(m)$ is a 1-dimensional $\mathbf{F}_3$-vector space generated by α^2. By Corollary 6.3, the ring

$$R' = \mathbf{Z}[\sqrt[3]{17}, \beta], \qquad \text{with} \qquad \beta = \frac{\alpha^2}{3} = \frac{(1 + \sqrt[3]{17})^2}{3},$$

is a subring of O_F strictly containing R. Since $\Delta(R/\mathbf{Z}) = 3^3 \cdot 17^2$, the index satisfies $[R' : R] = 3$ and the discriminant of R' is equal to $3 \cdot 17^2$. It follows that $O_F = R'$.

In the remainder of this section we explain how one can explicitly compute the prime ideals of the ring of integers O_F of a number field F.

By Proposition 5.5 any non-zero prime ideal contains an integer and hence a prime number p. Therefore, fixing a prime number p, the prime ideals containing p correspond exactly the prime ideals of the quotient ring O_F/pO_F. More precisely, the prime ideals $\mathfrak{p}$ dividing p are of the form

$$\mathfrak{p} = \{x \in O_F : x \pmod{p} \in \mathfrak{P}\}, \quad \text{for some prime ideal } \mathfrak{P} \text{ of } R/pR.$$

The ring R/pR is a finite $\mathbf{F}_p$-algebra and therefore it is a product of local $\mathbf{F}_p$-algebras $R/pR \cong \prod_i A_i$, where A_i is local with nilpotent maximal ideal. This is a computation with a finite $\mathbf{F}_p$-algebra that is in practice not very difficult.

It is easy to make this explicit in terms of the prime ideals $\mathfrak{p}$ of O_F that divide p. Indeed, since O_F is a Dedekind ring, the O_F-ideal (p) admits a factorization as a product of prime ideals $(p) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$. Here the product runs over *distinct* prime ideals $\mathfrak{p}$. By the Chinese Remainder Theorem we have then that

$$R/pR \quad \cong \quad \prod_{\mathfrak{p}|p} O_F/\mathfrak{p}^{e_{\mathfrak{p}}}.$$

Each of the factors is a local $\mathbf{F}_p$-algebra with maximal nilpotent ideal $\mathfrak{p}/\mathfrak{p}^{e_{\mathfrak{p}}}$.

Before we give some explicit examples, we introduce some terminology. For a prime ideal $\mathfrak{p}$ oif O_F, the exponent $e_{\mathfrak{p}}$ is called the *inertia index* of $\mathfrak{p}$. Prime ideals $\mathfrak{p}$ for which $e_{\mathfrak{p}}$ exceeds 1 are said to be *ramified*. If $\mathfrak{p}$ contains the prime number p, then the residue field $O_F/\mathfrak{p}$ is a finite field extension of $\mathbf{F}_p$. We denote by $f_{\mathfrak{p}}$ the degree of this extension. We have that $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$. A prime number p is said to be *inert* if the O_F-ideal (p) is a prime ideal of O_F. It is said to be *ramified* if some prime ideal divising it is ramified. A prime number is said to be *totally split* if $(p) = \prod_{\mathfrak{p}} \mathfrak{p}$ and $f_{\mathfrak{p}} = 1$ for every $\mathfrak{p}$.

Proposition 6.5. *Let F be a number field and let p be a prime number. Then*

(i) Denoting by $\mathfrak{p}$ the prime divisors of the O_F-ideal (p), we have that

$$\sum_{\mathfrak{p}|p} f_{\mathfrak{p}} e_{\mathfrak{p}} = n = [F : \mathbf{Q}].$$

(ii) The prime p is ramified if and only if it divides $\Delta(O_F/\mathbf{Z})$. In particular, there are only finitely many ramified primes.

Proof. To prove *(i)*, just take the norm of the relation $(p) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$. To prove part *(ii)*, note that the discriminant of the $\mathbf{F}_p$-algebra $O_F/(p)$ is just $\Delta(O_F/\mathbf{Z}) \pmod{p}$. Therefore p divides the discriminant of O_F if and only the $\mathbf{F}_p$-algebra is not a product of fields. This means that one of the local factors is of the form $O_F/\mathfrak{p}^{e_{\mathfrak{p}}}$ with $e_{\mathfrak{p}}$ stricly larger than 1. In other words, if and only if p is ramified.

Example. Take $F = \mathbf{Q}(\sqrt[3]{17})$ and $p \neq 3$. Since the index of the ring $R = \mathbf{Z}[\sqrt[3]{17}]$ inside O_F is 3, which is prime to p, the natural map $R/pR \longrightarrow O_F/(p)$ is an isomorphism. It is convenient to work with R rather than O_F. For instance $R/2R \cong \mathbf{F}_2[X]/(X^3 - 17) \cong \mathbf{F}_2[X]/(X+1) \times \mathbf{F}_2[X]/(X^2+X+1)$ since $X^3 - 17 \equiv (X+1)(X^2+X+1) \pmod 2$. Therefore $(2) = \mathfrak{p}_2\mathfrak{p}_4$ with $\mathfrak{p}_2 = (2, 1 + \sqrt[3]{17})$ and $\mathfrak{p}_4 = (2, 1 + \sqrt[3]{17} + \sqrt[3]{17}^2)$. We have that $f_{\mathfrak{p}_2} = 1$ and $f_{\mathfrak{p}_4} = 2$. Since $R/2R$ is a product of fields, the inertia indices $e_{\mathfrak{p}_2}$ and $e_{\mathfrak{p}_4}$ are equal to 1. Indeed, we have that $f_{\mathfrak{p}_2}e_{\mathfrak{p}_2} + f_{\mathfrak{p}_4}e_{\mathfrak{p}_4} = 1 + 2 = [F : \mathbf{Q}]$.

For the prime 3 we do not use the ring R and turn to the ring O_F instead. We have shown above that $O_F = \mathbf{Z}[\alpha, \beta]$ with $\alpha = \sqrt[3]{17} + 1$ and $\beta = (\sqrt[3]{17} + 1)^2/3$. In order to write a presentation of O_F as a $\mathbf{Z}$-algebra, we compute all possible products between the two generators:

$$\begin{aligned}
\alpha^2 &= 3\beta, \\
\alpha\beta = \frac{\alpha^3}{3} &= \frac{3\alpha^2 - 3\alpha + 18}{3} = 3\beta - \alpha + 6 \\
\beta^2 = \frac{\alpha^4}{9} &= \frac{3\beta\alpha - \alpha^2 + 6\alpha}{3} = \beta\alpha - \beta + 2\alpha = 2\beta + \alpha + 6.
\end{aligned}$$

This means that

$$O_F \cong \mathbf{Z}[X, Y]/(X^2 - 3Y, XY - 3Y + X - 6, Y^2 - 2Y - X + 6)$$

and hence

$$\begin{aligned}
O_F/(3) &\cong \mathbf{F}_3[X, Y]/(X^2, XY + X, Y^2 + Y - X), \\
&\cong \mathbf{F}_3[Y]/((Y^2+Y)^2, (Y^2+Y)(Y+1)), \\
&\cong \mathbf{F}_3[Y]/((Y^2+Y)(Y+1)), \\
&\cong \mathbf{F}_3[Y]/(Y) \times \mathbf{F}_3[Y]/((Y+1)^2).
\end{aligned}$$

It follows that $(3) = \mathfrak{p}_3^2\mathfrak{p}_3'$ with $\mathfrak{p}_3 = (\beta + 1, 3)$ and $\mathfrak{p}_3' = (\beta, 3)$.

Exercises.

6.1 (Kummer's Lemma) Suppose $f \in \mathbf{Z}[T]$ is an irreducible polynomial. Let α denote a zero of f and let $F = \mathbf{Q}(\alpha)$. Let p be a prime number not dividing the index $[O_F : \mathbf{Z}[\alpha]]$. Suppose the polynomial f factors in $\mathbf{F}_p[T]$ as

$$f(T) = h_1(T)^{e_1} \cdot \ldots \cdot h_g(T)^{e_g}$$

where the polynomials $h_1, \ldots, h_g$ are the distinct irreducible factors of f modulo p. Show that the prime factorization of the ideal (p) in O_F is given by

$$pO_F = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g},$$

where the $\mathfrak{p}_i = (h_i(\alpha), p)$ are distinct prime ideals with $N(\mathfrak{p}_i) = p^{\deg(h_i)}$.

6.2 Let $F = \mathbf{Q}(\alpha)$ where α be a zero of the polynomial $T^3 - T - 1$. Show that the ring of integers of F is $\mathbf{Z}[\alpha]$. Find the factorizations in $\mathbf{Z}[\alpha]$ of the primes less than 10.

6.3 Let d be a squarefree integer and let $F = \mathbf{Q}(\sqrt{d})$ be a quadratic field. Show that for *odd* primes p one has that p splits (is inert, ramifies) in F over $\mathbf{Q}$ if and only if d is a square (non-square, zero) modulo p.

6.4 Let ζ_5 denote a primitive 5th root of unity. Determine the decomposition into prime factors in $\mathbf{Q}(\zeta_5)$ of the primes less than 14.

6.5 Show that the ring of integers of $F = \mathbf{Q}(\sqrt[3]{20})$ is equal to $\mathbf{Z}[\sqrt[3]{20}, \sqrt[3]{50}]$. Show there is no $\alpha \in O_F$ such that $O_F = \mathbf{Z}[\alpha]$.

6.6 Show that the following three polynomials have the same discriminant:

$$T^3 - 18T - 6,$$
$$T^3 - 36T - 78,$$
$$T^3 - 54T - 150.$$

Let α, β and γ denote zeroes of the respective polynomials. Show that the fields $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\beta)$ and $\mathbf{Q}(\gamma)$ have the same discriminants, but are not isomorphic. (Hint: the splitting behavior of the primes is not the same.)

6.7*(Samuel) Let $f(T) = T^3 + T^2 - 2T + 8 \in \mathbf{Z}[T]$. Show that f is irreducible.

(i) Show that $\mathrm{Disc}(f) = -4 \cdot 503$. Show that the ring of integers of $F = \mathbf{Q}(\alpha)$ admits $1, \alpha, \beta = (\alpha^2 - \alpha)/2$ as a $\mathbf{Z}$-basis.

(ii) Show that O_F has precisely three distinct ideals of index 2. Conclude that 2 splits completely in F over $\mathbf{Q}$.

(iii) Show that there is no $\alpha \in F$ such that $O_F = \mathbf{Z}[\alpha]$. Show that for every $\alpha \in O_F - \mathbf{Z}$, the prime 2 divides the index $[O_F : \mathbf{Z}[\alpha]]$.

6.8*(Dedekind's Criterion.) Suppose α is an algebraic integer with minimum polynomial over $f(T) \in \mathbf{Z}[T]$. Let $F = \mathbf{Q}(\alpha)$. For p be a prime number, let $f_1, \ldots, f_g \in \mathbf{Z}[T]$ and $e_1, \ldots, e_g \in \mathbf{Z}_{\geq 1}$ such that $f = f_1^{e_1} \cdot \ldots \cdot f_g^{e_g}$ is the decomposition of f into distinct irreducible polynomials f_i modulo p. Show that

$$p \text{ divides the index } [O_F : \mathbf{Z}[\alpha]]$$

if and only if there is an index j such that

$$f_j \text{ divides } \left(\frac{f(T) - \prod_j f_j(T)^{e_j}}{p} \right) \quad \text{in } \mathbf{F}_p[T] \qquad \text{and} \qquad e_j \geq 2.$$

7. Arakelov divisors.

In this section we introduce the Arakelov class group. Let F be a number field. To every prime ideal $\mathfrak{p}$ of its ring of integers O_F we associate a $\mathfrak{p}$-adic absolute value on F by putting

$$|x|_{\mathfrak{p}} = e^{-\mathrm{ord}_{\mathfrak{p}} x}, \qquad \text{for } x \in F^*$$

and $|0|_{\mathfrak{p}} = 0$. We have the following properties:

$$\begin{aligned} |xy|_{\mathfrak{p}} &= |x|_{\mathfrak{p}}|y|_{\mathfrak{p}}, \\ |x+y|_{\mathfrak{p}} &\leq \max(|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}) \leq |x|_{\mathfrak{p}} + |y|_{\mathfrak{p}} \end{aligned}$$

for $x, y \in F$. The second property is called the Triangle Inequality. In this way, F acquires the structure of a metric toplogical space. The two properties are shared by the usual absolute values on $\mathbf{R}$ or $\mathbf{C}$. Inverting the process, we now define for each infinite prime the homomorphism $\mathrm{ord}_\sigma : F^* \longrightarrow \mathbf{R}$ given by

$$\mathrm{ord}_\sigma(x) = -\log|\sigma(x)|.$$

Definition. Let F be a number field. The *Arakelov divisor group* or *divisor group* Div_F of F is defined as

$$\mathrm{Div}_F \;=\; \bigoplus_{\mathfrak{p}} \mathbf{Z} \;\times\; \bigoplus_{\sigma} \mathbf{R}.$$

Here the first sum runs over the non-zero prime ideals of the ring of integers O_F of F and the second sum runs over the infinite primes $\sigma : F \longrightarrow \mathbf{C}$. Elements of Div_F are called *divisors* or *Arakelov divisors*. We write elements $D \in \mathrm{Div}_F$ as finite formal sums

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$$

with $x_\sigma \in \mathbf{R}$ and $n_{\mathfrak{p}} \in \mathbf{Z}$. All but finitely many of the $n_{\mathfrak{p}}$ are zero. The *support* of D is the set of primes $\mathfrak{p}$ and σ with non-zero coefficients.

Consider the homomorphism

$$d : F^* \quad \longrightarrow \quad \mathrm{Div}_F$$

that maps $x \in F^*$ to the *principal divisor* $(x) = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma\sigma$ given by $n_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(x)$ for primes $\mathfrak{p}$ of O_F and $x_\sigma = \mathrm{ord}_\sigma(x)$ for infinite primes σ.

Proposition 7.1. *Let F be a number field. The kernel of the map $d : F^* \longrightarrow \mathrm{Div}_F$ given by $x \mapsto (x)$ is a finite group equal to the group of roots of unity μ_F of F.*

Proof. Let $x \in \mu_F$. Then $x^m = 1$ for some integer $m \geq 1$. Then x is a unit so that $\mathrm{ord}_{\mathfrak{p}} x = 0$ for all primes $\mathfrak{p}$. In addition, $|\sigma(x)|^m = 1$ and hence $|\sigma(x)| = 1$ so that $\mathrm{ord}_\sigma(x) = 0$ for every σ. This shows that μ_F is contained in the kernel of d. Now we show that $\ker(d)$ is finite. Any $x \in \ker(d)$ satisfies $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for all primes $\mathfrak{p}$ and $|\sigma(x)| = 1$ for

every σ. This implies that x is in O_F and that $x \in O_F \subset F_{\mathbf{R}}$ is contained in the bounded set of vectors $(v_\sigma) \in F_{\mathbf{R}} = \prod_\sigma F_\sigma$ satsifying $|v_\sigma| \leq 1$. Since O_F is a lattice, there are only finitely many possibilities for x and hence the kernel of d is a finite group. It follows that there is an integer $m \geq 1$ for which $x^m = 1$ for all x in $\ker d$, showing that the kernel of d is contained in μ_F as required.

We identify the real vector space $\oplus_\sigma \mathbf{R}$ with the subalgebra $\prod_\sigma \mathbf{R}$ of $F_{\mathbf{R}} = \prod_\sigma F_\sigma$ and equip it with the canonical scalar product of $F_{\mathbf{R}}$. It induces the usual topological group structure on $\oplus_\sigma \mathbf{R}$. Providing the group $\oplus_{\mathfrak{p}} \mathbf{Z}$ with the discrete topology, the group of Arakelov divisors Div_F acquires the structure of a locally compact Hausdorff topological group. It is a countable union of copies of the vector space $\oplus_\sigma \mathbf{R}$. Since we have a scalar product on $\oplus_\sigma \mathbf{R}$, the group Div_F is actually a *Riemannian manifold*.

Proposition 7.2. *Let F be a number field. Then the image of the map $d : F^* \longrightarrow \mathrm{Div}_F$ is a closed discrete subset of Div_F.*

Proof. For any divisor $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} + \sum_\sigma x_\sigma \sigma$ and any $\varepsilon > 0$, the set

$$U(D) = \{\sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} + \sum_\sigma x_\sigma \sigma : |y_\sigma - x_\sigma| < \varepsilon\}$$

is an open neighborhood of D in Div_F. Moreover, such sets form a basis for the topology on Div_F. It suffices to show that these kind of sets contain only finitely many principal divisors. Suppose there is at least one such divisor (x) in $U(D)$ and let (y) be a second one. Then $u = y/x$ has the property that $\mathrm{ord}_{\mathfrak{p}}(u) = n_{\mathfrak{p}} - n_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$. Therefore u is contained in O_F^*. From $|-\log|\sigma(x)| - x_\sigma| < \varepsilon$ and $|-\log|\sigma(y)| - x_\sigma| < \varepsilon$ we deduce that $|\log|\sigma(u)|| < 2\varepsilon$ for every σ. It follows that the collection of such units u is contained in a bounded subset of $F_{\mathbf{R}}$. Therefore there are only finitely many and the proposition follows.

Definition. Let F be a number field. By Pic_F we denote the quotient of the group Div_F by the image of F^* under the map d. In other words, Pic_F is the group of Arakelov divisors modulo principal Arakelov divisors.

Since the image of F^* is closed in Div_F, the group Pic_F has a natural induced structure of a topological group. It is Hausdorff and locally compact. In addition, Pic_F inherits the Riemannian structure from Div_F.

Definition. Let F be a number field. The *degree* of a non-zero prime ideal is defined by

$$\deg(\mathfrak{p}) = \log N(\mathfrak{p}).$$

The degree of an infinite prime σ is defined to be 1 or 2 depending on whether σ is real or complex. We extend the degree linearly to the entire divisor group and in this way we obtain a continuous homomorphism

$$\deg : \mathrm{Div}_F \longrightarrow \mathbf{R}.$$

The degree map is surjective. Its kernel is denoted by Div_F^0.

Proposition 7.3. *(Product Formula) Principal Arakelov divisors have degree zero.*

Proof. Let $x \in F^*$. By Prop. 5.7 we have that

$$N((x)) = |N(x)|.$$

Let $xO_F = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ be the prime decomposition of the principal ideal generated by x. It follows from the multiplicativity of the norm map and Lemma 5.1 that

$$\prod_{\mathfrak{p}} N(\mathfrak{p})^{n_{\mathfrak{p}}} = \prod_{\sigma} |\sigma(x)|^{\deg \sigma}.$$

Taking logarithms implies the result.

Proposition 7.3 says that the image of F^* under the map d is contained in the subgroup Div_F^0. This leads to the following definition.

Definition. Let F be a number field. The *Picard-Arakelov class group* or *Arakelov class group* Pic_F^0 is the group Div_F^0 modulo the image of F^* under the map d.

There is a natural exact sequence

$$0 \longrightarrow \quad \mathrm{Pic}_F^0 \quad \longrightarrow \quad \mathrm{Pic}_F \quad \stackrel{\deg}{\longrightarrow} \quad \mathbf{R} \quad \longrightarrow 0.$$

The Arakelov class group inherits its structure of a topological group and Riemannian manifold from the group Pic_F. In the rest of this section we relate it to the class group and the unit group of the Dedekind ring O_F. The image of the principal Arakelov divisors under the projection map from Div_F to the group of fractional ideals $\oplus_{\mathfrak{p}} \mathbf{Z}$ is precisely the group Pr_F of *principal* fractional ideals. This leads to the following commutative diagram with exact rows and columns.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & O_F^*/\mu_F & \longrightarrow & F^*/\mu_F & \longrightarrow & \mathrm{Pr}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{\sigma} \mathbf{R} & \longrightarrow & \mathrm{Div}_F & \longrightarrow & \bigoplus_{\mathfrak{p}} \mathbf{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T & \longrightarrow & \mathrm{Pic}_F & \longrightarrow & Cl(O_F) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Here T is defined as the cokernel of the homomorphism $O_F^* \longrightarrow \oplus_{\sigma} \mathbf{R}$. Recall that the latter homomorphism maps a unit u to the vector$(-\log|\sigma(u)|)$. Note that the quotient

topology on $Cl(O_F)$ is discrete. All homomorphisms in the diagram all continuous. This is either trivially so or it follows from the universal property of the quotient topology.

Now we take degree zero parts. First in the central column. Since F has at least one infinite prime, the projection map $\mathrm{Div}_F^0 \longrightarrow \oplus_{\mathfrak{p}} \mathbf{Z}$ is still surjective. Its kernel is given by

$$(\oplus_\sigma \mathbf{R})^0 = \{(x_\sigma) \in \oplus_\sigma \mathbf{R} : \sum_\sigma \deg(\sigma) x_\sigma = 0\}.$$

Denoting the cokernel of the homomorphism $O_F^*/\mu_F \longrightarrow (\oplus_\sigma \mathbf{R})^0$ by T^0 we obtain the following commutative diagram with exact rows and columns and continuous homomorphisms. The bottom row shows that Pic_F^0 is an extension of the discrete ideal class group $Cl(O_F)$ by the connected group T^0.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & O_F^*/\mu_F & \longrightarrow & F^*/\mu_F & \longrightarrow & \mathrm{Pr}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \left(\underset{\sigma}{\oplus} \mathbf{R}\right)^0 & \longrightarrow & \mathrm{Div}_F^0 & \longrightarrow & \underset{\mathfrak{p}}{\oplus} \mathbf{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T^0 & \longrightarrow & \mathrm{Pic}_F^0 & \longrightarrow & Cl(O_F) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

For $F = \mathbf{Q}$ there is only one infinite prime and therefore T^0 is trivial. Since $\mathbf{Z}$ is a unique factorization domain, the class group is trivial as well. It follows that $\mathrm{Pic}_{\mathbf{Q}}$ is trivial and that

$$\mathrm{Pic}_{\mathbf{Q}} \quad \underset{\cong}{\overset{\deg}{\longrightarrow}} \quad \mathbf{R}$$

is an isomorphism. See sections 10 and 13 for non-trivial examples of Arakelov-Picard class groups.

Definition. Let F be a number field. We define a norm on the connected component T of Pic_F by putting

$$\|x\|_{\mathrm{Pic}} = \min_{\varepsilon \in O_F^*} \|\varepsilon x\|.$$

Here $\|\varepsilon x\|$ denotes the length of $\varepsilon x \in F_{\mathbf{R}}$ with respect to the canonical scalar product.

The norm on Pic_F satisfies the triangle inequality and induces the usual metric structure on Pic_F.

Exercises.

7.1 Let G be a topological group with neutral element 1.
(i) Show that for every open neighborhood U of $1 \in G$, there is an open neighborhood V of 1 for with $V^2 \subset U$. Here $V^2 = \{vw : v, w \in V\}$.
(ii) Show that G is Hausdorff if and only if 1 is closed.

7.2 Let G be a topological group.
(i) Show that every open subgroup of G is also closed.
(ii) Let $H \subset G$ be a normal subgroup. Show that G/H, equipped with the quotient topology, is Hausdorff if and only if H is closed in G.

7.3 Let $F = \mathbf{Q}(\sqrt[3]{-2})$. Let $x = 1 - \sqrt[3]{-2}$. Compute the coordinates of the principal Arakelov divisor (x). Check that $\deg((x)) = 0$.

7.4 Show that the $\mathrm{Pic}^0_F = 0$ for $F = \mathbf{Q}(i)$.

7.5 Let F be a number field and let $x, y \in T = (\oplus_\sigma \mathbf{R})\,/\mathrm{im}(O_F^*)$. Show that $\|x + y\|_{\mathrm{Pic}} \leq \|x\|_{\mathrm{Pic}} + \|y\|_{\mathrm{Pic}}$.

8. Ideal lattices.

In this section we interpret Arakelov divisors as ideal lattices. We show that the Arakelov class group classifies ideal lattices up to isometry. We first introduce the *Hermitian line bundle* associated to an Arakelov divisor.

Let F be a number field and let $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma \sigma$ be an Arakelov divisor. We put $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ and call it the *ideal associated to* D. Then we let u denote the vector $(u_\sigma) \in \prod_\sigma \mathbf{R}^*_{>0}$ for which $u_\sigma = \exp(-x_\sigma)$ for each σ. Since the group $\prod_\sigma \mathbf{R}^*_{>0}$ is contained in $F^*_{\mathbf{R}} \cong \prod_\sigma F^*_\sigma$, we may view u as an element of $F^*_{\mathbf{R}}$. It is *totally positive* in the sense that each coordinate u_σ is contained in the subgroup $\mathbf{R}^*_{>0}$ of F^*_σ.

Notation. Let F be a number field and let$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma \sigma$ be an Arakelov divisor. Then the *Hermitian line bundle* associated to D is the pair (I, u) where I is a fractional ideal and u is a totally positive unit in $F^*_{\mathbf{R}}$ as explained above.

For any Arakelov divisor $D = (I, u)$ we have that $N(D)^{-1} = N(u)N(I)$. To D we associate the O_F-submodule

$$uI = \{ux : x \in I\} \ \subset \ F_{\mathbf{R}}.$$

Since I is a lattice in $F_{\mathbf{R}}$, so is uI. We have by Prop. 5.5 that

$$\mathrm{covol}(uI) = N(u)N(I)\sqrt{|\Delta_F|} = e^{-\deg(D)}\sqrt{|\Delta_F|}.$$

Definition. Let F be a number field. An *ideal lattice* associated to F is a projective O_F-module M of rank 1 together with a scalar product on the $F_{\mathbf{R}}$-module $L \otimes_{\mathbf{Z}} \mathbf{R}$ that satisfies $\langle \lambda x, y\rangle = \langle x, \overline{\lambda} y\rangle$ for all $x, y \in L \otimes_{\mathbf{Z}} \mathbf{R}$ and all $\lambda \in F_{\mathbf{R}}$. Two ideal lattices L and L' are said to be *isometric* if there is an isomorphism $f : L \longrightarrow L'$ of O_F-modules that is compatible with the scalar products on $L \otimes_{\mathbf{Z}} \mathbf{R}$ and $L' \otimes_{\mathbf{Z}} \mathbf{R}$.

Proposition 8.1. *Let F be a number field. Then two Arakelov divisors $D = (I, u)$ and $D' = (I', u')$ have the same classes in Pic_F if and only if the associated ideal lattices uI and $u'I'$ are isometric.*

Proof. If $D + (f) = D'$ for some $f \in F^*$, then we have that $I = fI'$ and $u|f| = u'$. This means that the map $F_{\mathbf{R}} \longrightarrow F_{\mathbf{R}}$ given by multiplication by $u^{-1}f^{-1}u'$ is O_F-linear and maps I to I'. Since $|u^{-1}f^{-1}u'| = 1$ it also preserves the canonical scalar product on $F_{\mathbf{R}}$. This is the content of by Exer. 5.7. Conversely, suppose that $\varphi : uI \longrightarrow u'I'$ is O_F-linear and compatible with the scalar products on $uI \otimes_{\mathbf{Z}} \mathbf{R} = u'I' \otimes_{\mathbf{Z}} \mathbf{R} = F_{\mathbf{R}}$. Then the induced map $F_{\mathbf{R}} \longrightarrow F_{\mathbf{R}}$ is $F_{\mathbf{R}}$-linear and compatible with the canonical scalar product. By Exer. 5.7 it is therefore given by multiplication my some element $x \in F_{\mathbf{R}}^*$ with $|x| = 1$. It follows that the element $f = u^{-1}x^{-1}u'$ is in F^* and satisfies $|u^{-1}f^{-1}u'| = u^{-1}|f|^{-1}u' = 1$. Since $fI' = I$, we see that $D + (f) = D'$. This proves the proposition.

Proposition 8.2. *Let F be a number field. The map that associates to an Arakelov divisor $D = (I, u)$ the ideal lattice uI induces a bijection*

$$\mathrm{Pic}_F \quad \stackrel{\cong}{\longrightarrow} \quad \{\textit{ideal lattices up to isometry}\}.$$

Proof. By the previous proposition the map that associates the lattice uI to an Arakelov divisor $D = (I, u)$ is well defined and injective. We need to show it is surjective. Let L be an ideal lattice. Then there is an isomorphism of O_F-modules $L \cong I$ for some fractional ideal I. By means of this isomorphism we identify $L \otimes_{\mathbf{Z}} \mathbf{R}$ with $I \otimes_{\mathbf{Z}} \mathbf{R} = F_{\mathbf{R}}$. In this way, the scalar product on $L \otimes_{\mathbf{Z}} \mathbf{R}$ leads to a scalar product $\langle -, - \rangle_L$ on $F_{\mathbf{R}}$ that satisfies $\langle \lambda x, y \rangle_L = \langle x, \overline{\lambda} y \rangle_L$ for $x, y, \lambda \in F_{\mathbf{R}}$. For every infinite prime σ, let $e_\sigma \in F_{\mathbf{R}}$ denote the idempotent that has all its coordinates in $F_{\mathbf{R}} \cong \prod_\sigma F_\sigma$ equal to zero, except the σ-th one, which is 1. Put $u = \sum_\sigma \langle e_\sigma, e_\sigma \rangle_L^{1/2} e_\sigma \in F_{\mathbf{R}}^*$. Since the idempotents e_σ are orthogonal, we have for every $x, y \in F_{\mathbf{R}}$ that

$$\langle ux, uy \rangle = \sum_\sigma u_\sigma^2 x_\sigma \overline{y}_\sigma = \sum_\sigma x_\sigma \overline{y}_\sigma \langle e_\sigma, e_\sigma \rangle_L = \langle x, y \rangle_L.$$

Therefore the isomorphism $L \longrightarrow I$ above induces an isomorphsm of ideal lattices $(I, u) \cong L$ as required.

The following result says that ideal lattices are 'beautiful' in the sense that they admit bases that are not very skew. In other words, ideal lattices do not contain any very short vectors.

Proposition 8.3. *Let F be a number field of degree n and let $D = (I, u)$ be an Arakelov divisor. Then for every non-zero y in the associated ideal lattice uI we have that*

$$\|y\|^2 \geq n e^{-\frac{2}{n}\deg(D)}.$$

In particular, when $\deg(D) = 0$, the shortest non-zero vectors of the lattice uI have length at least $\sqrt{n}$.

Proof. Let $0 \neq y \in uI$. By the Arithmetic-Geometric Mean inequality we have that

$$\|y\|^2 = \sum_\sigma \deg(\sigma)|y_\sigma|^2 \geq n\left(\prod_\sigma |y_\sigma|^{2\deg(\sigma)}\right)^{1/n} = n|N(y)|^{2/n}.$$

Since $y = ux$ for some non-zero $x \in I$ and since $|N(x)| \geq N(I)$ we have therefore that

$$\|y\|^2 \geq n|N(u)N(x)|^{2/n} \geq n|N(u)N(I)|^{2/n} = ne^{-\frac{2}{n}\deg(D)}.$$

The last inequality follows from the fact that $e^{-\deg(D)} = N(D)^{-1} = N(U)N(I)$. This proves the proposition.

Exercises.

8.1 Let $D = (I, u)$ and $D' = (I', u')$ be two Arakelov divisors of a number field F. Check that $D + D' = (II', uu')$. Check that the neutral element of Div_F is the pair $(O_F, 1)$. Show that the degree of $D = (I, u)$ is equal to $-\log(N(u)N(I))$.

8.2 Let F be a number field of degree n. If the lattice associated to an Arakelov divisor $D = (I, u)$ of degree 0 contains a vector ux of length $\sqrt{n}$, then D is the principal divisor generated by x.

8.3 Show that under the isomorphism $\deg : \mathrm{Pic}_{\mathbf{Q}} \cong \mathbf{R}$, the Arakelov divisor corresponding to $x \in \mathbf{R}$ is $x \cdot \sigma$ where $\sigma : \mathbf{Q} \hookrightarrow \mathbf{R}$ is the inclusion map. Show that the ideal lattice corresponding to $x \in \mathbf{R}$ is given by $e^{-x}\mathbf{Z}$.

8.4 Let $F = \mathbf{Q}(\sqrt{-5})$. Let I be the O_F-ideal generated by 2 and $1 + \sqrt{-5}$. Show that $D = (I, 1/\sqrt{2})$ is a Hermitian line bundle of degree 0. Draw pictures of the ideal lattices associated to $(O_F, 1)$ and D.

9. Minkowski and Dirichlet.

In this section we show that the Arakelov divisor class group Pic_F^0 of a number field F is a compact topological group. The proof is constructive in the sense that we cover Pic_F^0 with an explicit finite set of closed simplices. As a consequence we obtain Minkowski's Theorem that the ideal class group $Cl(O_F)$ of the ring of integers O_F of a number field F is finite and Dirichlet's Unit Theorem that the unit group O_F^* is finitely generated.

Proposition 9.1. *Let F be a number field. For any divisor $D = (I, u)$ in Div_F^0 there exists an element $x \in I$, so that the O_F-ideal $J = xI^{-1}$ satisfies*

$$N(J) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_F|}$$

and $v = u|x| \in F_{\mathbf{R}}^*$ satisfies

$$\log|v_\sigma| = \log|u_\sigma \sigma(x)| \leq \frac{1}{n}\log(\sqrt{|\Delta_F|}) - \frac{r_2}{n}\log(\frac{\pi}{2}), \qquad \textit{for all infinite primes } \sigma.$$

Proof. Let $D = (I, u)$ be a divisor of degree 0. The corresponding ideal lattice $uI \subset F_{\mathbf{R}}$ has covolume $\sqrt{|\Delta_F|}$. The volume of the bounded symmetric and convex 'box'

$$B(R) = \{(x_\sigma) \in F_{\mathbf{R}} : |x_\sigma| \leq R\}$$

is equal to $2^{r_1}(2\pi)^{r_2}R^n$. Here r_1 and r_2 denote the number of real and complex primes of F respectively. Let $\varepsilon \geq 0$ and let $R > 0$ be determined by $2^{r_1}(2\pi)^{r_2}R^n = 2^n\sqrt{|\Delta_F|} + \varepsilon$. By Minkowski's Convex Body Theorem Thm. 4.2, there is a non-zero element in $uI \cap B(R)$ when $\varepsilon > 0$. Since $uI \cap B(R)$ is finite, it follows then that there exists also a non-zero $x \in uI \cap B(R)$ when $\varepsilon = 0$.

In other words, there is a non-zero $x \in I$ for which $|u_\sigma\sigma(x)| \leq R$ for all σ and hence

$$|N(x)N(u)| = \prod_\sigma |u_\sigma\sigma(x)|^{\deg(\sigma)} \leq R^n = \frac{2^n\sqrt{|\Delta_F|}}{2^{r_1}(2\pi)^{r_2}}.$$

We put $J = xI^{-1}$. Since $\deg(D) = 0$ we have that $|N(u)| = N(I)^{-1}$ and we find that

$$N(J) = |N(x)|/N(I) \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\Delta_F|}.$$

Moreover

$$\log|u_\sigma\sigma(x)| \leq \frac{1}{n}\log\left((\frac{2}{\pi})^{r_2}\sqrt{|\Delta_F|}\right), \qquad \text{for all } \sigma,$$

as required.

Theorem 9.2. *Let F be a number field. Then the group Pic_F^0 is compact.*

Proof. By Prop. 9.1 there exists for every divisor $D = (I, u)$ of degree 0 a principal divisor (x) and a divisor of the form (J^{-1}, v) with $J \subset O_F$ and $v \in F_{\mathbf{R}}^*$ totally positive satisfying

$$\begin{aligned} N(J) &\leq \left(\tfrac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_F|}, \\ \log(v_\sigma) &\leq \tfrac{1}{n}\log(\sqrt{|\Delta_F|}) - \tfrac{r_2}{n}\log(\tfrac{\pi}{2}) \quad \text{for all } \sigma, \end{aligned}$$

so that

$$D + (x) \quad = \quad (J^{-1}, v).$$

In other words, Pic_F^0 is the continuous image of the subset S of Arakelov divisors of degree zero that are of the form (J^{-1}, v) with J and v as above.

Since $\deg(J^{-1}, v) = 0$, we have that $\sum_\sigma \deg(\sigma)\log(v_\sigma) = 0$. Therefore the elements $v \in F_{\mathbf{R}}^*$ satisfying the conditions above form a *compact* simplex. Indeed, the inequality of Exercise 9.1 implies that

$$\|v\|_{\mathrm{Pic}}^2 \leq \sum_\sigma \deg(\sigma)\log^2|u_\sigma\sigma(x)| \leq \frac{n(n-1)}{n^2}\log^2\sqrt{|\Delta_F|}$$

and hence $\|v\|_{\mathrm{Pic}} \leq \frac{1}{2}\log|\Delta_F|$.

By Prop. 5.7 there are only finitely many ideals $J \subset O_F$ of bounded norm. This implies the set S is a *compact* subset of Div_F. It follows that Pic_F^0 is itself compact.

Corollary 9.3. *Let F be a number field. Then*

(i) (Minkowski) the ideal class group $Cl(O_F)$ is finite;

(ii) (Dirichlet) the image of O_F^* in the Euclidean space $(\oplus_\sigma \mathbf{R})^0$ is a lattice. In particular, O_F is a finitely generated abelian group isomorphic to $\mathbf{Z}^{r_1+r_2-1} \times \mu_F$.

Proof. By section 7 there is an exact sequence

$$0 \longrightarrow T^0 \longrightarrow \mathrm{Pic}_F^0 \longrightarrow Cl_F \longrightarrow 0.$$

with continuous homomorphisms. Since Pic_F^0 is compact, so is Cl_F. On the other hand Cl_F has the discrete topology. It follows that Cl_F is finite. This proves *(i)*. The T^0 is of the form $(\oplus_\sigma \mathbf{R})^0$ modulo the discrete subgroup formed by the image of the unit group. Since T^0 is a closed subgroup of Pic_F^0, it is compact. It follows that the image of the unit group is a lattice inside the real vector space $(\oplus_\sigma \mathbf{R})^0$ of dimension $r_1 + r_2 - 1$. Since the kernel of the map $O_F^* \longrightarrow (\oplus_\sigma \mathbf{R})^0$ given by $\varepsilon \mapsto (\log|\sigma(\varepsilon)|)_\sigma$ consists precisely of the subgroup of roots of unity, part *(ii)* follows.

Proposition 9.4. *Let F be a number field of degree n with r_1 real and r_2 complex infinite primes. Then the natural volume of the Arakelov class group is equal to*

$$2^{\frac{r_2}{2}}\frac{h}{\sqrt{n}}\left|\det\begin{pmatrix} 1 & \log|\sigma_1\varepsilon_1| & \dots & \log|\sigma_1\varepsilon_{r-1}| \\ 1 & \log|\sigma_2\varepsilon_1| & \dots & \log|\sigma_2\varepsilon_{r-1}| \\ \vdots & \vdots & & \vdots \\ 1 & \log|\sigma_r\varepsilon_1| & \dots & \log|\sigma_r\varepsilon_{r-1}| \end{pmatrix}\right|.$$

Here $r = r_1 + r_2$ denotes the number of infinite primes σ_i. By $h = \#Cl(O_F)$ we denote the class number of F and by $\varepsilon_1, \ldots, \varepsilon_{r-1}$ a set of generators of the unit group O_F^* modulo torsion. The matrix is therefore an r by r-matrix.

Proof. The vector $1 \in \oplus_\sigma \mathbf{R}$ is orthogonal to $(\oplus_\sigma \mathbf{R})^0$ and has length $\sqrt{n}$. Therefore the volume of the torus T^0 is equal to the determinant above times the volume of the unit block $\{(v_\sigma) \in F_{\mathbf{R}} : |v_\sigma| \leq 1 \text{ for all } \sigma\}$ divided by $\sqrt{n}$. The unit block has volume $2^{r_2/2}$. The proposition now follows from the fact that the volume of Pic_F^0 is equal to the volume T^0 times the class number.

It follows from Theorem 9.1 that for a number field F, every ideal class in $Cl(O_F)$ contains an integral ideal of norm at most $\left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_F|}$. This result can be improved somewhat by choosing another kind of 'box' in $F_{\mathbf{R}}$.

Proposition 9.5. *Let F be a number field of degree n with r_1 real and r_2 complex infinite primes. Then every ideal class contains an ideal $I \subset O_F$ with*

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_F|}.$$

Proof. Let $R > 0$ and consider the set

$$B'(R) = \{(x_\sigma) \in F_{\mathbf{R}} : \mathrm{Tr}|x_\sigma| \leq R\}.$$

This a bounded symmetric convex set and by Exercise 9.3, its volume is equal to

$$\mathrm{vol}(B'(R)) = 2^{r_1} \pi^{r_2} \frac{R^n}{n!}.$$

Let I' be an ideal in the inverse of a given ideal class in $Cl(O_F)$. The covolume of the lattice $I' \subset F \subset F_{\mathbf{R}}$ is $N(I')\sqrt{|\Delta_F|}$. Let $\varepsilon \geq 0$ and let R be such that

$$2^{r_1} \pi^{r_2} \frac{R^n}{n!} = 2^n N(I') \sqrt{|\Delta_F|} + \varepsilon.$$

If $\varepsilon > 0$ there is by Theorem 4.2 a non-zero vector $x \in I' \cap B'(R)$. This implies that the ideal $I = x{I'}^{-1}$ is contained in O_F. It is contained in the ideal class that was given above. By an argument similar to the one used in the proof of Thm. 9.1, the same is true with $\varepsilon = 0$. By the Arithmetic-Geometric Mean inequality of Exer. 9.2 we have that

$$|N(x)| = \prod_\sigma |\sigma(x)|^{\deg(\sigma)} \leq \left(\frac{R}{n}\right)^n$$

and hence

$$N(I) = |N(x)|/N(I') \leq \left(\frac{R}{n}\right)^n \frac{1}{N(I')} = \frac{(2^n N(I') \sqrt{|\Delta_F|}) n!}{n^n 2^{r_1} \pi^{r_2} N(I')}.$$

This proves the proposition.

Corollary 9.6. *Let F be a number field of degree n with r_1 real and r_2 complex primes. Then*
(i)

$$|\Delta_F| \geq \left(\frac{n^n}{n!} (\frac{\pi}{4})^{r_2} \right)^2 ;$$

(ii) $|\Delta_F| \geq \frac{\pi^n}{4}$. *In particular,* $|\Delta_F| > 1$ *whenever* $F \neq \mathbf{Q}$.

Proof. Part *(i)* follows by applying the proposition to the trivial class. To prove *(ii)* one verifies inductively that $n^n \geq 2^{n-1} n!$ for all $n \geq 1$. Part *(i)* implies then that

$$|\Delta_F| \geq \left(\frac{n^n}{n!} \right)^2 \left(\frac{\pi}{4} \right)^{2r_2} \geq (2^{n-1})^2 \left(\frac{\pi}{4} \right)^n = \frac{\pi^n}{4}.$$

This proves the corollary.

In the rest of this section we consider the covering of Pic_F^0 of Theorem 9.2 in some more detail. Let F be a number field of degree n. For every ideal $J \subset O_F$, we let Σ_J denote the set of divisors given by

$$\Sigma_J = \{(J^{-1}, v) \in \mathrm{Div}_F^0 : \log(v_\sigma) \leq \tfrac{1}{n} \log(\sqrt{|\Delta_F|}) - \tfrac{r_2}{n} \log(\tfrac{\pi}{2}) \text{ for all } \sigma\}.$$

If $N(J) \leq \left(\frac{\pi}{2}\right)^{r_2} \sqrt{|\Delta_F|}$, the set Σ_J is a simplex. To see this, notice that in that case Σ_J contains the divisor $(J^{-1}, N(J)^{1/n})$ and that the elements in Σ_J are sums of $(J^{-1}, N(J)^{1/n})$ and an element in the following subset of $(\oplus_\sigma \mathbf{R})^0 \subset \mathrm{Div}_F^0$:

$$\{(w_\sigma) \in \left(\bigoplus_\sigma \mathbf{R} \right)^0 : w_\sigma \leq \tfrac{1}{n} \log(\sqrt{|\Delta_F|}/N(J)) - \tfrac{r_2}{n} \log(\tfrac{\pi}{2})\}.$$

In order to compare the size of the images of the various Σ_J in Pic_F^0, we fix a connected component, i.e. a coset of the torus $T^0 = (\oplus_\sigma \mathbf{R})^0 / \mathrm{im}(O_F^*)$, and choose an ideal $I \subset O_F$ in the ideal class that corresponds to it. Then the divisor $(I^{-1}, N(I)^{1/n})$ lies on the component. Let $J \subset O_F$ in the same ideal class as I. We have that $I = \beta J$ for some $\beta \in F^*$. The divisors of degree zero of the form (J^{-1}, v) lie on the component $(I^{-1}, N(I)^{1/n}) + T^0$ and we have that

$$\begin{aligned} (J^{-1}, v) = (\beta I^{-1}, v) &\sim (I^{-1}, |\beta| v), \\ &\sim (I^{-1}, N(I)^{1/n}) + (O_F, \frac{|\beta|}{N(\beta)^{1/n}}) + (O_F, \frac{v}{N(J)^{1/n}}). \end{aligned}$$

Suppose now that $N(J) < \left(\frac{\pi}{2}\right)^{r_2} \sqrt{|\Delta_F|}$ and consider the image of the simplex Σ_J in the component $(I^{-1}, N(I)^{1/n}) + T^0$. The elemenst of Σ_J are sums of $(I^{-1}, N(I)^{1/n})$ and elements of the set

$$\{\left(\log(\frac{|\sigma(\beta)|}{N(\beta)^{1/n}}) \right) + (w_\sigma)\} \quad \subset \quad (\bigoplus_\sigma \mathbf{R})^0$$

with $w_\sigma \leq \frac{1}{n}\log(\frac{\sqrt{|\Delta_F|}}{N(J)}) - \frac{r_2}{n}\log(\frac{\pi}{2})$ and $\sum_\sigma \deg(\sigma)w_\sigma = 0$. The size of the simplex gets smaller as the norm $N(J)$ of J becomes larger.

Exercises.

9.1 Let $x_i \in \mathbf{R}$ for $1 \leq i \leq n$. Suppose that $\sum_i x_i \geq 0$ and that $x_i \leq a$ for some $a \in \mathbf{R}$. Then $\sum_i x_i^2 \leq n(n-1)a^2$.

9.2 (Arithmetic-Geometric Mean Inequality) Let $x_i \in \mathbf{R}_{\geq 0}$ for $1 \leq i \leq n$ Then

$$(x_1 \cdots x_n)^{1/n} \leq \frac{x_1 + \ldots + x_n}{n}.$$

(Hint: Put $\mu = \frac{x_1+\ldots+x_n}{n}$ and show that $e^{x_i/\mu - 1} \geq \frac{x_i}{\mu}$ for each i with equality holding if and only if $x_i = \mu$.

9.3 Let $r_1, r_2 \in \mathbf{Z}_{\geq 0}$ and put $r_1 + r_2 = n$. Let $R \geq 0$ and put

$$W(r_1, r_2, R) = \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} : \sum_{i=1}^{r_1} |x_i| + \sqrt{2}\sum_{j=1}^{r_2} |z_j| \leq R\}$$

(i) Show that the volume of the subset $B'(R)$ of $F_{\mathbf{R}}$ is equal to the volume of $W(r_1, r_2, R)$ (with respect to the usual metrics on $\mathbf{R}$ and $\mathbf{C}$.

(ii) Show that $\mathrm{vol}(W(1, 0, R)) = 2R$ and that $\mathrm{vol}(W(0, 1, R)) = \pi R^2$.

(iii) Show that

$$\mathrm{vol}(W(r_1, r_2, R)) = 2^{r_1}\pi^{r_2}\frac{R^n}{n!}.$$

(Hint: proceed by induction.)

10. Explicit computation.

In this section we present two explicit examples. We compute the Arakelov class groups of two quadratic fields.

Example 10.1. $F = \mathbf{Q}(\sqrt{-26})$.

The field F is a *complex quadratic* field. This means that it cannot be embedded into $\mathbf{R}$ and admits, up to conjugation, only one embedding into $\mathbf{C}$. In other words, F has $r_1 = 0$ real infinite primes and $r_2 = 1$ infinite complex prime. It follows that the vector space $(\prod_\sigma \mathbf{R})^0$ and hence the torus T^0 are both trivial. As a consequence the natural map

$$\mathrm{Pic}_F^0 \quad \xrightarrow{\cong} \quad Cl(O_F)$$

that maps Arakelov divisors $D = (I, u)$ to the class of the ideal I, is an isomorphism. Since $-26 \not\equiv 1 \pmod 4$, Exer. 3.4 implies that the ring of integers of F is given by $O_F = \mathbf{Z}[\sqrt{-26}]$. The minimum polynomial of $\alpha = \sqrt{-26}$ is equal to $f(T) = T^2 + 26$. The unit group O_F^* is finite. Any unit $\varepsilon = x + y\alpha \in O_F^*$ has norm $x^2 + 26y^2$ equal to 1. In order to compute them we solve the equation

$$x^2 + 26y^2 = 1, \qquad \text{for } x, y \in \mathbf{Z}.$$

The only solutions are $x = \pm 1$ and $y = 0$. It follows that $O_F^* = \{\pm 1\}$. The discriminant Δ_F is defined as the discriminant of the free $\mathbf{Z}$-algebra O_F over $\mathbf{Z}$. By Prop. 3.1 is equal to the discriminant of $f(T)$, i.e., we have that $\Delta_F = -4 \cdot 26 = -104$. Alternatively, one may compute Δ_F using its definition. Since $\{1, \alpha\}$ is a $\mathbf{Z}$-basis for O_F and since $\mathrm{Tr}(\alpha) = 0$, we have that

$$\Delta_F = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & -52 \end{pmatrix} = -104.$$

By Prop. 6.5 the only ramified primes are 2 and 13. By Prop. 9.5, the ideal class group $Cl(O_F)$ is generated by the primes of norm less than $\frac{2}{\pi}\sqrt{104} = 6.49\ldots$. We now compute explicit *generators* for these prime ideals and find *relations* among them by factoring suitable principal ideals into products of prime ideals. This is conveniently done simultaneously as follows.

We first compute $f(k) = k^2 + 26$ for several small integers k and factor these numbers into a product of prime numbers. The result is given below.

Table 10.2.

	k	$f(k) = k^2 + 26$	$(\alpha - k)$
(i)	0	$26 = 2 \cdot 13$	$\mathfrak{p}_2\mathfrak{p}_{13}$
(ii)	1	$27 = 3^3$	$\mathfrak{p}_3{}^3$
(iii)	2	$30 = 2 \cdot 3 \cdot 5$	$\mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5$
(iv)	3	$35 = 5 \cdot 7$	$\mathfrak{p}_5'\mathfrak{p}_7$

Since 2 is ramified there is only one prime $\mathfrak{p}_2$ that divides 2. We have that $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2^2 = (2)$. It follows from the table that the polynomial $f(T)$ has zeroes modulo the

primes 3 and 5. This implies that these primes split in F. We have that $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ with $\mathfrak{p}_3 = (\alpha - 1, 3)$ and $\mathfrak{p}_3' = (\alpha + 1, 3)$. This follows from the fact that the maximal ideals of the ring $O_F/(3) \cong \mathbf{F}_3[X]/(X^2 - 1) \cong \mathbf{F}_3[X]/(X - 1) \times \mathbf{F}_3[X]/(X + 1)$ are generated by $X - 1$ and $X + 1$ respectively. The ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are then the kernels of the maps $O_F \twoheadrightarrow \mathbf{F}_3[X]/(X - 1)$ and $O_F \twoheadrightarrow \mathbf{F}_3[X]/(X + 1)$ respectively. Similarly, $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ with $\mathfrak{p}_5 = (\alpha - 2, 5)$ and $\mathfrak{p}_5' = (\alpha + 2, 5)$.

The class group Cl_F is therefore generated by the classes of the ideals $\mathfrak{p}_2'$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_5$ and $\mathfrak{p}_5'$. In order to determine the structure of Cl_F factor certain principal ideals into products of prime ideals. The factorizations $(2) = \mathfrak{p}_2^2$ and the ones of (p) for $p = 3$, 5 and 7 give rise to the relation $\mathfrak{p}_2^2 \sim 1$ and the relations $\mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$ and $\mathfrak{p}_5' \sim \mathfrak{p}_5^{-1}$ respectively. Here "$\sim$" denotes equality up to principal ideals and '1' denotes the trivial class. It follows at once that Cl_F is already generated by the classes of $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_5$. We use Table 10.2 to obtain more relations. Entry (iii) of the table implies that $\mathfrak{p}_5 \sim \mathfrak{p}_2^{-1}\mathfrak{p}_3'^{-1} \sim \mathfrak{p}_2\mathfrak{p}_3$. Therefore $\mathfrak{p}_5$ is contained in the subgroup generated by $\mathfrak{p}_2$ and $\mathfrak{p}_3$ and we don't need it as a generator. Entry (ii) of the table implies that $\mathfrak{p}_3^3 \sim 1$. It follows from entry (ii) and the fact that $\mathfrak{p}_2^2 \sim 1$ that Cl_F is a quotient of the free group generated by $\mathfrak{p}_2$ and $\mathfrak{p}_3$ modulo the relations $\mathfrak{p}_2^2 \sim 1$ and $\mathfrak{p}_3^3 \sim 1$. Therefore Cl_F is a quotient of the group $\mathbf{Z}/6\mathbf{Z}$.

When one does more computations like this, one keeps finding relations that are implied by the ones already found. For instance, since $f(7) = 49 + 26 = 75 = 3 \cdot 5^2$, the principal ideal $(\alpha - 7)$ factors as $\mathfrak{p}_5^2\mathfrak{p}_3$. It follows that $\mathfrak{p}_5^2 \sim \mathfrak{p}_3^{-1}$. But this already follows from entry (iii). Indeed, from $\mathfrak{p}_5 \sim \mathfrak{p}_3\mathfrak{p}_2^{-1}$ we deduce that $\mathfrak{p}_5^2 \sim \mathfrak{p}_3^2\mathfrak{p}_2^{-2} \sim \mathfrak{p}_3^{-1}$. Instead, we are going to try to *prove* that $Cl_F \cong \mathbf{Z}/6\mathbf{Z}$. It suffices to show that $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are not principal. Suppose that $\mathfrak{p}_2$ is principal. Then $\mathfrak{p}_2 = (\beta)$ for some $\beta \in O_F$. Since $O_F = \mathbf{Z}[\sqrt{-26}]$, we have that $\beta = x + y\sqrt{-26}$ for some $x, y \in \mathbf{Z}$. Taking norms we find that

$$2 = x^2 + 26y^2.$$

It is easy to see that this equation has no solutions $x, y \in \mathbf{Z}$. Therefore β does not exist and $\mathfrak{p}_2$ is not principal. One shows in a similar way that $\mathfrak{p}_3$ is not principal. In this case it is the Diophantine equation $x^2 + 26y^2 = 3$ that does not admit any solutions $x, y \in \mathbf{Z}$ with $y \neq 0$. Finally we notice that the six ideal classes are the classes of O_F, $\mathfrak{p}_3$, $\mathfrak{p}_3]$, $\mathfrak{p}_2$, $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3'$. The two ideals $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ are contained in the classes of $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3'$ respectively.

Example 10.4. $F = \mathbf{Q}(\sqrt{105})$.

The field F is an *real quadratic* field. It admits two embeddings σ and σ' into $\mathbf{R}$. This implies that $r_1 = 2$ and $r_2 = 0$. The Arakelov class group fits therefore in an exact sequence

$$0 \longrightarrow (\mathbf{R} \times \mathbf{R})^0 / \mathrm{im}(O_F^*) \longrightarrow \mathrm{Pic}_F^0 \longrightarrow Cl_F \longrightarrow 0.$$

Here $(\mathbf{R} \times \mathbf{R})^0$ is the one dimensional vector space $\{(x, -x) : x \in \mathbf{R}\}$ and by $\mathrm{im}(O_F^*)$ we denote the discrete subgroup of elements of the form $(-\log|\sigma(u)|, -\log|\sigma'(u)|)$ where $u \in O_F^*$. As a Riemannian manifold, Pic_F^0 is a finite union of circles having the same circumference.

Since $105 \equiv 1 \pmod 4$, the ring of integers of F is equal to $\mathbf{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{105}}{2}$. The minimum polynomial of α is given by $f(T) = T^2 - T - 26$ and the discriminant of F is

equal to the discriminant of $f(T)$ which in turn is equal to 105. We observe that the only ramified primes are 3, 5 and 7. Let $\mathfrak{p}_3 = (3, \alpha+1)$, $\mathfrak{p}_5 = (5, \alpha+2)$ and $\mathfrak{p}_7 = (7, \alpha+3)$ denote the unique primes of norm 3,5 and 7 respectively. We have that $\mathfrak{p}_3^2 = (3)$, $\mathfrak{p}_5^2 = (5)$ and $\mathfrak{p}_7^2 = (7)$. Since $f(T) \equiv T(T+1) \pmod 2$, the ring $O_F/(2)$ is isomorphic to a a product of two finite fields of order 2. Therefore $2 = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2 = (2, \alpha)$ and $\mathfrak{p}_2' = (2, \alpha+1)$ are two distinct prime ideals of norm 2. By Theorem 9.3, the group Pic_F^0 can be covered by open intervals of the form (J^{-1}, u) where $J \subset O_F$ is an ideal of norm $N(J)$ at most $\sqrt{105} = 10.2469\ldots$ and $\log|u_\sigma|$, $\log|u_\sigma| \le \frac{1}{2}\log\sqrt{105} = 1.16\ldots$. In particular, the ideal class group Cl_F is generated by the prime ideals in the set $P = \{\mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7\}$. This implies that there is an isomorphism

$$\mathrm{Pic}_F^0 \quad \cong \quad \left(\bigoplus_{\mathfrak{p} \in P} \mathbf{Z} \times \mathbf{R} \times \mathbf{R} \right)^0 / \mathrm{Princ}(P)$$

where $\mathrm{Princ}(P)$ denotes the subgroup of principal divisors that are supported in the set P and the two infinite primes. Next we search for elements in $\mathrm{Pr}(P)$ by factoring principal ideals of O_F. As in the previous example, we consider elements of the form $\alpha - k$ with $k \in \mathbf{Z}$, because by Exer. 3.5 their norms are equal to $k^2 - k - 26$ and are easy to compute. We take k close to the zero $\frac{1+\sqrt{105}}{2} = 5.6234\ldots$ of $f(T) = T^2 - T - 26$.

Table 10.5.

	k	$f(k) = k^2 - k - 26$	$(\alpha - k)$
(i)	3	$-20 = -2^2 \cdot 5$	$\mathfrak{p}_2'^{\,2}\mathfrak{p}_5$
(ii)	4	$-14 = -2 \cdot 7$	$\mathfrak{p}_2\mathfrak{p}_7$
(iii)	5	$-6 = -2 \cdot 3$	$\mathfrak{p}_2'\mathfrak{p}_3$
(iv)	6	$4 = 2^2$	$\mathfrak{p}_2^2$
(v)	7	$16 = 2^4$	$\mathfrak{p}_2'^{\,4}$
(vi)	8	$30 = 2 \cdot 3 \cdot 5$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$

Table 10.6.

	x	$\mathfrak{p}_2$	$\mathfrak{p}_2'$	$\mathfrak{p}_3$	$\mathfrak{p}_5$	$\mathfrak{p}_7$	σ	σ'
	2	1	1	0	0	0	$-\log 2$	$-\log 2$
	3	0	0	2	0	0	$-\log 3$	$-\log 3$
	5	0	0	0	2	0	$-\log 5$	$-\log 5$
	7	0	0	0	0	2	$-\log 7$	$-\log 7$
(i)	$\alpha - 3$	0	2	0	1	0	$-\log\lvert\frac{-5+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-5-\sqrt{105}}{2}\rvert$
(ii)	$\alpha - 4$	1	0	0	0	1	$-\log\lvert\frac{-7+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-7-\sqrt{105}}{2}\rvert$
(iii)	$\alpha - 5$	0	1	1	0	0	$-\log\lvert\frac{-9+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-9-\sqrt{105}}{2}\rvert$
(iv)	$\alpha - 6$	2	0	0	0	0	$-\log\lvert\frac{-11+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-11-\sqrt{105}}{2}\rvert$
(v)	$\alpha - 7$	0	4	0	0	0	$-\log\lvert\frac{-13+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-13-\sqrt{105}}{2}\rvert$
(vi)	$\alpha - 8$	1	0	1	1	0	$-\log\lvert\frac{-15+\sqrt{105}}{2}\rvert$	$-\log\lvert\frac{-15-\sqrt{105}}{2}\rvert$

In Table 10.6 we list the ten principal Arakelov divisors that correspond to the six entries of Table 10.5 plus the four 'trivial' factorizations $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ and $(p) = \mathfrak{p}_p^2$ for $p = 3$, 5 and 7. They happen all to be supported in the set $\mathrm{Princ}(P)$ mentioned above. The row corresponding to an element x contains the coefficients $n_\mathfrak{p}$ and x_σ of the principal divisor (x).

These principal divisors lead to relations between the generators of Pic_F^0. In this way we can eliminate some of the generators. More precisely, the principal divisors (ii), (i) and (iii) express $\mathfrak{p}_7$, $\mathfrak{p}_5$ and $\mathfrak{p}_3$ in terms of $\mathfrak{p}_2$, $\mathfrak{p}_2'$ and the infinite primes in Pic_F^0. Similarly, the principal divisor (2) expresses $\mathfrak{p}_2'$ in terms of $\mathfrak{p}_2$ and the infinite primes. We apply the Gaussian elimination method. First eliminate $\mathfrak{p}_7$: subtract relation (ii) twice from the fourth row and then omit it. Eliminate $\mathfrak{p}_5$: subtract relation (i) once from relation (vi) and twice from the third row. Then omit it. In a similar way one eliminates the primes $\mathfrak{p}_3$ and $\mathfrak{p}_2'$. Of course, in the x column one multiplies and divides rather than adds and subtracts.

This leads to the following list of six principal divisors supported in $\mathfrak{p}_2$, σ and σ'. The numbers in the last column are merely approximations.

Table 10.7.

x	$\mathfrak{p}_2$	σ	σ'
$12/(\alpha-5)^2$	2	-3.4298	2.0435
$80/(\alpha-3)^2$	4	-2.4530	-0.3196
$7/(\alpha-4)^2$	-2	-0.9768	2.3631
$\alpha-6$	2	0.9768	-2.3631
$(\alpha-7)/16$	-4	2.4530	0.3196
$8(\alpha-8)/(\alpha-3)(\alpha-5)$	4	-2.4530	-0.3196

There is an isomorphism

$$\mathrm{Pic}_F^0 \quad \cong \quad (\mathbf{Z}\times\mathbf{R}\times\mathbf{R})^0\,/\mathrm{Pr}(P')$$

where the factor $\mathbf{Z}$ corresponds to the prime $\mathfrak{p}_2$ and $\mathrm{Pr}(P')$ denotes the group of principal divisors that are supported in $\mathfrak{p}_2$, σ and σ'. In particular, the class group Cl_F is generated by $\mathfrak{p}_2$. In the $\mathfrak{p}_2$-column all entries are even. This means that we cannot eliminate $\mathfrak{p}_2$. If we were to search for additional relations, we would continue to find even entries in the $\mathfrak{p}_2$-column.

Table 10.8.

x	σ	σ'
$12/(\alpha-5)^2(\alpha-6)$	-4.4066	4.4066
$80/(\alpha-3)^2(\alpha-6)^2$	-4.4066	4.4066
$7(\alpha-6)/(\alpha-4)^2$	0	0
$(\alpha-7)(\alpha-6)^2/16$	4.4066	-4.4066
$8(\alpha-8)/(\alpha-6)^2(\alpha-3)(\alpha-5)$	-4.4066	4.4066

We proceed as follows. The fourth row of Table 10.6 says that $\mathfrak{p}_2^2 = (\alpha - 6)$. Therefore the ideal class group Cl_F has order at most 2. Before showing that $Cl_F \cong \mathbf{Z}/2\mathbf{Z}$, we perform Gaussian elimination with the fourth row and obtain Table 10.8: a list of Arakelov divisors (x) that are supported in the infinite primes. All elements x in this table are units of O_F. The element in the third row is equal to ± 1 because both coefficients at the infinite primes vanish. Looking at the other entries in the last two columns, one sees that the corresponding units are equal to $\pm\varepsilon^{\pm 1}$ for some unit ε. Using the fact that $\alpha^2 - \alpha - 12 = 0$, we simplify the expression for the unit in the fourth row.

$$\varepsilon = \frac{(\alpha - 7)(\alpha - 6)^2}{16} = \frac{128\alpha - 720}{16} = 8\alpha - 45 = -41 + 4\sqrt{105}.$$

If we were to search for any additional units, we would continue to find the same unit ε or powers of it. Therefore we suspect that the unit group O_F^* is actually generated by ε and -1.

Class group computation. Before determining the unit group, we come back to the issue of whether the class group is trivial or isomorphic to $\mathbf{Z}/2\mathbf{Z}$. We suspect that Cl_F is not trivial. Suppose the contrary is true. Then $\mathfrak{p}_2 = (\beta)$ for some $\beta \in O_F^*$. The Diophantine equation that expresses the fact that β has norm 2 is

$$x^2 - 26y^2 = \pm 2, \qquad \text{for } x, y \in \mathbf{Z},$$

is not so easy to solve as in the previous example. We proceed in a different way. Since $\mathfrak{p}_2^2 = (\alpha - 6)$, we would have that β^2 is equal to $\alpha - 6$ times a unit $u \in O_F^*$. We suspect that O_F^* is generated by $\varepsilon = -41 + 4\sqrt{105}$ and -1, so that we would have that

$$(\alpha - 6)(-1)^l \varepsilon^m \quad \text{is a square for some } l, m \in \mathbf{Z}. \qquad (*)$$

The multiplicative group U generated by $\alpha - 6$, -1 and ε *modulo squares* is a vector space over $\mathbf{F}_2$. We now show that its dimension is equal to 3. This implies first of all that -1 and ε generate O_F^* modulo squares. But then the hypothetical unit u above is actually equal to $(-1)^l \varepsilon^m$ times a square. This means that we the relation (*) actually would hold. However, if U has dimension 3 this is impossible.

To show that U has dimension 3, we construct a homomorphism to a suitable explicit vector space V over $\mathbf{F}_2$ and compute the image. We put

$$V = (\mathbf{R}^*/\mathbf{R}^{*2}) \times (\mathbf{R}^*/\mathbf{R}^{*2}) \times (O_F/\mathfrak{p}_3)^* \times (O_F/\mathfrak{p}_5)^*/(O_F/\mathfrak{p}_5)^{*2}.$$

This is a vector space of dimension 4 over $\mathbf{F}_2$. The homomorphism $U \longrightarrow V$ is given by $u \mapsto (\sigma(u), \sigma'(u), u \pmod{\mathfrak{p}_3}, u \pmod{\mathfrak{p}_5})$. It so happens that all three elements $\alpha - 6$, -1 and ε have the property that their images under σ and σ' are all negative. The element -1 is a square modulo $\mathfrak{p}_5$ bot not modulo $\mathfrak{p}_3$. The unit $\varepsilon = -41 + 4\sqrt{105}$ is congruent to 1 (mod 3) and congruent to -1 (mod 5). Therefore it is a square modulo both primes. Finally $\alpha - 6$ is not a square modulo any of them. Identifying V with $\mathbf{F}_2^4$ in the obvious way, the image of U is therefore spanned by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Since the rank of this matrix is 3 over $\mathbf{F}_2$, the dimension of U is equal to 3. We conclude that Cl_F has order 2 as required.

Unit group computation. Next we show that -1 and ε generate O_F^*. Since we already know that this is so modulo squares, we must have that

$$\varepsilon = \pm\eta^k, \qquad \text{for some integer } k \geq 3$$

if -1 and ε do not generate O_F^*. This implies that

$$|\sigma(\eta)| \leq |\sigma(\varepsilon)|^{1/3} = 4.3442\ldots,$$
$$|\sigma'(\eta)| \leq |\sigma'(\varepsilon)|^{1/3} = 0.2302\ldots,$$

Writing $\eta = x + y\alpha$ for some $x, y \in \mathbf{Z}$ we have that $\|\eta\|^2 = (x + y\sigma(\alpha))^2 + (x + y\sigma'(\alpha))^2 = 2x^2 + 2xy + 53y^2$. It follows that

$$2x^2 + 2xy + 53y^2 = \|\eta\|^2 \leq (4.3442\ldots)^2 + (0.2302\ldots)^2 = 18.9256\ldots$$

However it follows easily by completing the square of the quadratic form that necessarily $y = 0$, so that $\eta \in \mathbf{Z}$ which is absurd. We conclude that O_F^* is generated by -1 and ε.

The group Pic_F^0 is therefore isomorphic to

$$(\mathbf{Z} \times \mathbf{R} \times \mathbf{R})^0 / \langle v_1, v_2 \rangle$$

where

$$v_1 = (2, -\ln|(-11 + \sqrt{105})/2|, -\ln|(-11 - \sqrt{105})/2|),$$
$$v_2 = (0, -\ln|-41 + 4\sqrt{105}|, -\ln|-41 - 4\sqrt{105}|).$$

Its volume is equal to $2\sqrt{2} \cdot \ln|41 + 4\sqrt{105}| = 12.4636\ldots$. Finally we project the group $(\mathbf{Z} \times \mathbf{R} \times \mathbf{R})^0$ on its first two coordinates. This simplifies the presentation:

$$\mathrm{Pic}_F^0 \cong (\mathbf{Z} \times \mathbf{R}) / \langle w_1, w_2 \rangle,$$

with

$$w_1 = (2, -\ln|(-11 + \sqrt{105})/2|),$$
$$w_2 = (0, -\ln|-41 + 4\sqrt{105}|).$$

The topological group Pic_F^0 consists of two circles Putting $R = \log|41 + 4\sqrt{105}|$, these are the connected component of identity $\{(0, y) : y \in \mathbf{R}/R\mathbf{Z}\}$ and its non-trivial coset $\{(1, y) : y \in \mathbf{R}/R\mathbf{Z}\}$.

Covering the Arakelov class group. We now verify that Pic_F^0 is covered by simplices of the form (J^{-1}, v) where $J \subset O_F$ is an ideal of norm at most $\sqrt{105} = 10.2\ldots$ and v has the property that $\log|v_\sigma|$ and $\log|v_{\sigma'}|$ are at most $\frac{1}{4}\log(105) = 1.16\ldots$. The simplices are 1-dimensional intervals in this case. We show that the intervals associated to the ideals J of norm at most 7 already suffice to cover Pic_F^0. There are ten such ideals.

It follows from the factorizations in Table 10.4 that for the ideals $J = O_F$, (2), $\mathfrak{p}_2^2$ and $\mathfrak{p}_2'^2$, $\mathfrak{p}_5$, $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2'\mathfrak{p}_3$ the simplex (J^{-1}, v) is contained in the connected component of the identity of Pic_F^0. On this component we choose, in the notation of section 9, $I = O_F$. The elements β for which $I = \beta_J$ are listed in the second column of Table 10.8. It is convenient to project the intervals on the first coordinate of $T^0 = (\oplus_\sigma \mathbf{R})^0$. The third column contains the center $\log|\frac{\beta}{N(\beta)^{1/n}}$ of the intervals and the fourth column contains the endpoints $\log|\frac{\beta}{N(\beta)^{1/n}}| \pm \frac{1}{n}\log(\frac{\sqrt{\Delta}}{N(J)})$.

Table 10.9.

J	β^{-1}	center	simplex
O_F	1	0	$(-1.163,\ \ 1.163)$
$\mathfrak{p}_2^2$	$\frac{11-\sqrt{105}}{2}$	$\log\lvert\frac{4}{11-\sqrt{105}}\rvert = \ \ 1.670$	$(1.199,\ \ 2.140)$
$\mathfrak{p}_2'^2$	$\frac{11+\sqrt{105}}{2}$	$\log\lvert\frac{4}{11+\sqrt{105}}\rvert = -1.670$	$(-2.140, -1.199)$
(2)	2	0	$(-0.470,\ \ 0.470)$
$\mathfrak{p}_5$	$10-\sqrt{105}$	$\log\lvert\frac{\sqrt{5}}{10-\sqrt{105}}\rvert = \ \ 2.203$	$(1.845,\ \ 2.562)$
$\mathfrak{p}_2\mathfrak{p}_3$	$\frac{9+\sqrt{105}}{2}$	$\log\lvert\frac{2\sqrt{6}}{9+\sqrt{105}}\rvert = -1.368$	$(-1.636, -1.101)$
$\mathfrak{p}_2'\mathfrak{p}_3$	$\frac{9-\sqrt{105}}{2}$	$\log\lvert\frac{2\sqrt{6}}{9-\sqrt{105}}\rvert = \ \ 1.368$	$(1.101,\ \ 1.636)$

On the other component we choose $I = \mathfrak{p}_3$ and the divisor $(\mathfrak{p}_3^{-1}, \sqrt{3})$ as our point of reference. Recall that both cosets are circles with circumference equal to $R = 41+4\sqrt{105} = 4.4065\ldots$ The reader easily checks from the data in the tables that both circles are covered by the intervals listed in the fourth column.

Table 10.10.

J	β^{-1}	center	simplex
$\mathfrak{p}_3$	1	0	$(-1.228,\ \ 1.228)$
$\mathfrak{p}_2$	$\frac{9+\sqrt{105}}{6}$	$\log\lvert\frac{2\sqrt{6}}{9+\sqrt{105}}\rvert = -1.368$	$(-2.185, -0.551)$
$\mathfrak{p}_2'$	$\frac{9-\sqrt{105}}{6}$	$\log\lvert\frac{2\sqrt{6}}{9-\sqrt{105}}\rvert = \ \ 1.368$	$(0.551,\ \ 2.185)$
$\mathfrak{p}_7$	$\frac{21-2\sqrt{105}}{6}$	$\log\lvert\frac{\sqrt{21}}{21-2\sqrt{105}}\rvert = \ \ 2.203$	$(2.012,\ \ 2.394)$

Exercises.

10.1 Compute the ideal class group $Cl(O_F)$ and the unit group O_F^* for the number fields $F = \mathbf{Q}(\sqrt{d})$ for $d = -47$, -71, -163 and -147.

10.2 Compute the ideal class group $Cl(O_F)$and the unit group O_F^* for the number fields $F = \mathbf{Q}(\sqrt{d})$ for $d = 19$, 145, 46 and 200.

11. The Riemann-Roch Theorem.

The main result of this section is Theorem 11.4. At the end of the section we explain why it should be viewed as the arithmetic analogue of the Riemann-Roch theorem.

Definition. Let F be a number field. Let $D = (I, u)$ be an Arakelov divisor. Then we put

$$h^0(D) = \log\left(\sum_{y \in uI} e^{-\pi\|y\|^2}\right).$$

We have that $h^0(D) \in \mathbf{R}_{>0}$. Since $h^0(D)$ only depends on the lattice $uI \subset F_{\mathbf{R}}$ associated to D. By Prop. 8.1 lattices associated to equivalent divisors are isometric. Therefore the map $D \mapsto h^0(D)$ induces a well defined function on the quotient group Pic_F. We

Lemma 11.1. *Let F be a number field of degree n and let $D = (I, u)$ be an Arakelov divisor. Let λ denote the length of the shortest non-zero vector in the ideal lattice uI. Then*

$$\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi\|y\|^2} \leq \pi \int_{\lambda^2}^{\infty} (1 + \tfrac{2\sqrt{t}}{\lambda})^n e^{-\pi t} dt.$$

Proof. We have that

$$\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi\|y\|^2} = \sum_{\substack{y \in uI \\ y \neq 0}} \int_{\|y\|^2}^{\infty} \pi e^{-\pi t} dt \leq \pi \int_{\lambda^2}^{\infty} \#B_t e^{-\pi t} dt,$$

where $B_t = \{y \in uI : \|y\|^2 \leq t\}$. The balls with centers in $y \in B_t$ and radius $\lambda/2$ are disjoint. Their union is contained in a ball with center 0 and radius $\sqrt{t} + \lambda/2$. Therefore

$$(\frac{\lambda}{2})^n \#B_t \leq (\sqrt{t} + \lambda/2)^n$$

and hence $\#B_t \leq (1 + \frac{2\sqrt{t}}{\lambda})^n$. This implies the lemma.

Proposition 11.2. *Let F be a number field of degree n and let D be an Arakelov divisor. Then*

(i)

$$h^0(D) \leq \deg(D) + 1, \qquad \text{when } \deg(D) \geq 0;$$

(ii)

$$h^0(D) \leq e^{h^0(D)} - 1 \leq 2 \cdot 3^n \cdot \exp\left(-\pi n e^{-\frac{2}{n}\deg(D)}\right), \qquad \text{when } \deg(D) \leq 0.$$

Proof. *(i)* We use the lemma and the fact that $1 + \frac{2\sqrt{t}}{\lambda} \leq \frac{3\sqrt{t}}{\lambda}$ for $t \geq \lambda^2$. This leads to

$$\begin{aligned}\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi\|y\|^2} &\leq \pi \int_{\lambda^2}^{\infty} \left(3\frac{\sqrt{t}}{\lambda}\right)^n e^{-\pi t} dt = \int_{\frac{\lambda^2}{\pi}}^{\infty} \left(3\frac{\sqrt{x}}{\sqrt{\pi}\lambda}\right)^n e^{-x} dx, \\ &\leq \frac{3^n}{\pi^{n/2}\lambda^n} \int_0^{\infty} x^{n/2} e^{-x} dx = \frac{3^n \Gamma(\frac{n}{2} - 1)}{\pi^{n/2}} \lambda^{-n}.\end{aligned}$$

Here Γ denotes the Gamma function. See Exer 11.3. Since λ satisfies $\lambda \geq \sqrt{n}N(D)^{-1/n}$ we find that

$$\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi \|y\|^2} \leq \frac{3^n \Gamma(\frac{n}{2} - 1)}{\pi^{n/2} n^{n/2}} N(D) \leq \tfrac{3}{2} N(D).$$

Since $\deg(D) \geq 0$, this implies that

$$h(D) \leq \log(1 + \tfrac{3}{2}N(D)) \leq \log(N(D)) + 1 = \deg(D) + 1,$$

as required.
(ii) The first inequality is clear. For the second we use the estimate of the lemma together with the the rough estimate $1 + 2(t/\lambda^2)^{1/2} \leq 3^{t/\lambda^2}$ for $t \geq \lambda^2$. This leads to

$$\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi \|y\|^2} \leq \pi \int_{\lambda^2}^{\infty} 3^{nt/\lambda^2} e^{-\pi t} dt = \frac{\pi e^{n \log(3) - \pi \lambda^2}}{\pi - n \log(3)/\lambda^2}.$$

Since $\deg(D) \leq 0$ we have that $\lambda^2 \geq n$ and hence

$$\sum_{\substack{y \in uI \\ y \neq 0}} e^{-\pi \|y\|^2} \leq \frac{\pi 3^n}{\pi - \log(3)} e^{-\pi \lambda^2}.$$

The result now follows from the estimate for λ provided by the lemma.

By section 4, the $\mathbf{Z}$-dual of the lattice uI associated to an Arakelov divisor $D = (I, u)$ is the lattice

$$\{y \in F_{\mathbf{R}} : \mathrm{Tr}(y\overline{z}) \in \mathbf{Z} \text{ for all } z \in I\} \quad \subset \quad F_{\mathbf{R}}.$$

It is in general not an ideal lattice because multiplication by O_F does not map $\overline{I}$ to itself. However the conjugate of the $\mathbf{Z}$-dual is. It is given by

$$\overline{uI}^{\vee} = \{y \in F_{\mathbf{R}} : \mathrm{Tr}(yz) \in \mathbf{Z} \text{ for all } z \in I\}.$$

Definition. Let F be a number field. The *canonical divisor class* κ of F is the divisor class corresponding to the ideal lattice $\overline{O_F}^{\vee}$.

The ideal lattice

$$\kappa = \{y \in F_{\mathbf{R}} : \mathrm{Tr}(yz) \in \mathbf{Z} \text{ for all } z \in O_F\}$$

contains O_F and is contained in $\frac{1}{|\Delta_F|} O_F$. The second inclusion follows by choosing a $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ for O_F and writing $z = \lambda_1 \omega_1 + \ldots + \lambda_n \omega_n$ with $\lambda_i \in \mathbf{R}$. The conditions $\mathrm{Tr}(yz) \in \mathbf{Z}$ for $z = \omega_i$ lead to a linear system with coefficient matrix $(\mathrm{Tr}(\omega_i \omega_j))$. By Cramer's rule, the solutions λ_i are rational numbers with denominators dividing $\Delta_F = \det(\mathrm{Tr}(\omega_i \omega_j))$.

Therefore κ is the ideal lattice associated to the divisor $(\partial^{-1}, 1)$ where $\partial \subset O_F$ is the *different* of F. It is the inverse of the fractional ideal $\{y \in F : \mathrm{Tr}(yz) \in \mathbf{Z} \text{ for all } z \in O_F\}$. We often call $(\partial^{-1}, 1)$ itself the canonical divisor and denote it by κ.

Proposition 11.3. *Let F be a number field with canonical divisor κ. Then*

(i) $\deg(\kappa) = \log|\Delta_F|$ *and* $N(\partial) = |\Delta|$.

(ii) Let $D = (I, u)$ be an Arakelov divisor. Then the Arakelov divisor class corresponding to the ideal lattice $\overline{uI}^\vee$ is $\kappa - D$.

(iii) There is an isomorphism of O_F-modules $\Omega^1_{O_F/\mathbf{Z}} \cong O_F/\partial$.

Proof. The covolume of κ is equal to $1/\mathrm{covol}(O_F) = |\Delta_F|^{-1/2}$. Since $\mathrm{covol}(\kappa) = e^{-\deg(\kappa)}\sqrt{|\Delta_F|}$, part *(i)* follows. The ideal lattice associated to the divisor $\kappa - D$ is given by $u^{-1}\partial^{-1}I^{-1}$. It is contained in $\overline{uI}^\vee$ because $\mathrm{Tr}(u^{-1}xyuz) \in \mathbf{Z}$ for all $x \in \partial^{-1}$, $y \in I^{-1}$ and $z \in I$. On the other hand, by Prop 5.5 the covolume of the lattice associated to $\kappa - D$ is $e^{-\deg(\kappa - D)}\sqrt{|\Delta_F|}$ which by part *(i)* is equal to $1/\mathrm{covol}(D)$. This proves the proposition.

Theorem 11.4. *(Riemann-Roch) Let F be a number field. Then for every Arakelov divisor D we have that*

$$h^0(D) - h^0(\kappa - D) = \deg(D) - \tfrac{1}{2}\log|\Delta_F|.$$

Proof. Since the ideal lattice associated to $\kappa - D$ is the conjugate of the dual of the lattice associated to $D = (I, U)$, an application of the Poisson summation formula of Thm. 4.3 to the lattice uI gives us that

$$\sum_{y \in uI} e^{-\pi\|y\|^2} = \frac{1}{\mathrm{covol}(D)} \sum_{y \in u^{-1}\partial^{-1}I^{-1}} e^{-\pi\|y\|^2}.$$

Taking logarithms gives the required result.

In the remainder of this section we explain why Theorem 11.4is analogous to the Riemann-Roch Theorem for algebraic curves. First we introduce the analogue of the geometric notion of an *effective* divisor D on a curve. The corresponding arithmetic notion $\mathrm{eff}(D)$ is a real number between 0 and 1. It varies continuously in the coefficients of the infinite primes in the support of D. If $\mathrm{eff}(D)$ is 0 or close to zero, D should be thought of as being not effective or 'close to being not effective'. On the other hand, if $\mathrm{eff}(D)$ is close to 1, the divisor D is close to being effective.

Definition. Let F be a number field. The *effectivity* $\mathrm{eff}(D)$ of an Arakelov divisor $D = (I, u)$ is defined as

$$\mathrm{eff}(D) \quad = \quad \begin{cases} e^{-\pi\|u\|^2}; & \text{if } O_F \subset I, \\ 0; & \text{otherwise.} \end{cases}$$

If $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma\sigma$, the condition that $O_F \subset I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ means precisely that all coefficients $n_{\mathfrak{p}}$ are non-negative.

We have that

$$e^{-\pi\|u\|^2} = \exp\left(-\pi \sum_\sigma \deg(\sigma) e^{-2x_\sigma}\right)$$

and this shows that the effectivity function behaves in a way that is analogous to the geometric function. Indeed, if $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$ is a divisor and we have that $n_{\mathfrak{p}} < 0$ for some prime $\mathfrak{p}$, then $\mathrm{eff}(D) = 0$. If all $n_{\mathfrak{p}}$ are non-negative, but at least one coeffient x_σ is negative, the exponential e^{-2x_σ} is large and so is the sum $\sum_\sigma \deg(\sigma) e^{-2x_\sigma}$. Therefore $\mathrm{eff}(D)$ is a small positive number. The more negative x_σ becomes, the closer it gets to 0. Conversely, if $n_{\mathfrak{p}} \geq 0$ for all $\mathfrak{p}$ and the coefficients x_σ are positive, than the exponents e^{-2x_σ} are all small, so that $\mathrm{eff}(D)$ is close to 1. The larger the coefficients x_σ become, the closer the effectivity $\mathrm{eff}(D)$ is to 1.

Definition. Let F be a number field. Let $D = (I, u)$ be an Arakelov divisor. Then we put

$$H^0(D) = \{x \in F^* : \mathrm{eff}(D + (x)) > 0\} \cup \{0\}.$$

We have that $\mathrm{eff}(D + (x)) > 0$ if and only if $O_F \subset I$. Since this is precisely the case when $x \in I$, the set $H^0(D)$ is equal to the ideal I. We view $H^0(D)$ as being analogous to the space of sections of the line bundle associated to the divisor on an algebraic curve. In order to measure the size of $H^0(D)$ in some way, we weight its elements x by the effectivity $\mathrm{eff}(D + (x))$ of the divisor $D + (x)$ to which they give rise. Since $D + (x) = (x^{-1}I, |x|u)$ we have that

$$\mathrm{eff}(D + (x)) = e^{-\pi \|xu\|^2}.$$

The logarithm of the sum of all these 'effectivities' should be viewed as some kind of *dimension* of $H^0(D)$. Adding 1 for the contribution of $0 \in I$ we recover the definition of $h^0(D)$ given above.

$$h^0(D) = \log\left(1 + \sum_{\substack{x \in I \\ x \neq 0}} e^{-\pi \|xu\|^2}\right) = \log\left(\sum_{y \in uI} e^{-\pi \|y\|^2}\right).$$

The canonical divisor class κ defined above is the analogue of the canonical divisor κ_X of an algebraic curve X. We briefly explain why. In the geometric situation, the degree of the canonical divisor is equal to $2g-2$, where g is the genus of X. The functional equation of the zeta function $Z_X(s)$ and algebraic curve X over $\mathbf{F}_q$ can be expressed by saying that the function

$$q^{(g-1)s} Z_X(s)$$

is invariant under the substitution $s \leftrightarrow 1 - s$. In Chapter 12 it is shown that the zeta function$Z_F(s)$ of a number field F has the property that $|\Delta_F|^{s/2} Z_F(s)$ is invariant under the substitution $s \leftrightarrow 1 - s$. Therefore the analogue of $g - 1$ is $\frac{1}{2}\log|\Delta_F|$. This means that for $F = \mathbf{Q}$, the degree of κ must be zero. In section 7 we saw that the degree map induces an isomorphism $\mathrm{Pic}^0_{\mathbf{Q}} \cong \mathbf{R}$. Therefore we put $\kappa = 0$ for the number field $\mathbf{Q}$. The Riemann-Hurwitz formula says that for a finite cover $\pi : Y \longrightarrow X$ of curves we have that $\kappa_Y = \pi^* \kappa_X + \delta_{Y/X}$, where $\delta_{Y/X}$ denotes the different. The arithmetic analogue of this formula for $\pi : \mathrm{Spec}(O_F) \longrightarrow \mathbf{Z}$ leads to our definition of the canonical divisor.

Exercises.

11.1 Let $D = (I, u)$ be an Arakelov divisor associated to a number field F. Show that $(\overline{uI})^\vee = \overline{(uI^\vee)}$. Show that $\overline{uI}^\vee$ is an O_F-submodule of $F_{\mathbf{R}}$.

12. Zeta functions.

In this section we discuss the zeta functions associated to number fields. We derive their functional equations and determine their residues in $s = 1$.

Definition. The *Riemann zeta function* $\zeta(s)$ is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \text{for } s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 1.$$

By comparing $\zeta(s)$ to the integral $\int_1^\infty \frac{dx}{x^s}$ it follows easily that $\zeta(s)$ converges absolutely and uniformly on compact subsets of $\{s \in \mathbf{C} : \mathrm{Re}(s) > 1\}$.

Proposition 12.1. *We have that*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}, \qquad \textit{for } s \in \mathbf{C} \textit{ with } \mathrm{Re}(s) > 1.$$

More precisely, the product converges absolutely and its limit is $\zeta(s)$.

Proof. Let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. We take the logarithm of the absolute value of the product. Since $|1 - p^{-s}| = 1 - p^{-\mathrm{Re}(s)}|$, this gives

$$\sum_{p \text{ prime}} \log\left(1 - \frac{1}{p^{\mathrm{Re}(s)}}\right) \leq \sum_{p \text{ prime}} \left(\frac{1}{p^{\mathrm{Re}(s)}} + \frac{1}{2p^{2\mathrm{Re}(s)}} + \dots\right)$$
$$\leq \sum_{p \text{ prime}} \frac{1}{p^{\mathrm{Re}(s)} - 1} \leq \sum_{n=2}^{\infty} \frac{1}{n^{\mathrm{Re}(s)} - 1}.$$

Comparing the latter sum to the integral $\int_2^\infty \frac{dx}{x^{\mathrm{Re}(s)-1}}$ shows that the product converges absolutely when $\mathrm{Re}(s) > 1$. To show that the limit is $\zeta(s)$, we consider the partial products. Since every integer $n > 0$ is a product of prime numbers in a unique way, for every $n < M$ there is exactly one term n^{-s} in

$$\prod_{p<M} \frac{1}{1 - p^{-s}} = \prod_{p<M} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) = \sum_{\substack{n \text{ is product} \\ \text{of primes } p < M}} \frac{1}{n^s}.$$

Therefore

$$\left| \prod_{p<M} \frac{1}{1 - p^{-s}} - \zeta(s) \right| \leq \sum_{n \geq M} \frac{1}{n^{\mathrm{Re}(s)}},$$

which tends to zero as $M \to \infty$, because the sum converges absolutely. This proves the proposition.

Definition. The *Dedekind zeta function* $\zeta_F(s)$ is defined as

$$\zeta_F(s) = \sum_{0 \neq I \subset O_F} \frac{1}{N(I)^s}, \qquad \text{for } s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 1.$$

Here I runs over the non-zero ideals of O_F.

The convergence of $\zeta_F(s)$ is guaranteed by the next proposition.

Proposition 12.2. *Let F be a number field. For every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$ we have that*

$$\zeta_F(s) = \sum_{0 \neq I \subset O_F} \frac{1}{N(I)^s} = \prod_{0 \neq \mathfrak{p} \subset O_F} \frac{1}{1 - N(\mathfrak{p})^{-s}}.$$

(the product runs over the non-zero prime ideals of O_F). Both product and sum converge absolutely and uniformly on compact subsets of $\{s \in \mathbf{C} : \mathrm{Re}(s) > 1\}$ and the limits are equal.

Proof. By Prop. 6.5 we have for every prime number p that

$$(p) = \prod_{\mathfrak{p} | p} \mathfrak{p}^{e_\mathfrak{p}}$$

and that $\sum_{\mathfrak{p}|p} e_\mathfrak{p} f_\mathfrak{p} = n = [F : \mathbf{Q}]$. Here $f_\mathfrak{p}$ is the degree of the finite field $O_F/\mathfrak{p}$ over $\mathbf{F}_p$. In other words, $N(\mathfrak{p}) = p^{f_\mathfrak{p}}$. Since $e_\mathfrak{p}$ and $f_\mathfrak{p}$ are at least 1, we see that $N(\mathfrak{p}) \geq p$ and that (p) admits at most n distinct prime divisors $\mathfrak{p}$. Therefore

$$\begin{aligned}
\log \left| \prod_{0 \neq \mathfrak{p} \subset O_F} \frac{1}{1 - N(\mathfrak{p})^{-s}} \right| &= \sum_{0 \neq \mathfrak{p} \subset O_F} -\log(1 - N(\mathfrak{p})^{-\mathrm{Re}(s)}), \\
&= \sum_{0 \neq \mathfrak{p} \subset O_F} \left(\frac{1}{N(\mathfrak{p})^{\mathrm{Re}(s)}} + \frac{1}{2N(\mathfrak{p})^{2\mathrm{Re}(s)}} + \dots \right), \\
&\leq \sum_{0 \neq \mathfrak{p} \subset O_F} \frac{1}{N(\mathfrak{p})^{\mathrm{Re}(s)} - 1} = \sum_{p \text{ prime}} \sum_{\mathfrak{p} | p} \frac{1}{N(\mathfrak{p})^{\mathrm{Re}(s)} - 1}, \\
&\leq \sum_{p \text{ prime}} \frac{n}{p^{\mathrm{Re}(s)} - 1} \leq \sum_{m \geq 2} \frac{n}{m^{\mathrm{Re}(s)} - 1}.
\end{aligned}$$

Comparing with the integral $\int_2^\infty \frac{dx}{x^{\mathrm{Re}(s)-1}}$, it follows that the product converges absolutely when $\mathrm{Re}(s) > 1$. By Thm. 2.3 every non-zero ideal of the Dedekind ring O_F is a product of prime ideals in a unique way. It follows that

$$\sum_{N(I) < M} N(I)^{-\mathrm{Re}(s)} \leq \prod_{0 \neq \mathfrak{p} \subset O_F} \frac{1}{1 - N(\mathfrak{p})^{-\mathrm{Re}(s)}}$$

Therefore the series converges absolutely when $\mathrm{Re}(s) > 1$. The infinite product converges to the *same* limit because

$$\left| \sum_{0 \neq I \subset O_F} \frac{1}{N(I)^s} - \prod_{N(\mathfrak{p}) < M} \frac{1}{1 - N(\mathfrak{p})^{-s}} \right| \leq \sum_{N(I) \geq M} \frac{1}{N(I)^{\mathrm{Re}(s)}}$$

which tends to zero as $M \to \infty$. This proves the Proposition.

For an irreducible projective smooth algebraic curve X over a finite field $\mathbf{F}_q$, the zeta function $Z_X(s)$ is defined as

$$Z_X(s) = \sum_{D \geq 0} N(D)^{-s}, \qquad \text{for } s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 1.$$

Here $N(D) = e^{-\deg(D)}$ and the sum runs over the *effective* divisors D of X. This suggests to involve the *effectivity* of section 11 and leads to the following definition.

Definition. Let F be a number field. The *zeta function* $Z_F(s)$ associated to F is the function of a complex variable defined by

$$Z_F(s) = \int_{\mathrm{Div}_F} N(D)^{-s} \mathrm{eff}(D) dD, \qquad \text{for } \mathrm{Re}(s) > 1.$$

To see that $Z_F(s)$ converges for $\mathrm{Re}(s) > 1$, we write $D = (I, u)$ and observe that $N(D)^{-1} = NuN(I)$. Since the integrand is non- zero only when $O_F \subset I$, putting $J = I^{-1}$ this leads to

$$Z_F(s) = \sum_{0 \neq J \subset O_F} N(J)^{-s} \int_{\prod_\sigma \mathbf{R}^*_{>0}} N(u)^s e^{-\pi \|u\|^2} d\mu$$

Here $d\mu$ denotes the measure induced by the natural metric on $\prod_\sigma \mathbf{R} \cong \prod_\sigma \mathbf{R}^*_{>0}$. Since $N(u) = \prod_\sigma u_\sigma^{\deg \sigma}$ and $\|u\|^2 = \sum_\sigma \deg(\sigma) u_\sigma^2$, the integral over $\prod_\sigma \mathbf{R}^*_{>0}$ is a product of integrals of the form

$$\sqrt{\deg(\sigma)} \int_0^\infty t^{\deg(\sigma) s} e^{-\pi \deg(\sigma) t^2} \frac{dt}{t}.$$

This is equal to

$$\tfrac{1}{2} \pi^{-\frac{s}{2}} \Gamma(\tfrac{s}{2}) \quad \text{or} \qquad \tfrac{1}{\sqrt{2}} (2\pi)^{-s} \Gamma(s)$$

depending on whether σ is real or complex. Since the sum $\sum_{0 \neq J \subset O_F} N(J)^{-s}$ converges to the Dedekind zeta function $\zeta_F(s)$ when $\mathrm{Re}(s) > 1$ and since the integral defining the Gamma function converges on $\{s \in \mathbf{C} : \mathrm{Re}(s) > 0\}$, the integral that defines $Z_F(s)$ converges for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

Theorem 12.3. *Let F be a number field of degree n and discriminant Δ_F. The zeta function $Z_F(s)$ admits a meromorphic continuation to $\mathbf{C}$. It satisfies the functional equation: the function*

$$|\Delta_F|^{\frac{s}{2}} Z_F(s)$$

is invariant under the substitution $s \leftrightarrow 1-s$. *The only poles of* $Z_F(s)$ *are at* $s = 0$ *and* $s = 1$. *They are of order 1. We have that*

$$\operatorname*{Res}_{s=1} Z_F(s) = \frac{\mathrm{vol}(\mathrm{Pic}_F^0)}{w_F\sqrt{n}\sqrt{|\Delta_F|}} \qquad \textit{and} \qquad \operatorname*{Res}_{s=0} Z_F(s) = \frac{\mathrm{vol}(\mathrm{Pic}_F^0)}{w_F\sqrt{n}}.$$

Proof. We compute $Z_F(s)$ by first integrating the function $N(D)^{-s}\mathrm{eff}(D)dD$ over each coset of the subgroup of principal divisors of Div_F and then integrating over Pic_F. We write the integral over the cosets of the discrete subgroup of principal divisors as sums rather than integrals. Since $N(D)$ only depends on the class of D in Pic_F, this leads to

$$\begin{aligned} Z_F(s) &= \int_{\mathrm{Pic}_F} \left(\sum_{(x)} \mathrm{eff}(D+(x)) \right) N(D)^{-s} dD, \\ &= \int_{\mathrm{Pic}_F} \left(\frac{1}{w_F} \sum_{x \in F^*} \mathrm{eff}(D+(x)) \right) N(D)^{-s} dD. \end{aligned}$$

Here w_F denotes the order of the group μ_F of roots of unity. The second equality follows from the fact that the kernel of the map $x \mapsto (x)$ from F^* to Div_F is equal to μ_F. In terms of the function $h^0(D)$ introduced in section 11, we have therefore that

$$Z_F(s) = \int_{\mathrm{Pic}_F} \left(\frac{e^{h^0(D)} - 1}{w_F} \right) N(D)^{-s} dD, \qquad \text{for } s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 1.$$

Next we split the integral into two parts: the first integrates over the divisor classes D of $\deg(D) < \frac{1}{2}\deg(\kappa)$ or equivalently with $N(D) < N(\kappa)^{1/2} = \sqrt{|\Delta_F|}$. The second integral involves the divisor classes D with $N(D) \geq \sqrt{|\Delta_F|}$. In the second integral we make a change of variables: we replace D by $\kappa - D$. Since $N(\kappa - D) \leq N(\kappa)^{1/2}$ whenever $N(D) \geq N(\kappa)^{1/2}$, this gives us the following expression for $Z_F(s)$ when $\mathrm{Re}(s) > 1$.

$$w_F Z_F(s) = \int\limits_{\substack{D \in \mathrm{Pic}_F \\ N(D) < N(\kappa)^{1/2}}} \left(e^{h^0(D)} - 1 \right) N(D)^{-s} dD \; + \int\limits_{\substack{D \in \mathrm{Pic}_F \\ N(D) < N(\kappa)^{1/2}}} \left(e^{h^0(\kappa - D)} - 1 \right) \left(\frac{N(\kappa)}{N(D)} \right)^{-s} dD.$$

The key step is an application of the Riemann-Roch Theorem: in the second integral we use the equality

$$e^{h^0(\kappa - D)} = e^{h^0(D)} N(\kappa)^{1/2} / N(D).$$

The second integral becomes equal to

$$\int\limits_{\substack{D \in \mathrm{Pic}_F \\ N(D) < N(\kappa)^{1/2}}} \left(e^{h^0(D)} - 1 \right) \frac{N(\kappa)^{1/2}}{N(D)} \left(\frac{N(\kappa)}{N(D)} \right)^{-s} dD \; + \int\limits_{\substack{D \in \mathrm{Pic}_F \\ N(D) < N(\kappa)^{1/2}}} \left(\frac{N(\kappa)^{1/2}}{N(D)} - 1 \right) \left(\frac{N(\kappa)}{N(D)} \right)^{-s} dD.$$

This leads to the following expression for the zeta function.

$$w_F N(\kappa)^{s/2} Z_F(s) = \int\limits_{\substack{D\in \mathrm{Pic}_F \\ N(D)<N(\kappa)^{1/2}}} \left(e^{h^0(D)}-1\right)\left(\left(\frac{N(\kappa)^{1/2}}{N(D)}\right)^s + \left(\frac{N(\kappa)^{1/2}}{N(D)}\right)^{1-s}\right) dD$$
$$+ \int\limits_{\substack{D\in \mathrm{Pic}_F \\ N(D)<N(\kappa)^{1/2}}} \left(\frac{N(\kappa)^{1/2}}{N(D)}-1\right)\left(\frac{N(\kappa)^{1/2}}{N(D)}\right)^{-s} dD$$

We evaluate the second integral. Since the integrand does depend on the norm $N(D)$ rather than D itself, we use the exact sequence

$$0 \longrightarrow \quad \mathrm{Pic}_F^0 \quad \longrightarrow \quad \mathrm{Pic}_F \quad \stackrel{\deg}{\longrightarrow} \quad \mathbf{R} \longrightarrow 0$$

Therefore the second integral is equal to the *volume* of Pic_F^0 times an integral over $\mathbf{R}$. Note however that the degree map is not compatible with the metrics on Pic_F and $\mathbf{R}$. Indeed, the element $1 \in \oplus_\sigma \mathbf{R} \subset F_{\mathbf{R}}$ has length $\sqrt{n}$, but its degree $n \in \mathbf{R}$ has length n. Therefore the integral is smaller by a factor $\sqrt{n}$ when we integrate with respect to the usual Haar measure on $\mathbf{R}$. Switching to the multiplicative variable $t = e^x = e^{\deg(D)}$ we have that $dx = \frac{dt}{t}$. The second integral becomes

$$\mathrm{vol}(\mathrm{Pic}_F^0)\frac{1}{\sqrt{n}}\left(N(\kappa)^{(1-s)/2}\int_{-\infty}^{\sqrt{N(\kappa)}} t^{s-1}\frac{dt}{t} - N(\kappa)^{-s/2}\int_{-\infty}^{\sqrt{N(\kappa)}} t^s \frac{dt}{t}\right)$$

which is equal to $\mathrm{vol}(\mathrm{Pic}_F^0)/s(s-1)\sqrt{n}$. We find that

$$w_F N(\kappa)^{s/2} Z_F(s) = \frac{\mathrm{vol}(\mathrm{Pic}_F^0)}{s(s-1)\sqrt{n}} + \int\limits_{\substack{D\in \mathrm{Pic}_F \\ N(D)<N(\kappa)^{1/2}}} \left(e^{h^0(D)}-1\right)\left(\left(\frac{N(\kappa)^{1/2}}{N(D)}\right)^s + \left(\frac{N(\kappa)^{1/2}}{N(D)}\right)^{1-s}\right) dD.$$

We claim that the integral expression on the right converges absolutely and uniformly in compact subsets of $\mathbf{C}$. This means that we have found a meromorphic continuation for $Z_F(s)$. The symmetry under $s \leftrightarrow 1-s$ is evident and since the volume of Pic_F^0 is not zero, there are two simple poles at $s = 0$ and $s = 1$ with the required residues.

The convergence follows from the estimate

$$h^0(D) \leq 2 \cdot 3^n \cdot \exp\left(-\pi n e^{-\frac{2}{n}\deg(D)}\right)$$

of Proposition 11.2. It shows that the absolute value of the integral is at most

$$2 \cdot 3^n \frac{\mathrm{vol}(\mathrm{Pic}_F^0)}{\sqrt{n}} \int_0^{\sqrt{N(\kappa)}} e^{-\pi n t^{-\frac{2}{n}}} \left(\left(\frac{N(\kappa)^{1/2}}{t}\right)^s + \left(\frac{N(\kappa)^{1/2}}{t}\right)^{1-s}\right)\frac{dt}{t}.$$

It suffices to show that the integral

$$\int_0^{\sqrt{N(\kappa)}} e^{-\pi n t^{-\frac{2}{n}}} t^s \frac{dt}{t}$$

has the required convergence properties. This becomes clear when we make the change of variable $y = t^{-2/n}$. The integral becomes

$$\int_{\frac{1}{\sqrt[n]{N(\kappa)}}}^{\infty} e^{-\pi n y} y^{ns/2} \frac{dy}{y}$$

and is easily seen to converge absolutely and uniformly in compact subsets of $\mathbf{C}$. This proves the theorem.

Since the product expression for the Dedekind zeta function

$$\zeta_F(s) = \prod_{0 \neq \mathfrak{p} \subset O_F} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

converges for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$, it follows from the functional equation that $Z_F(s)$ has all its zeroes in the *critical strip* $\{s \in \mathbf{C} : 0 \leq \mathrm{Re}(s) \leq 1\}$. Conjecturally all zeroes are in the center of the critical strip:

Generalized Riemann Hypothesis. Let F be a number field. Then every zero of $Z_F(s)$ has real part equal to $\frac{1}{2}$.

The zeroes of $Z_F(s)$ form a discrete subset of $\mathbf{C}$. For $F = \mathbf{Q}$, the first few zeroes are

$$\begin{aligned}
&\tfrac{1}{2} \pm 14.134725\ldots i,\\
&\tfrac{1}{2} \pm 21.022040\ldots i.\\
&\tfrac{1}{2} \pm 25.010856\ldots i.\\
&\tfrac{1}{2} \pm 30.424878\ldots i.\\
&\quad\vdots
\end{aligned}$$

The Riemann Hypothesis was formulated by G.B. Riemann for the Riemann zeta function $\zeta(s) = \zeta_{\mathbf{Q}}(s)$ in his 1859 paper on the distribution of prime numbers. It appears in D. Hilbert's famous list of problems presented at the international congress in 1900 in Paris. More recently, the Clay Institute (`www.claymath.org`) included the conjecture in its list of seven major unsolved problems. The institute pays $1,000,000 for a correct proof of the Riemann Hypothesis.

Recently it has been verified by computer that the first 10^{11} zeroes are on the critical line (`www.zetagrid.net/zeta/math/zeta.result.100billion.zeros.html`). The computation implies that all zeroes s with $|\mathrm{Im}(s)| < 29,538,618,432.236\ldots$ have real part equal to $\frac{1}{2}$.

For curves over finite fields the analogue of the Riemann Hypothesis has been proved by A. Weil in 1940–1948.

Exercises.

12.1 Let $\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}$ denote the *Gamma function*.

(i) Show that the integral converges for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 0$.

(ii) Show that $\Gamma(1) = 1$ and that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

(iii) Show that $\Gamma(s+1) = s\Gamma(s)$ for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 0$. Deduce that $\Gamma(n+1) = n!$ for every integer $n \geq 1$.

(iv) For any $s \in \mathbf{C}$ that is not a negative integer we define

$$\Gamma(s) = \frac{\Gamma(s+k+1)}{s(s+1)\cdots(s+k)},$$

where k is any integer for which $\mathrm{Re}(s) > -k$. Show that this defines a meromorphic continuation of $\Gamma(s)$ to $\mathbf{C}$. Show that $\Gamma(s)$ only admits poles at $k = 0, -1, -2, \ldots$. Show that the poles are simple and determine the residues.

(v) Show that $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$. (Hint: it suffices to show this for $s \in \mathbf{C}$ with $0 < \mathrm{Re}(s) < 1$.)

12.2

13. An explicit example.

Consider the following (randomly selected, Trento, december 1990) polynomial

$$f(T) = T^4 - 2T^2 + 3T - 7 \qquad \in \mathbf{Z}[T].$$

This polynomial is irreducible modulo 2. This follows from the fact that it is an Artin-Schreier polynomial, but it can also, easily, be checked directly. We study the number field $F = \mathbf{Q}(\alpha)$, where α is a zero of $f(T)$. In order to evaluate the discriminant of $f(T)$, we compute the sums p_i of the ith powers of its roots in $\mathbf{C}$ using Newton's relations (Exer.3.9):

$$\begin{aligned}
p_1 &= 0 \\
p_2 &= -2s_2 + p_1 s_1 = -2 \cdot 2 + 0 = 4 \\
p_3 &= 3s_3 + p_2 s_1 - p_1 s_2 = 3 \cdot (-3) + 0 + 0 = -9 \\
p_4 &= 2p_2 - 3p_1 + 7p_0 = 2 \cdot 4 - 0 + 7 \cdot 4 = 36 \\
p_5 &= 2p_3 - 3p_2 + 7p_1 = 2 \cdot (-9) - 3 \cdot 4 + 0 = -30 \\
p_6 &= 2p_4 - 3p_3 + 7p_2 = 2 \cdot 36 - 3 \cdot (-9) + 7 \cdot 4 = 127
\end{aligned}$$

We have that

$$\mathrm{Disc}(f(X)) = \det \begin{pmatrix} 4 & 0 & 4 & -9 \\ 0 & 4 & -9 & 36 \\ 4 & -9 & 36 & -30 \\ -9 & 36 & -30 & 127 \end{pmatrix} = -98443$$

which is a prime number. We conclude from Prop.4.8 that $\Delta_F = -98443$ and that $O_F = \mathbf{Z}[\alpha]$. From the fact that the complex zeroes of $f(X)$ are approximately equal to

$$\begin{aligned} \alpha_1 &= -2.195251731\ldots, \\ \alpha_2 &= 1.655743097\ldots, \\ \alpha_3, \overline{\alpha}_3 &= 0.269754317\ldots \pm 1.361277001\ldots i. \end{aligned}$$

we deduce that $r_1 = 2$ and that $r_2 = 1$.

Next we substitute all integers n with $-18 \leq n \leq 18$ in $f(T)$ and factor the result into a product of prime numbers:

Table 13.1.

n	$f(n) = N(n-\alpha)$
0	-7
1	-5
2	7
3	$5 \cdot 13$
4	229
5	$11 \cdot 53$
6	$5 \cdot 13 \cdot 19$
7	$7 \cdot 331$
8	$5 \cdot 797$
9	$7^2 \cdot 131$
10	$11 \cdot 19 \cdot 47$
11	$5^2 \cdot 577$
12	20477
13	$5 \cdot 5651$
14	$7 \cdot 5437$
15	$149 \cdot 337$

n	$f(n) = N(n-\alpha)$
0	-7
-1	-11
-2	-5
-3	47
-4	$5 \cdot 41$
-5	$7 \cdot 79$
-6	$11 \cdot 109$
-7	$5^2 \cdot 7 \cdot 13$
-8	$31 \cdot 127$
-9	$5 \cdot 19 \cdot 67$
-10	$13 \cdot 751$
-11	$83 \cdot 173$
-12	$5 \cdot 7 \cdot 11 \cdot 53$
-13	$19 \cdot 1483$
-14	$5^2 \cdot 7^2 \cdot 31$
-15	50123

By Minkowski's Theorem (Prop. 9.5), the class group $Cl(O_F)$ is generated by ideal $I \subset O_F$ of norm at most

$$\frac{4!}{4^4}\frac{4}{\pi}\sqrt{98443} = 37.45189\ldots.$$

In order to calculate the class group, we determine the primes of small norm first.

We see in Table 13.1 that the polynomial $f(T)$ has no zeroes modulo p for the primes $p = 2, 3, 17, 23$ and 29. We leave the verification that $f(T)$ has no zeroes modulo 37 either, to the reader. By Kummer's Lemma (Exer. 6.1) we conclude that there are no prime ideals of norm p for these primes p. It is easily checked that $f(T)$ is irreducible modulo 2 and 3 and that $f(T) \equiv (T-1)(T+2)(T^2 - T + 1) \pmod 5$. The polynomial $T^2 - T + 1$ is irreducible mod 5.

This gives us the following list of all prime ideals of norm less than $37.45\ldots$: the ideals (2) and (3) are prime and $(5) = \mathfrak{p}_5\mathfrak{p}_5'\mathfrak{p}_{25}$, where $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ have norm 5 and $\mathfrak{p}_{25}$ is a prime of norm 25. The other primes $\mathfrak{p}_p$ and $\mathfrak{p}_p'$ of norm less $37.45\ldots$ have prime norm p. They are listed in Table 13.2 and are easily computed from Table 13.1.

Table 13.2.

$\mathfrak{p}_5 = (5, \alpha - 1)$	$\mathfrak{p}'_5 = (5, \alpha + 2)$
$\mathfrak{p}_7 = (7, \alpha)$	$\mathfrak{p}'_7 = (7, \alpha - 2)$
$\mathfrak{p}_{11} = (11, \alpha + 1)$	$\mathfrak{p}'_{11} = (11, \alpha - 5)$
$\mathfrak{p}_{13} = (13, \alpha - 3)$	$\mathfrak{p}'_{13} = (13, \alpha - 6)$
$\mathfrak{p}_{19} = (19, \alpha - 6)$	$\mathfrak{p}'_{19} = (19, \alpha + 9)$
$\mathfrak{p}_{31} = (31, \alpha + 8)$	$\mathfrak{p}'_{31} = (31, \alpha + 14)$

The class group is generated by the classes of these primes and the class of $\mathfrak{p}_{25}$. There exist, however, many relations between these classes. In the following table we list the factorizations of some numbers of the form $q - p\alpha$, where $p, q \in \mathbf{Z}$. We have chosen numbers of this form because the norms $N(q - p\alpha) = p^4 f(q/p)$ can be computed so easily (Exer. 3.5). The factorizations into prime ideals of the principal ideals $(q - p\alpha)$ give rise to relations in the class group. For instance $\mathrm{N}(1 - 4\alpha) = -2015 = -5 \cdot 13 \cdot 31$ and $(1 - 4\alpha) = \mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$. This shows that the ideal class of $\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$ is trivial. Therefore the class of $\mathfrak{p}_{31}$ can be expressed in terms of classes of prime ideals of smaller norm:

$$\mathfrak{p}_{31} \sim \mathfrak{p}_5^{-1}\mathfrak{p}_{13}^{-1}.$$

We conclude that the ideal $\mathfrak{p}_{31}$ is not needed to generate the ideal class group. In a similar way one deduces from Table 13.3 below that the ideal classes of the primes of norm 31,19,13 and 11, can all be expressed in terms of ideal classes of primes of smaller norm.

Table 13.3.

	β	$\mathrm{N}(\beta)$	(β)
(i)	$4\alpha + 1$	$-5 \cdot 31 \cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{p}_{31}$
(ii)	$3\alpha - 2$	-31	$\mathfrak{p}'_{31}$
(iii)	$\alpha - 6$	$5 \cdot 13 \cdot 19$	$\mathfrak{p}_5\mathfrak{p}'_{13}\mathfrak{p}_{19}$
(iv)	$2\alpha - 1$	$-5 \cdot 19$	$\mathfrak{p}'_5\mathfrak{p}'_{19}$
(v)	$\alpha + 7$	$5^2 \cdot 7 \cdot 13$	${\mathfrak{p}'_5}^2\mathfrak{p}'_7\mathfrak{p}'_{13}$
(vi)	$3\alpha - 5$	13	$\mathfrak{p}'_{13}$
(vii)	$\alpha - 3$	$-5 \cdot 13$	$\mathfrak{p}'_5\mathfrak{p}_{13}$
(viii)	$\alpha + 1$	-11	$\mathfrak{p}_{11}$
(ix)	$3\alpha - 4$	$5^2 \cdot 11$	${\mathfrak{p}'_5}^2\mathfrak{p}'_{11}$

We conclude that $Cl(O_F)$ is generated by the primes $\mathfrak{p}_5$, $\mathfrak{p}'_5$, $\mathfrak{p}_7$, $\mathfrak{p}'_7$ and $\mathfrak{p}_{25}$. One does not need entry (vi) to conclude this, but this entry will be useful later. The primes of norm 5 and 7 are all principal. This follows form the first few lines of Table 13.1. Finally, since $\mathfrak{p}_5\mathfrak{p}'_5\mathfrak{p}_{25} = (5)$, one concludes that $\mathfrak{p}_{25}$ is principal. We have proved that the class group of $\mathbf{Q}(\alpha)$ is trivial.

By Dirichlet's Unit Theorem, the unit group has rank $r_1 + r_2 - 1 = 2 + 1 - 1 = 2$. The group of roots of unity is just $\{\pm 1\}$. In all our calculations, we have not encountered a single unit yet! To find units, it is convenient to calculate the norms of some elements of

the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbf{Z}$. This can be done as follows. We use the accurate approximations of the roots $\alpha_1, \alpha_2, \alpha_3, \overline{\alpha_3}$ of f in $\mathbf{C}$. By Lemma 5.1 one has that

$$\mathrm{N}(a + b\alpha + c\alpha^2) = \left(a + b\alpha_1 + c\alpha_1^2\right)\left(a + b\alpha_2 + c\alpha_2^2\right)\left|a + b\alpha_3 + c\alpha_3^2\right|^2.$$

Calculating norms of some small elements of the form $a + b\alpha + c\alpha^2$ one soon finds that $\mathrm{N}(1 + \alpha - \alpha^2) = 5$. This shows that the ideals $1 + \alpha - \alpha^2$ and $\mathfrak{p}_5'$ are equal. In Table 13.1, we read that $\mathfrak{p}_5' = (\alpha + 2)$. We conclude that

$$\varepsilon_1 = \frac{1 + \alpha - \alpha^2}{\alpha + 2} = \alpha^3 - 2\alpha^2 + 3\alpha - 4$$

is a unit. Similarly one finds that $\mathrm{N}(2 - 2\alpha + \alpha^2) = 65$. One easily checks that $(2 - 2\alpha + \alpha^2) = \mathfrak{p}_5'\mathfrak{p}_{13}'$. In Table III(vi) we see that $\mathfrak{p}_{13}' = (3\alpha - 5)$. We conclude that the principal ideals $(2 - 2\alpha + \alpha^2)$ and $((\alpha + 2)(3\alpha - 5))$ are equal. This implies that

$$\varepsilon_2 = \frac{2 - 2\alpha + \alpha^2}{(3\alpha - 5)(\alpha + 2)} = \alpha^3 + \alpha^2 + \alpha + 3$$

is a unit.

Rather then proving that the units $\varepsilon_1, \varepsilon_2$ and -1 generate the unit group, we provide merely evidence that these units generate the whole group. For this we use the main result of the section 12. We use the ζ-function of the field F. Theorem 12.3 gives us an expression for the residue of the zeta function $Z_F(s)$ associated to F at $s = 1$. Since the Riemann ζ-function $\zeta_{\mathbf{Q}}(s)$ has a residue equal to 1 at $s = 1$ and the since the Gamma factors $\frac{1}{2}\pi^{s/2}\Gamma(\frac{s}{2})$ and $\frac{1}{\sqrt{2}}(2\pi)^s\Gamma(s)$ have values in $s = 1$ equal to $\frac{1}{2}$ and $\frac{1}{2\sqrt{2}}$ respectively, one can express the content of Theorem 12.3 for a number field of degree n as follows

$$\lim_{s \to 1} \frac{\zeta_F(s)}{\zeta_{\mathbf{Q}}(s)} = \frac{2^{r_1}(2\pi\sqrt{2})^{r_2}}{w_F\sqrt{n}\sqrt{|\Delta_F|}}\mathrm{vol}(\mathrm{Pic}_F^0).$$

Using the Euler product formula for the ζ-functions and ignoring problems of convergence this gives rise to

$$\prod_p \frac{\prod_{\mathfrak{p}|p}\left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1}}{\left(1 - \frac{1}{p}\right)^{-1}} = \frac{2^{r_1}(2\pi\sqrt{2})^{r_2}}{w_F\sqrt{n}\sqrt{|\Delta_F|}}\mathrm{vol}(\mathrm{Pic}_F^0).$$

We can compute the right hand side: $r_1 = 2$, $r_2 = 1$, $w_F = 2$ and $\Delta = -98443$. By the calculation above we have that $h_F = 1$. If we *assume* that the units $\varepsilon_1, \varepsilon_2$ are fundamental, we can compute the regulator using the two real embeddings $\phi_1, \phi_2 : F \hookrightarrow \mathbf{R}$ given by $\alpha \mapsto \alpha_1$ and $\alpha \mapsto \alpha_2$ respectively. Denoting the three infinite primes by σ_1, σ_2 and σ_3 this gives

$$\mathrm{vol}(\mathrm{Pic}_F^0) = 2^{\frac{r_2}{2}}\frac{h}{\sqrt{n}}|\det\begin{pmatrix} 1 & \log|\sigma_1(\varepsilon_1)| & \log|\sigma_1(\varepsilon_2)| \\ 1 & \log|\sigma_2(\varepsilon_1)| & \log|\sigma_2(\varepsilon_2)| \\ 1 & \log|\sigma_3(\varepsilon_1)| & \log|\sigma_3(\varepsilon_2)| \end{pmatrix}|.$$

Substituting approximations to the $\sigma_j(\varepsilon_i)$ this gives

$$\mathrm{vol}(\mathrm{Pic}_F^0) = \frac{1}{\sqrt{2}}|\det\begin{pmatrix} 1 & 3.427619209 & 1.600462837 \\ 1 & -3.752710586 & 2.479594524 \\ 1 & 0.1625456885 & -2.0400286805 \end{pmatrix}| \approx 20.513421788$$

So, assuming that the units $\varepsilon_1, \varepsilon_2$ are fundamental we find that the right hand side of the equation is equal to

$$\frac{4 \cdot 2\pi\sqrt{2}}{2\sqrt{4}\sqrt{98443}} \cdot 20.513421788 \approx 0.5809524077.$$

If the units would *not* be fundamental, the volume of Pic_F^0 would be k times as small, for some positive integer k. This would imply that the value 0.5809524077 would be replaced by 0.2904762039 (when $k = 2$) or 0.1936508026 (when $k = 3$) or ... etc.

It can be shown that the Euler product on the left hand side converges. It converges only slowly and not absolutely: the contributions of the various prime ideals $\mathfrak{p}$ must be multiplied in increasing order of $N(\mathfrak{p})$. We explicitly determine the factors in the Euler product on the left hand side. For a given prime p, the factor is

$$\left(1 - \frac{1}{p}\right) \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1}.$$

To determine it, we must find the way the prime p splits in the extension F over $\mathbf{Q}$. Apart from the ramified prime 98443, there are five possibilities. Using Kummer's Lemma they can be distinguished by the factorization of $f(T) \in \mathbf{F}_p[T]$:

$$pO_F = \begin{cases} (i) \quad \mathfrak{p}_p\mathfrak{p}'_p\mathfrak{p}''_p\mathfrak{p}'''_p, & \text{if } f(T) \text{ has 4 zeroes mod } p, \\ (ii) \quad \mathfrak{p}_p\mathfrak{p}'_p\mathfrak{p}_{p^2}, & \text{if } f(T) \text{ has exactly 2 zeroes mod } p, \\ (iii) \quad \mathfrak{p}_p\mathfrak{p}_{p^3}, & \text{if } f(T) \text{ has only one zero mod } p, \\ (iv) \quad \mathfrak{p}_{p^2}\mathfrak{p}'_{p^2} & \text{if } f(T) \text{ has two irreducible quadratic factors mod } p, \\ (v) \quad (p), & \text{if } f(T) \text{ is irreducible mod } p. \end{cases}$$

here $\mathfrak{p}_p$, $\mathfrak{p}_{p^2}$, etc. denote primes of norm p, p^2 etc. We find that the product on the left hand side is equal to

$$\prod_p F(p)^{-1}$$

where

$$\begin{aligned} F(p) &= \left(1 - \frac{1}{p}\right)^3 && \text{in case } (i), \\ &= \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) && \text{in case } (ii), \\ &= \left(1 - \frac{1}{p^3}\right) && \text{in case } (iii), \\ &= \left(1 + \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) && \text{in case } (iv), \\ &= \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3}\right) && \text{in case } (v). \end{aligned}$$

We approximate the left hand side product by evaluating the contributions of the primes less than a certain moderately large number. A short computer program enables one to compute this product with some precision. It suffices to count the zeroes of $f(T)$ modulo p. This done by computing $\gcd(T^p - T, f(T))$ in the ring $\mathbf{F}_p[T]$. Most of the work is the calculation of T^p in the ring $\mathbf{F}_p[T]/(f(T))$. To distinguish between cases *(iv)* and *(v)* one observes that in case *(iv)*, the discriminant of $f(T)$ is a square modulo p, while in case *(v)* it isn't.

Using the primes less than 1657 one finds 0.5815983 for the value of the Euler product. This is close to the number 0.5809524077 that we found above. In view of the slow convergence of the Euler product, the error is not unusually large. It is rather unlikely that the final value will be two times, three times or even more times as small. This indicates, but does not prove, that the units ε_1 and ε_2 do indeed generate the unit group O_F^* modulo torsion. To *prove* that they do, one should employ different techniques, related to methods for searching short vectors in lattices.

Exercises.

13.1 Let $F = \mathbf{Q}(\sqrt[5]{2})$. Compute ring of integers O_F, ideal class group $Cl(O_F)$ and unit group O_F^*.

13.2 Let $f(T) = T^3 + T^2 + 5T - 16$. Show that f is irreducible and let $F = \mathbf{Q}(\alpha)$ where α is a zero of $f(T)$. Compute ring of integers O_F, ideal class group $Cl(O_F)$ and unit group O_F^*.