4. Geometry of numbers

Remark. All the rings are supposed to be commutative with identity.

Definition 4.1 (cf. 3.3 and "short visit to highschool" in the p-adic numbers chapter). Suppose B/A is an extension of the rings (i.e. $A \subset B$). B is called integral over A iff all the elements of B are integral over A.

Definition 4.2 (cf. 3.4). B is called finite over A iff B is finitely generated as an A-module.

Theorem 4.3. (cf. 3.5). If B/A is finite then it is integral.

Proof. Since B/A is finite there exists a surjective homomorphism $\phi : A^n \to B$. Suppose $b \in B$. Multiplication with b defines an A-linear endomorphism of the A-module B which could be lifted to an endomorphism $\widetilde{b}$ of A^n (choose a basis $\{x_i\}$ of A^n and define $\widetilde{b}\ (x_i)$ to be equal to some ϕ - preimage of $b\phi(x_i)$). Let $P(T)$ be the characteristic polynomial of $\widetilde{b}$, this is a monic polynomial with coefficients in A. By the Cayley - Hamilton theorem $P(\widetilde{b}) = 0$. Therefore $\forall x \in A^n \;\; 0 = P(\widetilde{b}\ (x)) = \phi(P(\widetilde{b}\ (x))) = P(\phi(\widetilde{b}\ (x))) = P(b\phi(x))$. Since ϕ is surjective $\exists x \in A^n$ such that $\phi(x) = 1$ hence $P(b) = 0$ ■

Theorem 4.4. (cf. 3.7). If $A \subset B \subset C$. If B/A and C/B are both finite, same is C/A.

Proof. Close to that of the Theorem 3.7 (use sets of generators instead of bases) ■

Theorem 4.5. (cf. 3.8). If B is integral over A and finitely generated as an A-algebra then B/A is finite.

Proof. Suppose $B = A[\beta]$ where β is integral over A. By the definition this means that $\exists P(T) \in A[T]$ monic such that $P(\beta) = 0$. If $\deg P = d$ then β^d is a linear combination of smaller powers of β. Clearly the same is true for greater powers of β hence the set $\{1, \beta, \ldots, \beta^{d-1}\}$ generates B as an A-module. Now one may use induction based on the Theorem 4.4 ■

Definition-Theorem 4.6. Suppose B/A is an extension of the rings. The subset of B consisting of all elements which are integral over A is called the integral closure of A in B. This subset is a subring of B.

Proof. Suppose $\alpha, \beta \in B$ are integral over A. The subring $A[\alpha, \beta] \subset B$ is finite over A by the theorems 4.5 & 4.4 therefore integral over A by the Theorem 4.3. Hence $\alpha - \beta$ and $\alpha\beta$ are integral over A ■

Theorem 4.7. Suppose $\mathcal{O}$ is an integrally closed Noetherian integral domain, k its field of fractions, K/k a finite separable extension. Then
1) The integral closure of $\mathcal{O}$ in K (notation $\mathcal{O}_K$) is finite over $\mathcal{O}$ and contains some basis of the k-vector space K.
2) If $\mathcal{O}$ is a principal ideal domain then $\mathcal{O}_K$ is a free $\mathcal{O}$-module with $n = [K : k]$ generators.

Lemma. Suppose $\mathcal{O}$ is a Noetherian ring, $N \subset \mathcal{O}^n$ an $\mathcal{O}$-submodule. Then N is finitely generated. If $\mathcal{O}$ is a principal ideal ring then N is free of rank $\leq n$.
Proof of the Lemma. Use induction. Let $\mathcal{O}^{n-1}$ be the submodule of $\mathcal{O}^n$ generated by the first $n-1$ coordinate vectors, $N_{n-1} \stackrel{\text{def}}{=} N \cap \mathcal{O}^{n-1}$. Let I be the ideal in $\mathcal{O}$ obtained by the projection of N to the last coordinate. Suppose $a_1, \ldots, a_r$ generate I. For each $1 \leq i \leq r$ choose $y_i \in N$ such that the last coordinate of y_i equals a_i. Then $N = N_{n-1} + \langle\{y_i\}\rangle$ which proves the first statement of the Lemma. To prove the second statement it suffices to point out that I is generated by one element a_1 hence $N = N_{n-1} \oplus \langle y_1 \rangle$, rk (N) being equal either to $\text{rk}(N_{n-1})$ (if $a_1 = 0$) or to $\text{rk}(N_{n-1}) + 1$ otherwise ■

Proof of the Theorem. If $x \in K$ then x is algebraic over k hence $\exists P(T) = \sum_{i=0}^{d} a_i T^i \in k[T]$ such that $P(x) = 0$. Multiplying P with the product of the denominators of all coefficients one may suppose that $\forall i \;\; a_i \in \mathcal{O}$. Then multiplying the equation $P(x) = 0$ with a_d^{d-1} one gets an integral equation for $a_d x$. Hence any basis of the vector space K over k after multiplying with suitable elements of $\mathcal{O}$ will consist of integral elements of K.
Now consider the trace bilinear form $Tr : K \times K \to k$ which is nondegenerate by the Theorem 3.53. For any $\mathcal{O}$-submodule N in K define $N^\vee \stackrel{\text{def}}{=} \{y \in K \text{ such that } \forall x \in N \;\; Tr(xy) \in \mathcal{O}\}$. Suppose $\{e_i\}$ is a basis of K consisting of integral elements (this one has just been constructed) and let N be the free $\mathcal{O}$-submodule of $\mathcal{O}_K$ generated by the $\{e_i\}$. Let $\{f_j\}$ be the dual basis to $\{e_i\}$ (i.e. $Tr(e_i f_j) = \delta_i^j$). Then $N^\vee$ coincides with the free $\mathcal{O}$-submodule of K generated by $\{f_j\}$ (see Problem 36). Since $N \subset \mathcal{O}_K \;\; \mathcal{O}_K^\vee \subset N^\vee$. Clearly for any x integral over $\mathcal{O}$ and $\sigma \in \Sigma_{K/k}^{\bar{k}/k} \;\; \sigma(x)$ is also integral over $\mathcal{O}$ thus $Tr(x)$ is integral over $\mathcal{O}$. But $Tr(x) \in k$ and $\mathcal{O}$ is integrally closed hence $Tr(\mathcal{O}_K) \subset \mathcal{O}$. In particular, $\mathcal{O}_K \subset \mathcal{O}_K^\vee$. Finally one may conclude that $\mathcal{O}_K \subset N^\vee$ therefore by the Lemma $\mathcal{O}_K$ is finitely generated as an $\mathcal{O}$-module and is free of rank $\leq n$ if $\mathcal{O}$ is a principal ideal ring. Since $\mathcal{O}_K$ contains the basis of K over k in the latter case the rank equals n ■

From now on in this chapter K is a finite extension of $\mathbf{Q}$, $\mathcal{O}_K$ its ring of integers (i.e. the integral closure of $\mathbf{Z}$ in K), $n = [K : \mathbf{Q}]$.

Definition-Theorem 4.8. Consider the action of the complex conjugation map τ on the set $\Sigma_{K/\mathbf{Q}}^{\mathbf{C}/\mathbf{Q}}$ which sends $\sigma \mapsto \tau \circ \sigma$. Let s be the number of one-element orbits of this action (which correspond to the homomorphisms σ such that $\sigma(K) \subset \mathbf{R}$, suppose $\{\sigma_1, \ldots, \sigma_s\}$ is their full list). Let t be the number of two-elements orbits (which correspond to the pairs $(\sigma,\ \overline{\sigma} = \tau \circ \sigma)$ such that $\sigma(K) \not\subset \mathbf{R}$). Choose a set $\{\sigma_{s+1}, \ldots, \sigma_{s+t}\}$ of homomorphisms $K/\mathbf{Q} \to \mathbf{C}/\mathbf{Q}$ containing just one element of each pair. Define the map $\phi : K \otimes_{\mathbf{Q}} \mathbf{R} \to \mathbf{R}^s \oplus \mathbf{C}^t$ with the formula $x \otimes 1 \mapsto (\sigma_1(x), \ldots, \sigma_s(x), \sigma_{s+1}(x), \ldots, \sigma_{s+t}(x))$ extending it by the R-linearity. Then ϕ is an $\mathbf{R}$-algebra isomorphism and $\phi(\mathcal{O}_K \otimes 1)$ is a full (i.e. n-dimensional) lattice in $\mathbf{R}^n = \mathbf{R}^s \oplus \mathbf{C}^t$.

Proof. Choose some irreducible $P(T) \in \mathbf{Q}[T]$ such that $K = \mathbf{Q}_P = \mathbf{Q}[T]/(P)$. The complex roots of P are in one-to-one correspondence with the elements of $\Sigma_{K/\mathbf{Q}}^{\mathbf{C}/\mathbf{Q}}$, so order them in that way. Namely, for $1 \leq i \leq s$ let $\alpha_i = \sigma_i(T)$ while for $s+1 \leq i \leq s+t$ let $(\alpha_i, \overline{\alpha_i}) = (\sigma_i(T), \overline{\sigma_i}(T))$. $K \otimes_{\mathbf{Q}} \mathbf{R}$ may now be identified with $\oplus\, \mathbf{R}[T]/(P_i)$ where $P_i = T - \alpha_i$ for $1 \leq i \leq s$ and $P_i = (T - \alpha_i)(T - \overline{\alpha_i})$ for $s+1 \leq i \leq s+t$ (cf. the proof of the Theorem 3.52). If $i \leq s$ then $\mathbf{R}[T]/((T - \alpha_i)) = \mathbf{R}$ canonically while to identify $\mathbf{R}[T]/((T-\alpha_i)(T-\overline{\alpha_i}))$ with $\mathbf{C}$ for $i > s$ one needs to choose one of $\alpha_i,\ \overline{\alpha_i}$ or, which is the same, one of $\sigma_i,\ \overline{\sigma_i}$. This proves that ϕ is an isomorphism. Any basis of K as a $\mathbf{Q}$-vector space is at the same time a basis of $K \otimes_{\mathbf{Q}} \mathbf{R}$ as an $\mathbf{R}$-vector space. By the Theorem 4.7. $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n containing a basis of K hence any basis of $\mathcal{O}_K$ is a basis of K whence the last statement of the Theorem ■

For what follows we need a simple but important theorem of geometric nature.

Theorem 4.9 (the Minkowski theorem). Suppose $D \subset \mathbf{R}^n$ is a bounded central symmetric convex domain, L a full lattice in $\mathbf{R}^n$. Suppose $\mathrm{vol}\,(D) > 2^n \mathrm{vol}\,(L)$ where $\mathrm{vol}\,(L)$ is the volume of its fundamental parallelotope. Then $\exists\ 0 \neq l \in L$ such that $l \in D$.

Proof. Since $\mathrm{vol}\,\left(\frac{1}{2}D\right) > \mathrm{vol}\,(L)$ there exist $l_1, l_2 \in L,\ l_1 \neq l_2$ such that $l_1 + \frac{1}{2}D \cap l_2 + \frac{1}{2}D \neq \emptyset$ (for the proof see Problem 37). This means that there exist $\frac{x}{2} \in \frac{1}{2}D$ and $\frac{y}{2} \in \frac{1}{2}D$ such that $l_1 + \frac{x}{2} = l_2 + \frac{y}{2}$. Then $l_1 - l_2 = \frac{x-y}{2}$, both x and y lying in D. Since D is central symmetric and convex $\frac{x-y}{2} \in D$ which ends the proof ■

Definition 4.10. The element $\epsilon \in \mathcal{O}_K$ is called a unit of the field K if it is invertible in $\mathcal{O}_K$ (i.e. $\epsilon \in \mathcal{O}_K^*$).

Theorem 4.11 (Dirichlet's unit theorem). $\mathcal{O}_K^* \simeq \mathbf{Z}^{s+t-1} \oplus W$ where s and t are defined in 4.8 while W is a finite group consisting of all roots of 1 in K.

Lemma 1. Any element of finite order in $\mathcal{O}_K^*$ is a root of 1. If $w \in K$ is a root of 1 then $w \in \mathcal{O}_K$. The group W is finite. If $s > 0$ then $W = \{\pm 1\}$.

Proof. First two statements are clear. If $s > 0$ then there exists an inclusion $K \to \mathbf{R}$. Since ± 1 are the only real roots of 1, the last statement folllows. Supose that $s = 0$ and $w \in W$. Then $\phi(w) \in \prod_1^t \{|z| = 1\}$ which is a compact set. Therefore it may contain no more than a finite number of the elements of the lattice $\phi(\mathcal{O}_K)$ ■

Lemma 2. Suppose $\epsilon \in \mathcal{O}_K$. Then $\epsilon \in \mathcal{O}_K^* \Leftrightarrow N_{K/\mathbf{Q}}(\epsilon) = \pm 1$.

Proof. $\Rightarrow$ clear; $\Leftarrow$ $\forall a \in \mathcal{O}_K$ and $\forall \sigma \in \Sigma_{K/\mathbf{Q}}^{\overline{\mathbf{Q}}/\mathbf{Q}}$ $\sigma(a)$ is integral over $\mathbf{Z}$ (while not necessary an element of K). Suppose $\epsilon \in \mathcal{O}_K$ and $N(\epsilon) = \pm 1$. By the Theorem 3.43 $N(\epsilon) = \prod_{\sigma \in \Sigma_{K/\mathbf{Q}}^{\overline{\mathbf{Q}}/\mathbf{Q}}} \sigma(\epsilon)$ hence $N(\epsilon) = \gamma\epsilon$ where γ is integral over $\mathbf{Z}$. But $N(\epsilon) = \pm 1$ by the assumption hence $\gamma \in K$, thus $\gamma \in \mathcal{O}_K$ ■

Lemma 3. Suppose m is a positive integer. Let $\mathcal{O}_{K,m}$ be the set of all $a \in \mathcal{O}_K$ such that $N(a) = \pm m$. Then $\mathcal{O}_{K,m}$ is a union of finite number of orbits with respect to the action of the group $\mathcal{O}_K^*$ by multiplication.

Proof. If $a \in \mathcal{O}_{K,m}$ then $a|m$ in $\mathcal{O}_K$ (as above, $N(a)$ is a product of a with another element of $\mathcal{O}_K$). Suppose $a, b \in \mathcal{O}_{K,m}$ and $a \equiv b \mod m$. Then a and b are on the same orbit of the $\mathcal{O}_K^*$-action. Indeed, since a and b both divide m, the assumption leads to $a|b$ and $b|a$. It remains to prove that the number of residue classes $\mod m$ in $\mathcal{O}_K$ is finite. But $\mathcal{O}_K$ is a free $\mathbf{Z}$-module of rank n hence $m|a$ in $\mathcal{O}_K \Leftrightarrow m|$(all coordinates of a) thus the number in question equals m^n). ■

Definition-Lemma 4. Let $B \subset \mathbf{R}^s \oplus \mathbf{C}^t$ be the set of all points without zero coordinates. Consider the map $l : B \to \mathbf{R}^{s+t}$, $\{x_1, \dots, x_s, x_{s+1}, \dots, x_{s+t}\} \mapsto \{\log|x_1|, \dots, \log|x_s|, 2\log|x_{s+1}|, \dots, 2\log|x_{s+t}|\}$. Now define the "logarithmic map" $l\phi : K^* \to \mathbf{R}^{s+t}$ with the formula $l\phi(a) = (l \circ \phi)(a)$. If $\{u_1, \dots, u_{s+t}\}$ are the coordinates in $\mathbf{R}^{s+t}$ then $\forall a \in K^*$ $\log(|N(a)|) = \sum_{i=1}^{s+t} u_i(l\phi(a))$.

Proof. Since the complex conjugate elements of $\mathbf{C}$ have the same absolute value this is clear ■

Lemma 5. $\ker(l\phi|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to \mathbf{R}^{s+t}) = W$.

Proof. See Problem 38 ■

Definition-Lemma 6.
1) $L_m \stackrel{\text{def}}{=} \{u \in \mathbf{R}^{s+t} \mid \sum_{i=1}^{s+t} u_i = \log(m)\}$.
2) Suppose $z \in \mathcal{O}_K$, $|N(z)| \leq m$. Then $C_{m,z} \stackrel{\text{def}}{=} \{u \in L_m \mid \forall i \;\; u_i \geq u_i(l\phi(z))\}$.

Then $l\phi(\mathcal{O}_{K,m}) \subset L_m$. $C_{m,z}$ is a bounded domain.

Proof. First statement is clear so we only need to prove the second one. By subtracting the vector $l\phi(z)$ one may see that $C_{m,z}$ is congruent to a subset of the $(s+t)$-dimensional real affine space consisting of the points with all positive coordinates the sum of which is fixed. This subset is a $(s+t-1)$-simplex ■

Lemma 7. If m is sufficiently large then $\bigcup_{z \in \mathcal{O}_K,\, |N(z)| \leq m} C_{m,z} = L_m$.

Proof. Suppose $u \in L_m$ is an arbitrary point. To cover u with one of $C_{m,z}$ one needs to find an element $z \in \mathcal{O}_K$ such that $|N(z)| \leq m$, $\quad \forall i \; (1 \leq i \leq s) \;\; \log|\sigma_i(z)| \leq u_i$ and $\forall i \; (s+1 \leq i \leq s+t) \;\; 2\log|\sigma_i(z)| \leq u_i$. It suffices to check the last two inequalities (if z fits both then the condition $|N(z)| \leq m$ is fulfilled automatically by the Lemma 4). Taking the exponents one gets the conditions $|\sigma_i(z)| \leq \exp(u_i)$ (resp. $|\sigma_i(z)|^2 \leq \exp(u_i)$) for $i \leq s$ (resp. $i > s$). These conditions define a bounded central symmetric convex domain in $\mathbf{R}^s \oplus \mathbf{C}^t$. Clearly its volume is a product of $\prod_{i=1}^{s+t} \exp(u_i) = \exp(\sum_{i=1}^{s+t} u_i) = m$ with a constant. Therefore for m sufficiently large the domain above and the lattice $\phi(\mathcal{O}_K)$ satisfy the conditions of the Theorem 4.9 whence the Lemma ■

Lemma 8. $l\phi(\mathcal{O}_K^*)$ is a discrete subgroup of the hyperplane $L_1 \subset R^{s+t}$.

Proof. Suppose the opposite is true. Then there exists a sequence $\epsilon_j \in \mathcal{O}_K^*$ such that $\forall j\ l\phi(\epsilon_j) \neq 0$ while $\lim\limits_{j\to\infty} l\phi(\epsilon_j) = 0$. This means that $\forall i(1 \leq i \leq s+t)\ \lim\limits_{j\to\infty} \log|\sigma_i(\epsilon_j)| = 0$ which implies the coordinates $\sigma_i(\epsilon_j)$ of the lattice points $\phi(\epsilon_j)$ are bounded. Therefore these lattice points are contained in some finite set which contradicts the assumption that $l\phi(\epsilon_j) \neq 0$ and $\lim\limits_{j\to\infty} l\phi(\epsilon_j) = 0$ ■

Proof of the Theorem. $\forall \epsilon \in \mathcal{O}_K^*\ \ C_{m,\epsilon z} = l\phi(\epsilon) + C_{m,z}$. Using Lemma 3 one may conclude that the set $\bigcup\limits_{r=1}^{m} \mathcal{O}_{K,r}$ is a union of a finite number of orbits with respect to the action of $\mathcal{O}_K^*$. Let $Z = \{z_1, \ldots, z_k\}$ be the full set of representatives of the orbits. Choose m sufficiently large for the statement of the Lemma 7 to be valid. Then $L_m = \bigcup\limits_{z\in Z}(\bigcup\limits_{\epsilon\in\mathcal{O}_K^*}(C_{m,z} + l\phi(\epsilon)) = \bigcup\limits_{\epsilon\in\mathcal{O}_K^*}((\bigcup\limits_{z\in Z} C_{m,z}) + l\phi(\epsilon))$. Since all the $C_{m,z}$ are bounded domains the same is their union. Therefore the discrete subgroup $l\phi(\mathcal{O}_K^*) \subset L_1$ must have the rank equal to the dimension of the affine space L_m which is $s+t-1$. Otherwise the shifts of the bounded domain with the vectors of that subgroup could not cover L_m.
We have constructed the surjective group homomorphism $l\phi : \mathcal{O}_K^* \to \mathbf{Z}^{s+t-1}$ such that $\ker(l\phi) = W$ (see Lemma 5). Since $\mathbf{Z}^{s+t-1}$ is free there exists a homomorhism
$\psi : \mathbf{Z}^{s+t-1} \to \mathcal{O}_K^*$ such that $l\phi \circ \psi = (Id)$. Clearly ψ is injective hence its image is also a free commutative group of rank $s+t-1$. If $\epsilon \in \mathcal{O}_K^*$ then $\epsilon = w(\epsilon)\psi(l\phi(\epsilon))$ where $w(\epsilon) \in W$ which ends the proof ■

Remark. The decompositon above is by no means canonical ($w(\epsilon)$ depends on the choice of the homomorphism ψ). So the situation differs from that in $\mathbf{Z}_p^*$ where the root of 1 is canonically defined by the residue of the element.

Now we are going to study the ideals of $\mathcal{O}_K$.

Definition-Theorem 4.12. A finitely generated $\mathbf{Z}$-submodule of K which contains a basis of the $\mathbf{Q}$-vector space K is called a lattice in K. Suppose N is a lattice in K. Then
1) N is a free $\mathbf{Z}$-module of rank n. Any $\mathbf{Z}$-basis of N is a $\mathbf{Q}$-basis of K.
2) Suppose $B \in \mathrm{End}_{\mathbf{Q}}(K)$ is an nondegenerate endomorphism such that $B(N) \subset N$. Then $(N : B(N)) = |\det(B)|$.
3) Let r be a positive integer. Then #(lattices $M \subset K$ such that $N \subset M$ and $(M : N) \mid r$) is finite.
4) Suppose $I \subset \mathcal{O}_K$ is a nonzero ideal. Then I is a lattice in K.
5) $\phi(N)$ is a full lattice (in usual sense) in $\mathbf{R}^n = \mathbf{R}^s \oplus \mathbf{C}^t$.

Proof. 1) Let $\{x_i,\ 1 \leq i \leq r\}$ be a system of generators of N. If $r > n$ then the set of linear relations $\sum_{i=1}^{r} a_i x_i = 0$ with coefficients $a_i \in \mathbf{Q}$ is nonempty. Clearly one may suppose all $a_i \in \mathbf{Z}$. Choose a linear relation containing a term with coefficient of minimal absolute value a_{min}, one may suppose that this term is $a_1 x_1$ without loss of generality. If a_1 divides all other coefficients of this relation then x_1 may be excluded of the set of generators. Otherwise let $a_i = a_i' + ca_1,\ a_i' \neq 0,\ |a_i'| < |a_1|$. Change the generator x_1 to $x_1 + cx_i$. Then $a_1 x_1 + a_i x_i = a_1(x_1 + cx_i) + a_i' x_i$ hence we have constructed another system of generators, the new a_{min} being strictly less. This proves the first statement, the second being afterwards clear ■
2) Choose a basis $\{e_i\}$ of N. $BN \subset N$ and $\mathrm{rk}(BN) = n$ therefore one may construct a basis $\{f_j\}$ of BN such that $\forall j\ f_j = \sum_{i=j}^{n} c_{ji} e_i$ for some matrix C with integer entries c_{ji}. This could be done by induction using the same method as in the proof of the Lemma to the Theorem 4.7 (for the full proof see Problem 39). Clearly one may suppose that all $c_{jj} \geq 0$. Then the set of the elements of N of the form $\sum a_i e_i,\ 0 \leq a_i < c_{ii}$ constitutes a set of representatives of the group N modulo the subgroup BN. Indeed, suppose that two representatives differ by $l = \sum_{j=1}^{n} l_j f_j,\ l_j$ being integer numbers. The first coordinate of l in the basis $\{e_i\}$ equals $l_1 c_{11}$, thus $l_1 = 0$. Since $l_1 = 0$ the second coordinate of l equals $l_2 c_{22}$, thus $l_2 = 0$ and so on, so $l = 0$. Conversely, starting with an arbitrary element $x = \sum_{i=1}^{n} x_i e_i \in N$, one may choose l_1 such that the first coordinate of $x - l_1 f_1$ will sit between 0 and $c_{11} - 1$, then subtract some $l_2 f_2$ to modify the second coordinate (the first one will not change) and so on. Finally, $(N : BN)$ is equal to the number

of representatives, therefore $(N : BN) = \prod_{i=1}^{n} c_{ii} = \det(C)$. Since $\{f_j\}$ is a basis of BN the matrix of B is a product of C with some invertible matrix with integer entries, thus $\det C = \pm \det B$ ■
3) $(M : N) \mid r \Rightarrow \#(M/N) | r \Rightarrow \forall \overline{z} \in M/N \; r\overline{z} = 0 \Rightarrow \forall z \in M \; rz \in N \Rightarrow rM \subset N \Rightarrow M \subset \frac{1}{r}N$. Clearly M is defined by its image in $\frac{1}{r}N/N$, the latter being a finite group ■
4) $\mathcal{O}_K$ is a lattice by the Theorem 4.7 hence I is a free $\mathbf{Z}$-module of rank $\leq n$ by the Lemma to that theorem. Choose $0 \neq a \in I$. Then the principal ideal $a\mathcal{O}_K$ is contained in I and contains some basis of K (as $\mathcal{O}_K$ does) thus $\mathrm{rk}(I) = n$ ■
5) Clearly if $\{e_i\}$ is a $\mathbf{Z}$-basis of N then $\{e_i \otimes 1\}$ is an $\mathbf{R}$-basis of $K \otimes_{\mathbf{Q}} \mathbf{R}$ ■

Definition-Theorem 4.13. The nonzero ideals $I, J \subset \mathcal{O}_K$ are called similar (notation $I \sim J$) iff, equivalently,
1) $\exists\, a, b \in \mathcal{O}_K$ such that $aI = bJ$, or
2) I and J are isomorphic as $\mathcal{O}_K$-modules
Further, $\sim$ is an equivalence relation on the set of the nonzero ideals of $\mathcal{O}_K$.

Proof. Clearly 1) $\Rightarrow$ 2). Suppose now that $\psi : I \to J$ is an isomorphism of $\mathcal{O}_K$-modules. I contains a basis of the $\mathbf{Q}$-vector space K, let $d \in \mathbf{Z}$ be a common denominator of the coordinates of the element $1 \in K$ in that basis. Then $d \in I$ hence $\forall x \in I$ $d\psi(x) = \psi(xd) = x\psi(d)$ which means that $dJ = \psi(d)I$. The last statement is clear. ■

Theorem 4.14. The number of the equivalence classes of ideals of $\mathcal{O}_K$ with respect to the equivalence relation $\sim$ is finite.

Lemma. There exists a positive real constant c which depends only on the field K (more precisely, only on the numbers t and $\mathrm{vol}\,(\phi(\mathcal{O}_K))$) such that for any nonzero ideal $I \subset \mathcal{O}_K$ there exists an element $a_I \in I$ such that $(I : (a_I\mathcal{O}_K)) < c$.

Proof of the Lemma. If $L_2 \subset L_1$ are two lattices in $\mathbf{R}^n$ then $\mathrm{vol}\,(L_2) = (L_1 : L_2)\mathrm{vol}\,(L_1)$. Choose $\{a_i \in \mathbf{R}_{>0}, \;\; 1 \leq i \leq s+t\}$ such that $2^s\pi^t \prod_{i=1}^{s+t} a_i = 2^n \mathrm{vol}\,(\phi(I))(1+\epsilon)$ for some $\epsilon > 0$. Let $\mathbf{R}^s \oplus \mathbf{C}^t \supset D \stackrel{\mathrm{def}}{=} \{|x_i| \leq a_i \text{ for } 1 \leq i \leq s, \;\; |x_i|^2 \leq a_i \text{ for } s+1 \leq i \leq s+t\}$. Then $\mathrm{vol}\,(D) = 2^s\pi^t \prod_{i=1}^{s+t} a_i$ hence by the Minkowski theorem 4.9 there exists a nonzero $z \in I$ such that $\phi(z) \in D$. For that z $\;|N_{K/\mathbf{Q}}(z)| \leq \prod_{i=1}^{s+t} a_i = \left(\frac{4}{\pi}\right)^t \mathrm{vol}\,(\phi(I))(1+\epsilon)$.

Since $(z\mathcal{O}_K) \subset I \subset \mathcal{O}_K$, $(\mathcal{O}_K : I)\mathrm{vol}\,(\phi(\mathcal{O}_K)) = \mathrm{vol}\,(\phi(I)$ and also by the Theorem 4.12.2) $(\mathcal{O}_K : (z\mathcal{O}_K)) = |N_{K/\mathbf{Q}}(z)|$. Using the inequality on the $|N_{K/\mathbf{Q}}(z)|$ above one gets $(I : (z\mathcal{O}_K)) \leq \left(\frac{4}{\pi}\right)^t \mathrm{vol}\,(\phi(\mathcal{O}_K))(1+\epsilon)$ ■

Proof of the Theorem. Suppose $I \subset \mathcal{O}_K$ is a nonzero ideal. Choose a_I from the Lemma. Then $c > (I : (a_I\mathcal{O}_K)) = (a_I^{-1}I : \mathcal{O}_K)$. By the Theorem 4.12.3) no more than a finite number of lattices in K may play the role of $a_I^{-1}I$. Since $I \sim a_I^{-1}I$ this ends the proof ■

Example. Quadratic field. Suppose $K = \mathbf{Q}(\sqrt{d})$, d a squarefree integer.

Theorem 4.15 (calculation of $\mathcal{O}_K$).

If $d \equiv 1 \mod 4$ then $\quad z \in \mathcal{O}_K \Leftrightarrow z = a + b\frac{\sqrt{d}+1}{2},\ \ a, b \in \mathbf{Z}.$
If $d \equiv 2 \text{ or } 3 \mod 4$ then $\quad z \in \mathcal{O}_K \Leftrightarrow z = a + b\sqrt{d},\ \ a, b \in \mathbf{Z}.$

Proof. Suppose $z = \alpha + \beta\sqrt{d},\ \alpha \in \mathbf{Q}, 0 \neq \beta \in \mathbf{Q}$. Then $P_z = T^2 - 2\alpha T + \alpha^2 - d\beta^2$. $z \in \mathcal{O}_K \Leftrightarrow P_z \in \mathbf{Z}[T] \Leftrightarrow$ either $\alpha, \beta \in \mathbf{Z}$ or $\alpha \in \mathbf{Z} + \frac{1}{2}$, $\beta \in \mathbf{Z} + \frac{1}{2}$ and $d \equiv 1 \mod 4$ ■

Theorem 4.16 (group of units).

$$\text{If } d < 0 \text{ then } \mathcal{O}_K^* = W \simeq \begin{cases} \mathbf{Z}/(4), & \text{if } d = -1; \\ \mathbf{Z}/(6), & \text{if } d = -3; \\ \mathbf{Z}/(2) & \text{other } d. \end{cases}$$

If $d > 0$ then $\mathcal{O}_K^* = (W \simeq \mathbf{Z}/(2)) \oplus \mathbf{Z}$.

Proof. For $d > 0$ Theorem 4.11 proves the statement. Suppose $d < 0$. Calculate all $z \in \mathcal{O}_K$ such that $|N(z)| = 1$. If $d \equiv 2 \text{ or } 3 \mod 4$ then $z = a + b\sqrt{d}$ $(a, b \in \mathbf{Z})$ hence $N(z) = a^2 - db^2$, so either $b = 0$ or $d = -1,\ a = 0,\ b = \pm 1$. If $d \equiv 1 \mod 4$ then $z = a + b\frac{\sqrt{d}+1}{2}$ $(a, b \in \mathbf{Z})$, hence $N(z) = a^2 + ab + \frac{1-d}{4}b^2 = \left(a + \frac{b}{2}\right)^2 - \frac{db^2}{4}$, so either $b = 0$ or $d = -3$ (since $|N(z)| = 1$). In the latter case either $a = \pm 1,\ b = 0$ or $a = -b, b = \pm 1$, or else $a = 0, b = \pm 1$ ■

Definition-Theorem 4.17 (calculation of the main unit). $\epsilon \in \mathcal{O}_K^*$ is called a main unit of K iff the image of ϵ generates the group $\mathcal{O}_K^*/\{\pm 1\} \simeq \mathbf{Z}$.
1) Suppose ϵ is a main unit. Then the full list of main units consists of $\epsilon, -\epsilon, \epsilon^{-1}, -\epsilon^{-1}$. The norm of the main unit (+1 or -1) does not depend on the choice.

2) Choose $\phi : K \to \mathbf{R}^2$ such that $\sigma_1 = \mathrm{Id}$ while $\sigma_2(\sqrt{d}) = -\sqrt{d}$, so K may be identified with $\sigma_1(K)$. Let ϵ be the unique main unit such that $\epsilon > 1$. Represent $\epsilon = a + be,\ a, b \in \mathbf{Z},\ e = \sqrt{d}$ if $d \equiv 2\,\mathrm{or}\,3 \mod 4$ (resp. $e = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$). Then $a \geq 0, b > 0$ ($a = 0$ just when $d = 5$). If $r \in \mathbf{Z}_{>1}$ then $\epsilon^r = a_r + b_r e$ where $a_r \geq a$ and $b_r > b$.
3) Let $v_K = \mathrm{vol}\,(\phi(\mathcal{O}_K))$. Then $v_K = 2\sqrt{d}$ if $d \equiv 2\,\mathrm{or}\,3 \mod 4$ (resp. $v_K = \sqrt{d}$ if $d \equiv 1 \mod 4$).
4) If ϵ is a main unit then $|\log(|\epsilon|)| \leq \log(v_K + 1) \sum\limits_{r \leq v_K + 1} r^2$.

Proof. 1) Clear ■
2) Since $N(\epsilon) = \pm 1$ $\sigma_2(\epsilon)$ is also a main unit. Obviously $e - \sigma_2(e) > 0$ while $\epsilon - \sigma_2(\epsilon) > 0$ by the choice of ϵ. Their quotient equals b thus $b > 0$. Since $\epsilon > 1$ $|a + b\sigma_2(e)| = |\sigma_2(\epsilon)| = |\pm\epsilon^{-1}| < 1$. If $d \neq 5$ then $\sigma_2(e) < -1$ hence $a > 0$. If $d = 5$ then e is a main unit. This ends the proof of the first statement, the second being then straightforward ■
3) The vectors (1,1) and $(e, \sigma_2(e))$ form a basis of the lattice $\phi(\mathcal{O}_K)$. The rest is a direct calculation ■
4) Use the notations of the Lemma 5 to the Theorem 4.11. The volume of the rectangle $(|x_1| \leq \exp(u_1), |x_2| \leq \exp(u_2))$ equals $4\exp(u_1 + u_2) = 4m$. Therefore if $4m > 4v_K$ the segments $C_{m,\,z}$ cover the line L_m by the Minkowski Theorem 4.9. The length of each $C_{m,\,z}$ cannot exceed $\sqrt{2}\log(m)$. The total number of $\mathcal{O}_K^*$-orbits in $\bigcup\limits_{r=1}^{m} \mathcal{O}_{K.r}$ cannot exceed $\sum\limits_{r=1}^{m} r^2$ by the Lemma 3 to the Theorem 4.11. Hence L_m is covered by the $l\phi(\epsilon)$-shifts of the certain union of segments of combined length not exceeding $\sqrt{2}\log(m)\sum\limits_{r=1}^{m} r^2$. This is possible only if the length of $l\phi(\epsilon)$ (which equals $\sqrt{2}\log|\epsilon|$) is less or equal. Now choose m such that $v_K < m \leq v_K + 1$. This ends the proof ■

Theorem 4.18 (example of a non-principal ideal).

Let $K = \mathbf{Q}(\sqrt{d}),\ d < 0,\ d \equiv 3 \mod 4,\ d \neq -1$. Let I be the $\mathbf{Z}$-submodule of K generated by 2 and $1 + \sqrt{d}$. Then I is a non-principal ideal in $\mathcal{O}_K$.
Proof. By the Theorem 4.15 $\mathcal{O}_K = \{a + b\sqrt{d},\quad a, b \in \mathbf{Z}\}$. By the definition $I = \{a + b\sqrt{d},\ \ a, b \in \mathbf{Z}$ are of the same parity$\}$. Since $\sqrt{d}\,I = I,\ I$ is an ideal in $\mathcal{O}_K$. Clearly $N(I) = (\mathcal{O}_K : I) = 2$. Suppose that I is a principal ideal. This means that there exists $x + y\sqrt{d} = z \in \mathcal{O}_K$ such that $I = z\mathcal{O}_K$. If this is the case then by the Theorem 4.12.2) $N(I) = |N(z)| = x^2 - dy^2$. Since the equation $x^2 - dy^2 = 2$ has no integer solutions (provided $d < -1$) this leads to a contradiction ■

Problems (the deadline for 36 is November, 10th, for 37-38 November, 17th, for 39-40 November, 24th).

36. Suppose N is a free $\mathcal{O}$-submodule of K of rank n generated by the basis $\{e_i\}$. Prove that the A-module $N^\vee$ is a free $\mathcal{O}$-submodule of K generated by the dual basis $\{f_j\}$.
37. Suppose L is a lattice in $\mathbf{R}^n$, C a bounded domain. Prove that $\mathrm{vol}\,(C) > \mathrm{vol}\,(L)$ implies there exist $l_1, l_2 \in L,\ l_1 \neq l_2$ such that $l_1 + C \cap l_2 + C \neq \emptyset$
38. Prove that $\ker(l\phi|_{\mathcal{O}_K^*} : \mathcal{O}_K^* \to \mathbf{R}^{s+t}) = W$.
39. Finish the proof of the Theorem 4.12.2) (i.e. prove that any sublattice of $\mathbf{Z}^n$ admits a basis with upper triangle generating matrix).
40. Calculate the main unit of $K = \mathbf{Q}(\sqrt{6})$.