14 Dirichlet's unit theorem

Let K be a number field with ring of integers $\mathcal{O}_K$. The two main theorems of classical algebraic number theory are:

(1) The class group $\operatorname{cl}\mathcal{O}_K$ of a number field is finite.

(2) The unit group $\mathcal{O}_K^\times$ of a number field is finitely generated of rank $r+s-1$.

We proved (1) in Lecture 13, along with several other finiteness results. Today we will prove (2), which is known as Dirichlet's Unit Theorem. Dirichlet (1805–1859) died five years before Minkowski (1864–1909) was born, so he did not have Minkowski's Lattice Point Theorem to work with. But we do, and we won't be shy about using it; this makes the proof of Dirichlet's theorem easier for us than it was for him.

14.1 The group of multiplicative divisors of a global field

As in previous lectures we use M_K to denote the set of places (equivalence classes of absolute values) of a global field K, and for each $v \in M_K$ we use $\| \|_v$ to denote the normalized absolute value for v, which we recall is not an absolute value when v is a complex place (it is the square of the usual absolute value on $\mathbb{C}$), but it is multiplicative and compatible with the topology on K_v (see Remark 12.31).

Definition 14.1. Let K be a global field. An *M_K-divisor* is a sequence of positive real numbers $c = (c_v)$ indexed by $v \in M_K$ such that for all $v < \infty$ we have $c_v = \|x\|_v$ for some $x \in K^\times$, and $c_v = 1$ for all but finitely many v. The set of M_K-divisors is an abelian group under multiplication $(c_v)(d_v) := (c_v d_v)$. The multiplicative group $K^\times$ is canonically embedded in M_K via the map $x \mapsto (\|x\|_v)$; such M_K-divisors are said to be *principal*, and the form a subgroup. The *size* of an M_K-divisor is the real number

$$\|c\| := \prod_{v \in M_K} c_v \in \mathbb{R}_{>0},$$

and we note that the map from the group of M_K-divisors to $\mathbb{R}^\times$ defined by $c \mapsto \|c\|$ is group homomorphism that contains the subgroup of principal M_K-divisors in its kernel (by the product formula). Corresponding to each M_K-divisor c is a subset $L(c)$ of K defined by

$$L(c) := \{x \in K : \|x\|_v \le c_v \text{ for all } v \in M_K\}.$$

Remark 14.2. M_K-divisors are the multiplicative analog of divisors of a smooth projective curve X/k. Recall that a divisor $D \in \operatorname{Div} X$ is a formal sum $D = \sum n_P P$ over the closed points of the curve X ($\operatorname{Gal}(\bar{k}, k)$-orbits of projective points, equivalently, maximal ideals in the coordinate ring of some affine piece of X), where each $n_P \in \mathbb{Z}$ and all but finitely many n_P are zero. Associated to each divisor is the *Riemann-Roch space*

$$L(D) := \{f \in k(X) : v_P(f) \ge -n_P \text{ for all closed points } P \in X\},$$

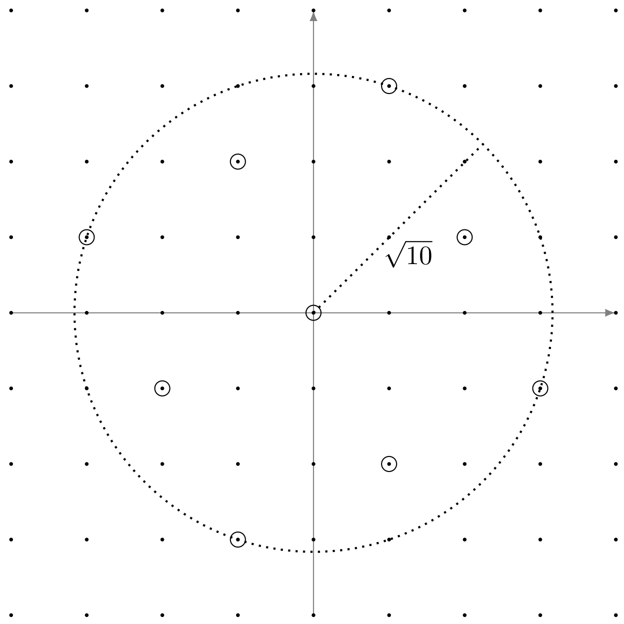
which is a k-vector space of finite dimension. If k is a finite field then $K = k(X)$ is a global field and there is a one-to-one correspondence between closed points of X and places in M_K, and a normalized absolute value $\| \|_P$ for each closed point P (indeed, one can take this as a definition). The constraint $v_P(f) \ge -n_P$ is equivalent to $\|f\|_P \le (\#\kappa(P))^{n_P}$, where

Lecture by Andrew Sutherland

$\kappa(P)$ is the residue field. If we let $c_P := (\#\kappa(P))^{n_P}$ then $c = (c_P)$ is an M_K-divisor with $L(c) = L(D)$. The Riemann-Roch space $L(D)$ is finite (since k is finite), and we will prove below that this also holds for $L(c)$ when K is a number field; in this case $L(c)$ is not a vector space, but it is a finite set.

In §6.2 we described the divisor group Div X as the additive analog of the ideal group $\mathcal{I}_A$ of the ring of integers $A = \mathcal{O}_K$ (equivalently, the coordinate ring $A = k[X]$) of the global function field $K = k(X)$. This is correct when X is an affine curve, but here X is a smooth projective curve and has "points at infinity" corresponding to places in M_K that do not arise from prime ideals of $\mathcal{O}_K$ but do arise from discrete valuations on K (in contrast to the number field case, these "places at infinity" are nonarchimedean). Taking the projective closure of an affine curve corresponds to including all the factors in the product formula and is precisely what is needed to ensure that principal divisors have degree 0 (every function $f \in k(X)$ has the same number of zeros and poles, when counted correctly).

Example 14.3. Let $K = \mathbb{Q}(i)$. The ideal $(2+i)$ lying above 5 is prime and corresponds to a nonarchimedean place $v_1 < \infty$, and there is a unique archimedean place $v_2|\infty$ which is complex. Let $c_{v_1} = 1/5$, let $c_{v_2} = 10$, and set $c_v = 1$ for all other $v \in M_K$. The image of $L(c) = \{x \in (2+i) : |x|_\infty \leq 10\}$ under the canonical embedding $K \hookrightarrow K_\mathbb{R} \simeq \mathbb{C}$ is the set of lattice points in the ideal $(2+i)$ that lie within a circle of radius $\sqrt{10}$ in the complex plane. Note that $\|x\|_{v_2}$ is the square of the usual absolute value on $\mathbb{C}$, which is why the circle has radius $\sqrt{10}$ rather than 10.



The set $L(c)$ is clearly finite; it contains exactly 9 points.

Now let K be a number field with ring of integers $\mathcal{O}_K$ and let c be an M_K-divisor. We may associate to c a fractional ideal of $\mathcal{O}_K$

$$I_c := \prod_{v<\infty} \mathfrak{q}_v^{-v(c_v)}$$

which we note contains the set $L(c)$. We then have

$$\|c\| = \mathrm{N}(I_c)^{-1} \prod_{v|\infty} c_v, \tag{1}$$

where $\mathrm{N}(I_c)$ is the absolute norm (a positive generator for $\mathrm{N}_{K/\mathbb{Q}}(I_c)$). We also define

$$R_c := \{x \in K_{\mathbb{R}} : |x|_v \le c_v \text{ for all } v|\infty\},$$

which we note is compact, convex, symmetric subset of the real vector space

$$K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n,$$

where $n = r + 2s = [K : \mathbb{Q}]$, r is the number of real places in M_K, and s is the number of complex places (pairs of distinct complex conjugate embeddings $\{\sigma, \bar{\sigma}\} \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$).

Lemma 14.4. *Let c be an M_K-divisor of a number field K. Then $L(c)$ is a finite set.*

Proof. Let Λ_c be the image of I_c under the canonical embedding $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = K_{\mathbb{R}}$; then the image of $L(c)$ in $K_{\mathbb{R}}$ is equal to $\Lambda_c \cap R_c$. The free $\mathbb{Z}$-module Λ_c is a lattice in $K_{\mathbb{R}}$, and in particular, discrete, so its intersection with the compact set R_c is finite. □

Proposition 14.5. *Let K be a number field of degree $n = r + 2s$, with r real places and s complex places. Define*

$$B_K := \frac{\sqrt{|\operatorname{disc} \mathcal{O}_K|}}{2^r(2\pi)^s} 2^n,$$

and let c be any M_K-divisor for which $\|c\| > B_K$. Then $L(c)$ contains an element of $K^\times$.

Proof. Let Λ_c be the image of the fractional ideal $I_c \subseteq K$ in $K_{\mathbb{R}}$. We apply Minkowski's lattice point theorem to the convex symmetric set $S := R_c$ and lattice Λ_c in $K_{\mathbb{R}}$. Let μ be the normalized Haar measure on $K_{\mathbb{R}}$; as explained in 13.2 this means that $\mu(S) = 2^s \mu_{\mathbb{R}^n}(S)$, where $\mu_{\mathbb{R}^n}$ is the standard Lebesgue measure on $\mathbb{R}^n \simeq K_{\mathbb{R}}$. For real places $v \in M_K$ the constraint $|x|_v \le c_v$ contributes a factor of $2c_v$ to $\mu_{\mathbb{R}^n}(S)$, and for complex $v \in M_K$ the constraint $|x|_v = |x|^2 \le c_v$ contributes a factor of πc_v (area of a circle of radius $\sqrt{c_v}$). Thus

$$\begin{aligned}
\frac{\mu(S)}{\operatorname{covol}(\Lambda_c)} &= \frac{2^s \mu_{\mathbb{R}^n}(S)}{\operatorname{covol}(\Lambda_c)} = \frac{2^s \left(\prod_{v \text{ real}} 2c_v\right)\left(\prod_{v \text{ complex}} \pi c_v\right)}{\operatorname{covol}(\Lambda_c)} \\
&= \frac{2^r (2\pi)^s \prod_{v|\infty} c_v}{\sqrt{|\operatorname{disc} \mathcal{O}_K|} N(I)} = \frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc} \mathcal{O}_K|}} \|c\| = \frac{\|c\|}{B_K} 2^n > 2^n
\end{aligned}$$

where we used Corollary 13.15 and (1) in the second line. Corollary 13.12 implies that $S = R_c$ contains a nonzero element of Λ_c; therefore $L(c)$ contains an element of $K^\times$. □

Remark 14.6. The bound in Proposition 14.5 can be turned into an asymptotic, that is, for M_K-divisors c, as $\|c\| \to \infty$ we have

$$\#L(c) = \left(\frac{2^r(2\pi)^s}{\sqrt{|\operatorname{disc} \mathcal{O}_K|}} + o(1) \right) \|c\|. \tag{2}$$

This can be viewed as an analog of the Riemann-Roch theorem for function fields, which states that for divisors $D = \sum n_P P \in \operatorname{Div} K$, as $\deg D := \sum n_P \to \infty$ we have

$$\dim_k L(D) = 1 - g + \deg D. \tag{3}$$

The constant g is the *genus*, an important invariant of the function field K which is often defined by (3); one could similarly use (2) to define $|\operatorname{disc} \mathcal{O}_K|$, equivalently, the discriminant ideal $D_{K/\mathbb{Q}}$. For sufficiently large $\|c\|$ the $o(1)$ error term will be small enough so that (2) uniquely determines $|\operatorname{disc} \mathcal{O}_K| \in \mathbb{Z}$. Conversely, with a bit more work one can adapt the proofs of Lemma 14.4 and Proposition 14.5 to give a proof of the Riemann-Roch theorem for global function fields.

14.2 The unit group of a number field

Let K be a number field with ring of integers $\mathcal{O}_K$. The multiplicative group $\mathcal{O}_K^\times$, the group of units in $\mathcal{O}_K$, is the *unit group* of $\mathcal{O}_K$, and (as an abuse of terminology) of K; of course the unit group of K is $K^\times = K - \{0\}$, but this abuse of language is standard and generally causes no harm; one usually refers to $K^\times$ as the multiplicative group of a field K, not its unit group.

Let us now define the topological group

$$K_{\mathbb{R}}^\times := \prod_{\text{real } v|\infty} \mathbb{R}^\times \prod_{\text{complex } v|\infty} \mathbb{C}^\times,$$

which we view as a subset of $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s$ with elements represented as tuples $(x_v)_{v|\infty}$ consisting of r real numbers and s complex numbers. Multiplication is defined componentwise, and we give $K_{\mathbb{R}}^\times$ the subspace topology from $K_{\mathbb{R}}$ (which makes multiplication and inversion continuous). Note that the topologies on $\mathbb{R}^n$ and $\mathbb{R}^r \times \mathbb{C}^s$ are identical under the map that sends pairs (x, y) of real numbers to the complex number $x + iy$; the multiplication is different, but it is continuous in both cases.

We now define a surjective morphism of locally compact groups

$$\begin{aligned} \operatorname{Log}\colon K_{\mathbb{R}}^\times &\to \mathbb{R}^{r+s} \\ (x_v) &\mapsto (\log \|x_v\|_v). \end{aligned}$$

The map is continuous because $\log\colon \mathbb{R}^\times \to \mathbb{R}$ is continuous, and it is a homomorphism because $\log \|x_v y_v\|_v = \log(\|x_v\|_v \|y_v\|_v) = \log \|x_v\|_v + \log \|y_v\|_v$; note that we are using the fact that the normalized absolute value $\|\ \|_v$ is multiplicative (even when it is not an absolute value). We may embed $K^\times$ in $K_{\mathbb{R}}^\times$ via the map $x \mapsto (\sigma_v(x))_v$, by fixing a choice of $\sigma_v \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ corresponding to each archimedean place $v|\infty$. When v is real there is only one choice for σ_v, but when v is complex there are two choices which are complex conjugates. No matter which we pick, the induced map $\operatorname{Log}\colon K^\times \to \mathbb{R}^{r+s}$ is uniquely determined, since

$$\|\sigma_v(x)\|_v = |\sigma_v(x)|^2 = \sigma_v(x)\bar{\sigma}_v(x).$$

We then have a commutative diagram of locally compact groups:

$$\begin{tikzcd}
K^\times \arrow[r, hook] \arrow[d, "\mathrm{N}_{K/\mathbb{Q}}"] & K_{\mathbb{R}}^\times \arrow[r, "\operatorname{Log}"] \arrow[d, "\mathrm{N}"] & \mathbb{R}^{r+s} \arrow[d, "\mathrm{T}"] \\
\mathbb{Q}^\times \arrow[r, hook] & \mathbb{R}^\times \arrow[r, "\log|\ |"] & \mathbb{R},
\end{tikzcd}$$

where the norm map $\mathrm{N}\colon K_{\mathbb{R}}^\times \to \mathbb{R}^\times$ is defined by

$$\mathrm{N}(x) := \prod_{v \text{ real}} x_v \prod_{v \text{ complex}} \|x_v\|_v = \prod_{v \text{ real}} x_v \prod_{v \text{ complex}} x_v \bar{x}_v,$$

and the trace map $\mathrm{T}\colon \mathbb{R}^{r+s} \to \mathbb{R}$ is defined by $\mathrm{T}(x) = \sum_i x_i$.

To check commutativity of the left square, note that for all $x \in K^\times$ we have

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(x) = \prod_{v \text{ real}} \sigma_v(x) \prod_{v \text{ complex}} \sigma_v(x)\bar{\sigma}_v(x) = \mathrm{N}((\sigma_v(x))_v),$$

To check the commutativity of the diagram as a whole, note that for all $x \in K^\times$ we have

$$\begin{aligned}
\log|\mathrm{N}_{K/\mathbb{Q}}(x)| &= \sum_{\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \log|\sigma(x)|\\
&= \sum_{v\text{ real}} \log|\sigma_v(x)| + \sum_{v\text{ complex}} (\log|\sigma_v(x)| + \log|\bar\sigma_v(x)|)\\
&= \sum_{v\text{ real}} \log|\sigma_v(x)| + \sum_{v\text{ complex}} \log|\sigma_v(x)|^2\\
&= \sum_{v\text{ real}} \log\|\sigma_v(x)\|_v + \sum_{v\text{ complex}} \log\|\sigma_v(x)\|_v\\
&= \mathrm{T}((\sigma_v(x))_v).
\end{aligned}$$

independent of the choices for σ_v that we used to embed $K^\times$ in $K_{\mathbb{R}}^\times$. Note that it is crucial here that we used the normalized absolute value $\|\ \|_v$ when defining Log. In view of the commutativity of the above diagram, we may also view Log as a map from $K^\times$ to $\mathbb{R}^{r+s}$ via the embedding $K^\times \hookrightarrow K_{\mathbb{R}}^\times$, and similarly view $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$ as a map from $K^\times$ to $\mathbb{R}^\times$. We can then succinctly summarize the commutative of the whole diagram by writing

$$\mathrm{T}(\mathrm{Log}(x)) = \log|\mathrm{N}(x)|$$

for all $x \in K^\times$ (and for all $x \in K_{\mathbb{R}}^\times$).

We now note that elements of the unit group $\mathcal{O}_K^\times$ all have norm ±1, since their norms must be units in $\mathbb{Z}$; they therefore lie in the kernel of the map $x \mapsto \log|\mathrm{N}(x)|$ and therefore also in the kernel of $x \mapsto \mathrm{T}(\mathrm{Log}(x))$. This implies that $\mathrm{Log}(\mathcal{O}_K^\times)$ is a subgroup of the *trace zero hyperplane*

$$\mathbb{R}_0^{r+s} := \{x \in \mathbb{R}^{r+s} : \mathrm{T}(x) = 0\},$$

which we note is both a subgroup of $\mathbb{R}^{r+s}$, and an $\mathbb{R}$-vector subspace of dimension $r+s-1$, by the linearity of the trace map T.

Proposition 14.7. *Let K be a number field with r real and s complex places, and let Λ_K be the image of the unit group $\mathcal{O}_K^\times$ in $\mathbb{R}^{r+s}$ under the* Log *map. The following hold:*

1. *We have a split exact sequence of abelian groups*

$$0 \to (\mathcal{O}_K^\times)_{\mathrm{tors}} \to \mathcal{O}_K^\times \xrightarrow{\mathrm{Log}} \Lambda_K \to 0;$$

2. *The torsion subgroup $(\mathcal{O}_K^\times)_{\mathrm{tors}}$ of the unit group is finite;*
3. *Λ_K is a lattice in the trace zero hyperplane $\mathbb{R}_0^{r+s}$.*

Proof. Let Z be the kernel of $\mathcal{O}_K^\times \xrightarrow{\mathrm{Log}} \Lambda_K$. To prove (1) we first show $Z = (\mathcal{O}_K^\times)_{\mathrm{tors}}$. Let c be the M_K-divisor with $I_c = \mathcal{O}_K$ and $c_v = 2$ for $v|\infty$, so that

$$L(c) = \{x \in \mathcal{O}_K : \|x\|_v \le 2 \text{ for all } v|\infty\}.$$

For $x \in \mathcal{O}_K^\times$ we have

$$x \in L(c) \Longleftrightarrow \mathrm{Log}(x) \in \mathrm{Log}\, R_c = \{z \in \mathbb{R}^{r+s} : z_i \le \log 2\}.$$

The set on the RHS includes the zero vector, thus $Z \subseteq L(c)$, which by Lemma 14.4 is a finite set. As a finite subgroup of $\mathcal{O}_K^\times$, we must have $Z \subseteq (\mathcal{O}_K^\times)_{\rm tors}$.

Now Λ_K is a subgroup of $\mathbb{R}^{r+s}$, hence torsion free, so the image of $(\mathcal{O}_K^\times)_{\rm tors}$ in Λ_K must be $\{0\}$. Thus $(\mathcal{O}_K^\times)_{\rm tors} \subseteq Z$ and $Z = (\mathcal{O}_K^\times)_{\rm tors}$ as claimed; this also proves (2) since $Z \subseteq L(c)$ is finite. It follows that the sequence in (1) is exact, and since $(\mathcal{O}_K^\times)_{\rm tors}$ is torsion and Λ_K is free, it must split (by the structure theorem for finite abelian groups); this proves (1).

For (3) we note that $\Lambda_K \cap \operatorname{Log}(R_c) = \operatorname{Log}\left(\mathcal{O}_K^\times \cap L(c)\right)$ is a finite set, since $L(c)$ is finite; it follows that 0 is an isolated point of Λ_K in $\mathbb{R}^{r+s}$, and in in the subgroup $\mathbb{R}_0^{r+s}$, therefore Λ_K is a discrete subgroup of $\mathbb{R}_0^{r+s}$. It remains only to show that it spans $\mathbb{R}_0^{r+s}$ (this will imply it is cocompact and therefore a lattice, by Proposition 13.2).

Let V be the subspace of $\mathbb{R}_0^{r+s}$ spanned by Λ_K. If $\dim V < \dim \mathbb{R}_0^{r+s}$ then $\mathbb{R}_0^{r+s}$ contains a unit vector w orthogonal to V. For every $\lambda \in \mathbb{R}_{>0}$ the open ball of radius λ about λw does not intersect Λ_K; thus we can find points in $\mathbb{R}_0^{r+s}$ that are arbitrarily far away from every point in Λ_K. To prove that Λ_K spans $\mathbb{R}_0^{r+s}$ it suffices to show that there is an upper bound on the maximum distance between any point $h \in \mathbb{R}_0^{r+s}$ and the closest point in Λ_K.

Fix $B > B_K$, where B_K is as in Proposition 14.5, so that every M_K-divisor c with $\|c\| \geq B$ has $L(c)$ containing a nonzero element. Let $(\alpha_1), \ldots, (\alpha_m)$ be the list of all nonzero principal ideals with $\mathrm{N}(\alpha_j) \leq B$ (this is a finite list, by Lemma 13.19). Fix a vector $b \in \mathbb{R}^{r+s}$ for which $\mathrm{T}(b) = \sum_i b_i = \log B$. Notice that the bound B_K, the generators α_j, and the vector b have all been fixed independent of any particular h.

Now let h be a point in $\mathbb{R}_0^{r+s}$, and define the M_K divisor c by $I_c := \mathcal{O}_K$ and for $v|\infty$ let $c_v := \exp(h_i + b_i)$, where i is the coordinate in $\mathbb{R}^{r+s}$ corresponding to v under the Log map. Noting that $\mathrm{T}(h) = 0$ (because $h \in \mathbb{R}_0^{r+s}$), we have

$$\|c\| = \prod_v c_v = \exp\Bigl(\sum_i (h_i + b_i)\Bigr) = \exp(\mathrm{T}(h+b)) = \exp(\mathrm{T}(h) + \mathrm{T}(b)) = \exp(\mathrm{T}(b)) = B > B_K,$$

so $L(c)$ contains a nonzero $\gamma \in \mathcal{O}_K$, by Proposition 14.5. Let $g = \operatorname{Log}(\gamma) \in \mathbb{R}^{r+s}$. For $1 \leq i \leq r+s$ we have $g_i \leq \log c_v = h_i + b_i$, where $v|\infty$ is the place corresponding to the index i, and therefore

$$\log |\mathrm{N}(\gamma)| = \mathrm{T}(\operatorname{Log}(\gamma)) \leq \mathrm{T}(h+b) = \mathrm{T}(b) = \log B,$$

thus $|N(\gamma)| \leq B$ and we must have $(\gamma) = (\alpha_j)$ for one of the α_j fixed above. Then $\gamma/\alpha_j \in \mathcal{O}_K^\times$ is a unit, and

$$\operatorname{Log}(\gamma/\alpha_j) = \operatorname{Log}(\gamma) - \operatorname{Log}(\alpha_j) \in \Lambda_K.$$

Now b was fixed independent of h, so the vector $g = \operatorname{Log}(\gamma)$ is within a bounded distance of h, and the α_j were also fixed independent of h, so the vector $\operatorname{Log}(\gamma/\alpha_j) \in \Lambda_K$ is also within a bounded distance of h, and this bound is independent of h. It follows that there is some absolute constant C such that every $h \in \mathbb{R}_0^{r+s}$ there is an element of Λ_K within a distance C of h; therefore Λ_K must span $\mathbb{R}_0^{r+s}$ as desired. □

Dirichlet's unit theorem follows is an immediate corollary of Proposition 14.7.

Theorem 14.8 (Dirichlet Unit Theorem). *Let K be a number field with r real and s complex places. The unit group $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$.*

Proof. The image of the torsion-free part of the unit group $\mathcal{O}_K^\times$ under the Log map is the (full) lattice Λ_K in the trace-zero hyperplane $\mathbb{R}_0^{r+s}$, which has dimension $r+s-1$. □

Example 14.9. Let $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ with $d > 1$ squarefree. Then $r = 2$ and $s = 0$ and the unit group $\mathcal{O}_K^\times$ has rank $r + s - 1 = 1$. The only torsion elements of $\mathcal{O}_K^\times \subseteq \mathbb{R}$ are ± 1, thus

$$\mathcal{O}_K^\times = \{\pm\epsilon^n : n \in \mathbb{Z}\},$$

for some $\epsilon \in \mathcal{O}_K^\times$ of infinite order. We may assume $\epsilon > 1$: if $\epsilon < 0$ then replace ϵ by $-\epsilon$, and if $\epsilon < 1$ then replace ϵ by ϵ^{-1} (we cannot have $\epsilon = 1$).

The assumption $\epsilon > 1$ uniquely determines ϵ. This follows from the fact that for $\epsilon > 1$ we have $|\epsilon^n| > |\epsilon|$ for all $n > 1$ and $|\epsilon^n| \le 1$ for all $n \le 0$.

This unique ϵ is called the *fundamental unit* of $\mathcal{O}_K$ (and of K). To explicitly determine ϵ, let $D = \operatorname{disc} \mathcal{O}_K$ (this means $D = d$ for $d = 1 \bmod 4$ and $D = 4d$ otherwise). Every element of $\mathcal{O}_K$ can be uniquely written as

$$\frac{x + y\sqrt{D}}{2},$$

where x and Dy are integers of the same parity. In the case of a unit we must have $\mathrm{N}(\frac{x+y\sqrt{D}}{2}) = \pm 1$, equivalently,

$$x^2 - Dy^2 = \pm 4. \tag{4}$$

Conversely, any solution $(x, y) \in \mathbb{Z}^2$ to the above equation has x and Dy with the same parity and corresponds to an element of $\mathcal{O}_K^\times$. The constraint $\epsilon = \frac{x+y\sqrt{D}}{2} > 1$ forces $x, y > 0$. This follows from the fact that $\epsilon^{-1} = \frac{|x-y\sqrt{D}|}{2} < 1$, so $-2 < x - y\sqrt{D} < 2$, and then adding and subtracting $x + y\sqrt{D} > 2$ shows $x > 0$ and $y > 0$ (respectively).

Thus we need only consider positive integer solutions (x, y) to (4). Among such solutions, $x_1 + y_1\sqrt{D} < x_2 + y_2\sqrt{D}$ implies $x_1 < x_2$, so the solution that minimizes x will give us the fundamental unit ϵ.

Equation (4) is a (generalized) *Pell equation*. Solving the Pell equation is a well-studied problem and there are a number of algorithms for doing so. The most well known uses continued fractions and is explored on Problem Set 7; this is not the most efficient method, but it is dramatically faster than an exhaustive search; see [1] for a comprehensive survey. A remarkable feature of this problem is that even when D is quite small, the smallest solution to (4) may be very large. For example, when $D = d = 889$ the fundamental unit is

$$\epsilon = \frac{26463949435607314430 + 887572376826907008\sqrt{889}}{2}.$$

14.3 The regulator of a number field

Let K be a number field with r real places and s complex places, and let $\mathbb{R}_0^{r+s}$ be the trace-zero hyperplane in $\mathbb{R}^{r+s}$. Choose any coordinate projection $\pi\colon \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$, and use the induced isomorphism $\mathbb{R}_0^{r+s} \xrightarrow{\sim} \mathbb{R}^{r+s-1}$ to endow $\mathbb{R}_0^{r+s}$ with a Euclidean measure. By Proposition 14.7, the image Λ_K of the unit group $\mathcal{O}_K^\times$ is a lattice in $\mathbb{R}_0^{r+s}$, and we can measure its covolume using the Euclidean measure on $\mathbb{R}_0^{r+s}$.

Definition 14.10. The *regulator* of a number field K is

$$R_K := \operatorname{covol}(\pi(\operatorname{Log}(\mathcal{O}_K^\times))) \in \mathbb{R}_{>0},$$

where $\pi\colon \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$ is any coordinate projection. The real number R_K does not depend on the choice of π. If $\epsilon_1, \ldots, \epsilon_{r+s-1}$ is a fundamental system of units (a $\mathbb{Z}$-basis for the free part of $\mathcal{O}_K^\times$), then R_K can be computed as the absolute value of the determinant of any $(r+s-1)\times(r+s-1)$ minor of the $(r+s)\times(r+s-1)$ matrix whose columns are the vectors $\operatorname{Log}(\epsilon_i)\in\mathbb{R}^{r+s}$.

Example 14.11. If K is a real quadratic field with discriminant $D=\operatorname{disc}\mathcal{O}_K$ and fundamental unit $\epsilon=\frac{x+y\sqrt{D}}{2}$, then $r+s=2$ and the product of the two real embeddings $\sigma_1(\epsilon),\sigma_2(\epsilon)\in\mathbb{R}$ is $\mathrm{N}(\epsilon)=\pm1$. Thus $\log|\sigma_2(\epsilon)|=-\log|\sigma_1(\epsilon)|$ and

$$\operatorname{Log}(\epsilon)=(\log|\sigma_1(\epsilon)|,\log|\sigma_2(\epsilon)|)=(\log|\sigma_1(\epsilon)|,-\log|\sigma_1(\epsilon)|).$$

Both 1×1 minors of the 2×1 transpose of $\operatorname{Log}(\epsilon)$ have determinant $\pm\log|\sigma_1(\epsilon)|$; the absolute value of the determinant does not depend on the minor we pick.

References

[1] Michael J. Jacobson and Hugh C. Williams, *Solving the Pell equation*, Springer, 2009.

18.785 Number Theory I
Fall 2015