15 Dirichlet's unit theorem

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

- The class group $\operatorname{cl}\mathcal{O}_K$ is finite.
- The unit group $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$.

We proved the first result in the previous lecture; in this lecture we prove the second, 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 (Theorem 14.10) to work with. But we do, and we won't be shy about using it; this simplifies the proof considerably.

15.1 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. For each place $v \in M_K$ we use K_v to denote the completion of K with respect to v (a local field), and we have a normalized absolute value $\|\ \|_v\colon K_v \to \mathbb{R}_{\geq 0}$ defined by

$$\|x\|_v := \frac{\mu(xS)}{\mu(S)},$$

where μ is a Haar measure on K_v and $\mu(S) \neq 0$. This definition does not depend on the choice of μ or S, it is determined by the topology of K_v (see Definition 13.17).

When K_v is nonarchimedean its topology is induced by a discrete valuation that we also denote v, and we use k_v to denote its residue field (to the quotient of its valuation ring by its maximal ideal), which is a finite field (Proposition 9.7). In Lecture 13 we showed that

$$\|x\|_v = \begin{cases} |x|_v = (\#k_v)^{-v(x)} & \text{if } v \text{ is nonarchimedean,}\\ |x|_{\mathbb{R}} & \text{if } K_v \simeq \mathbb{R},\\ |x|_{\mathbb{C}}^2 & \text{if } K_v \simeq \mathbb{C}\end{cases}$$

While $\|\ \|_v$ is not always an absolute value (if $K_v \simeq \mathbb{C}$ it does not satisfy the triangle inequality), it is always multiplicative and defines a continuous homomorphism $K_v^\times \to \mathbb{R}_{>0}^\times$ of locally compact groups that is surjective precisely when v is archimedean.

Definition 15.1. Let K be a global field. An M_K*-divisor* (or *Arakelov divisor*) is a sequence of positive real numbers $c = (c_v)$ indexed by $v \in M_K$ with all but finitely many $c_v = 1$ and $c_v \in \|K_v^\times\|_v := \{\|x\|_v : x \in K_v^\times\}$.[1] The set $\operatorname{Div} K$ of all 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 $\operatorname{Div} K$ via the map $x \mapsto (\|x\|_v)$; such M_K-divisors are said to be *principal*, and they form a subgroup.

Remark 15.2. The quotient of $\operatorname{Div} K$ by its subgroup of principal divisors is the *Arakelov class group*, which can be viewed as an extension of the ideal class group $\operatorname{cl}\mathcal{O}_K$ (as defined below, each M_K-divisor c has an associated fractional ideal I_c). Some authors define $\operatorname{Div} K$ (and the Arakelov class group) as additive groups by taking logarithms. We are specifically interested in the multiplicative group $\mathcal{O}_K^\times$, so we prefer to define $\operatorname{Div} K$ multiplicatively.

[1] When v is archimedean we have $\|K_v^\times\| = \mathbb{R}_{>0}$ and this constraint is automatically satisfied.

Definition 15.3. Let K be a global field. The *size* of an M_K-divisor is the real number

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

The map $\operatorname{Div} K \to \mathbb{R}_{>0}^{\times}$ defined by $c \mapsto \|c\|$ is a group homomorphism that contains the subgroup of principal M_K-divisors in its kernel (by the product formula, Theorem 13.21). Corresponding to each M_K-divisor c is a subset $L(c)$ of K defined by

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

We also associate to c a fractional ideal of $\mathcal{O}_K$ defined by

$$I_c := \prod_{v\nmid\infty} \mathfrak{q}_v^{v(c)},$$

where $\mathfrak{q}_v := \{a \in \mathcal{O}_K : v(a) \ge 0\}$ is the prime ideal corresponding to the discrete valuation v that induces $\|\ \|_v$, and $v(c) := -\log_{\#k_v}(c_v) \in \mathbb{Z}$ is the unique integer for which $v(x) = v(c)$ for all $x \in K_v^{\times}$ for which $\|x\|_v = (\#k_v)^{-v(x)} = c_v$. The fractional ideal I_c contains $L(c)$, and the map $c \mapsto \mathcal{I}_c$ is a group homomorphism $\operatorname{Div} K \to \mathcal{I}_{\mathcal{O}_K}$.

Remark 15.4. The set $L(c)$ associated to an M_K-divisor c is directly analogous to the *Riemann-Roch space*

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

associated to a divisor $D \in \operatorname{Div} X$ of a smooth projective curve X/k, which is a k-vector space of finite dimension. Recall that the divisor D is a formal sum $D = \sum n_P P$ over the closed points ($\operatorname{Gal}(\bar{k}/k)$-orbits) of the curve X where each $n_P \in \mathbb{Z}$ and all but finitely many n_P are zero.

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 $\kappa(P)$ is the residue field corresponding to P. 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 $L(c)$ is also finite (when K is a number field $L(c)$ is not a vector space, but it is a finite set.

In §6.3 we described the divisor group $\operatorname{Div} X$ 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 infinite places of M_K (those that do not correspond to primes ideals of $\mathcal{O}_K$). 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).

We now specialize to the case where K is a number field. Recall that the *absolute norm* $\mathrm{N}(I)$ of a fractional ideal of $\mathcal{O}_K$ is the unique $t \in \mathbb{Q}_{>0}$ for which $N_{\mathcal{O}_K/\mathbb{Z}}(I) = (t)$. We have

$$\mathrm{N}(I_c) = \prod_{v\nmid\infty} \mathrm{N}(\mathfrak{q}_v)^{v(c)} = \prod_{v\nmid\infty} (\#k_v)^{v(c)} = \prod_{v\nmid\infty} c_v^{-1},$$

and therefore

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

We also define

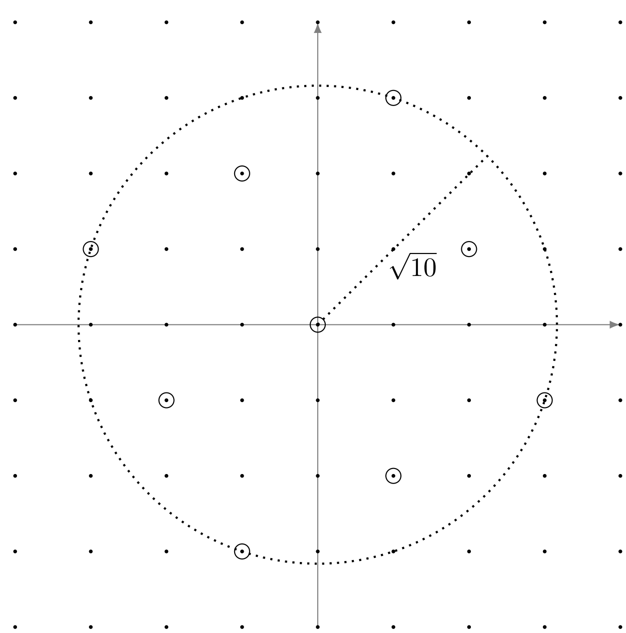
$$R_c := \{x \in K_{\mathbb{R}} : |x|_v \le c_v \text{ for all } v|\infty\},$$

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

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

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

Example 15.5. Let $K = \mathbb{Q}(i)$. The ideal $(2+i)$ lying above 5 is prime and corresponds to a finite place v_1, and there is a unique infinite 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 $v \in M_K$. We then have $I_c = (2+i)$ and the image of $L(c) = \{x \in (2+i) : |x|_\infty \le 10\}$ under the canonical embedding $K \hookrightarrow K_{\mathbb{R}} \simeq \mathbb{C}$ is the set of lattice points in the image of the ideal I_c that lie within a circle of radius $\sqrt{10}$ in the complex plane. Note that $\| \ \|_{v_2} = | \ |_{\mathbb{C}}^2$ 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.

Lemma 15.6. *Let c be an M_K-divisor of a number field K. Then $L(c)$ is a finite set.*

Proof. The fractional ideal I_c is a $\mathbb{Z}$-lattice in the $\mathbb{Q}$-vector space K, thus its image Λ_c under the canonical embedding $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = K_{\mathbb{R}}$ is a lattice in the $\mathbb{R}$-vector space $K_{\mathbb{R}}$. The image of $L(c)$ in $K_{\mathbb{R}}$ is $\Lambda_c \cap R_c$, the intersection of a discrete closed set with a compact set, which is necessarily finite (recall from Remark 14.2 that lattices are closed sets). □

Proposition 15.7. *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 I_c in $K_\mathbb{R}$. We apply Minkowski's lattice point theorem to the convex symmetric set R_c and the lattice Λ_c in $K_\mathbb{R}$. As defined in §14.2, we use the Haar measure μ on the locally compact group $K_\mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$ which is normalized so that $\mu(S) = 2^s \mu_{\mathbb{R}^n}(S)$ for any measurable $S \subseteq K_\mathbb{R}$. For real places $v|\infty$ the constraint $\|x\|_v = |x|_\mathbb{R} \le c_v$ contributes a factor of $2c_v$ to $\mu(R_c)$, and for complex places v the constraint $\|x\|_v = |x|_\mathbb{C}^2 \le c_v$ contributes a factor of πc_v (the area of a circle of radius $\sqrt{c_v}$). Thus

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

where we used Corollary 14.12 and (1) in the second line. Theorem 14.10 implies that R_c contains a nonzero element of Λ_c which must be the image in $K_\mathbb{R}$ of some $x \in L(c) \cap K^\times$. □

Remark 15.8. The bound in Proposition 15.7 can be turned into an asymptotic, that is, for $c \in \operatorname{Div} K$, 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 a multiplicative analog of the Riemann-Roch theorem for function fields, which states that for divisors $D = \sum n_P P$, as $\deg D := \sum n_P \to \infty$ we have

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

The constant g is the *genus*, an important invariant of a function field that 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 all 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 15.6 and Proposition 15.7 to give a proof of the Riemann-Roch theorem for global function fields.

15.2 The unit group of a number field

Let K be a number field with ring of integers $\mathcal{O}_K$. The multiplicative group $\mathcal{O}_K^\times$ consisting of the invertible elements of $\mathcal{O}_K$, is the *unit group* of $\mathcal{O}_K$; it is also often referred to as the unit group of K. Of course the unit group of K is actually $K^\times = K - \{0\}$, but this abuse of language is standard and generally causes no confusion; one usually refers to $K^\times$ as the multiplicative group of K, not its unit group.

As a ring, the finite étale $\mathbb{R}$-algebra $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ also has a unit group, and we have an isomorphism of topological groups[2]

$$K_\mathbb{R}^\times = \prod_{v|\infty} K_v^\times \simeq \prod_{\text{real } v|\infty} \mathbb{R}^\times \prod_{\text{complex } v|\infty} \mathbb{C}^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s.$$

[2]The additive group of $K_\mathbb{R}$ is isomorphic to $\mathbb{R}^n$ as a topological group (and $\mathbb{R}$-vector space), a fact we have used in our study of lattices in $K_\mathbb{R}$. But as topological rings (and $\mathbb{R}$-algebras) $K_\mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s \not\simeq \mathbb{R}^n$.

Writing elements of $K_{\mathbb{R}}^{\times}$ as vectors $x = (x_v)$ indexed by the infinite places v of K, we now define a surjective homomorphism of locally compact groups

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

It is surjective and continuous because each of the maps $x_v \mapsto \log \|x_v\|_v$ is, and it is a group homomorphism because

$$\operatorname{Log}(xy) = (\log \|x_v y_v\|_v) = (\log \|x_v\|_v + \log \|y_v\|_v) = (\log \|x_v\|_v) + (\log \|y_v\|_v = \operatorname{Log} x + \operatorname{Log} y.$$

Here we have used the fact that the normalized absolute value $\|\ \|_v$ is multiplicative.

Recall from Corollary 13.13 that there is a one-to-one correspondence between the infinite places $v \in M_K$ and the $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbits of $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. For each $v|\infty$ let us now pick a representative σ_v of its corresponding $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbit in $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$; for real places v there is a unique choice for σ_v, while for complex places there are two choices, σ_v and its complex conjugate $\bar{\sigma}_v$. Regardless of our choices, we then have

$$\|x\|_v = \begin{cases} |\sigma_v(x)|_{\mathbb{R}} & \text{if } v|\infty \text{ is real} \\ |\sigma_v(x)\bar{\sigma}_v(x)|_{\mathbb{R}} & \text{if } v|\infty \text{ is complex.} \end{cases}$$

The absolute norm $\mathrm{N}\colon K^{\times} \to \mathbb{Q}_{>0}^{\times}$ extends naturally to a continuous homomorphism of locally compact groups

$$\begin{aligned} \mathrm{N}\colon K_{\mathbb{R}}^{\times} &\to \mathbb{R}^{\times} \\ (x_v) &\mapsto \prod_{v|\infty} \|x_v\|_v \end{aligned}$$

which is compatible with the canonical embedding $K^{\times} \hookrightarrow K_{\mathbb{R}}^{\times}$. Indeed, we have

$$\mathrm{N}(x) = \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right| = \left|\prod_{\sigma} \sigma(x)\right|_{\mathbb{R}} = \prod_{v|\infty} \|x\|_v = \mathrm{N}(x)$$

where the $\mathrm{N}(x)$ on the left is the absolute norm on $K^{\times}$ and the the $\mathrm{N}(x)$ on the right is the absolute norm in $K_{\mathbb{R}}^{\times}$. We thus have a commutative diagram of locally compact groups

$$\begin{array}{ccccc} K^{\times} & \hookrightarrow & K_{\mathbb{R}}^{\times} & \xrightarrow{\operatorname{Log}} & \mathbb{R}^{r+s} \\ \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{T}} \\ \mathbb{Q}_{>0}^{\times} & \hookrightarrow & \mathbb{R}_{>0}^{\times} & \xrightarrow{\log} & \mathbb{R}, \end{array}$$

where the trace map $\mathrm{T}\colon \mathbb{R}^{r+s} \to \mathbb{R}$ is defined by $\mathrm{T}(x) = \sum_i x_i$. We may 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 N as a map from $K^{\times}$ to $\mathbb{R}^{\times}$.

We can succinctly summarize the commutativity of the above diagram by the identity

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

which holds for all $x \in K^{\times}$ (and all $x \in K_{\mathbb{R}}^{\times}$). The norm of a unit in $\mathcal{O}_K$ must be a unit in $\mathbb{Z}$, hence have absolute value 1. Thus $\mathcal{O}_K^{\times}$ lies in the kernel of the map $x \mapsto \log \mathrm{N}(x)$

and therefore also in the kernel of the map $x \mapsto \mathrm{T}(\operatorname{Log} x)$. It follows that $\operatorname{Log}(\mathcal{O}_K^\times)$ 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 $r+s-1$. The proof of Dirichlet's unit theorem amounts to showing that $\operatorname{Log}(\mathcal{O}_K^\times)$ is a lattice in $\mathbb{R}_0^{r+s}$.

Proposition 15.9. *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) *The torsion subgroup $(\mathcal{O}_K^\times)_{\mathrm{tors}}$ of the unit group is finite;*

(2) *We have a split exact sequence of abelian groups*

$$1 \to (\mathcal{O}_K^\times)_{\mathrm{tors}} \to \mathcal{O}_K^\times \xrightarrow{\operatorname{Log}} \Lambda_K \to 0; v$$

(3) *Λ_K is a lattice in the trace zero hyperplane $\mathbb{R}_0^{r+s}$.*

Proof. Let Z be the kernel of $\mathcal{O}_K^\times \xrightarrow{\operatorname{Log}} \Lambda_K$. We must have $(\mathcal{O}^\times)_{\mathrm{tors}} \subseteq Z$, since $\Lambda_K \subseteq \mathbb{R}^{r+s}$ is torsion free. We now show $Z \subseteq (\mathcal{O}^\times)_{\mathrm{tors}}$. 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

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

The set on the RHS includes the zero vector, thus $Z \subseteq L(c)$, which by Lemma 15.6 is a finite set. As a finite subgroup of $\mathcal{O}_K^\times$, we must have $Z \subseteq (\mathcal{O}_K^\times)_{\mathrm{tors}}$. as claimed. This proves (1) and that the sequence in (2) is exact. We now note that $\Lambda_K \cap \operatorname{Log}(R_c) = \operatorname{Log}\left(\mathcal{O}_K^\times \cap L(c)\right)$ is a finite, since $L(c)$ is finite. It follows that 0 is an isolated point of Λ_K in $\mathbb{R}^{r+s}$, and in $\mathbb{R}_0^{r+s}$, thus Λ_K is a discrete subgroup of the $\mathbb{R}$-vector space $\mathbb{R}_0^{r+s}$. It is therefore a free $\mathbb{Z}$-module of finite rank at most $r+s-1$, since it spans some subspace of $\mathbb{R}_0^{r+s}$ in which it is both discrete and cocompact, hence a lattice. It follows that $\mathcal{O}_K^\times$ is finitely generated, since it lies in a short exact sequence whose left and right terms are finitely generated, and by the structure theorem for finitely generated abelian groups, this exact sequence splits, since $(\mathcal{O}_K^\times)_{\mathrm{tors}}$ is the torsion subgroup of $\mathcal{O}_K^\times$.

To prove (3) it remains only to show that Λ_K spans $\mathbb{R}_0^{r+s}$. Let V be the subspace of $\mathbb{R}_0^{r+s}$ spanned by Λ_K and suppose for the sake of contradiction that $\dim V < \dim \mathbb{R}_0^{r+s}$. The orthogonal subspace $V^\perp$ then contains a unit vector u, and for every $\lambda \in \mathbb{R}_{>0}$ the open ball $B_{<\lambda}(\lambda u)$ does not intersect Λ_K. Thus $\mathbb{R}_0^{r+s}$ contains points arbitrarily far away from every point in Λ_K (with respect to any norm on $\mathbb{R}_0^{r+s} \subseteq \mathbb{R}^{r+s}$). To obtain a contradiction it is enough to show that every $h \in \mathbb{R}_0^{r+s}$ there is an $\ell \in \Lambda_K$ for which the sup-norm $\|h - \ell\| := \max_i |h_i - \ell_i|$ is bounded by some M that does not depend of h.

Let us fix a real number $B > B_K$, where B_K is as in Proposition 15.7, so that for every $c \in \operatorname{Div} K$ with $\|c\| \ge B$ the set $L(c)$ contains a nonzero element, and fix a vector $b \in \mathbb{R}^{r+s}$ with nonnegative components b_i such that $\mathrm{T}(b) = \sum_i b_i = \log B$. Let $(\alpha_1), \ldots, (\alpha_m)$ be the list of all nonzero principal ideals with $\mathrm{N}(\alpha_j) \le B$ (by Lemma 14.16 this is a finite list). Let M be twice the maximum of $(r+s)B$ and $\max_j \|\operatorname{Log}(\alpha_j)\|$.

Now let $h \in \mathbb{R}_0^{r+s}$, and define $c = c(h) \in \operatorname{Div} K$ by $I_c := \mathcal{O}_K$ and $c_v := \exp(h_i + b_i)$ for $v|\infty$, where i is the coordinate in $\mathbb{R}^{r+s}$ corresponding to v under the Log map. We have

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

thus $L(c)$ contains a nonzero $\gamma \in I_c \cap K = \mathcal{O}_K$ and $g = \operatorname{Log}(\gamma)$ satisfies $g_i \le \log c_v = h_i + b_i$. We also have $\mathrm{T}(g) = \mathrm{T}(\operatorname{Log}\gamma) = \log \mathrm{N}(\gamma) \ge 0$, since $\mathrm{N}(\gamma) \ge 1$ for all $\gamma \in \mathcal{O}_K$. The vector $v := g - h \in \mathbb{R}^{r+s}$ satisfies $\sum_i v_i = \mathrm{T}(v) = \mathrm{T}(g) - \mathrm{T}(h) = T(g) \ge 0$ and $v_i \le b_i \le B$ which together imply $|v_i| \le (r+s)B$, so $\|g - h\| = \|v\| \le M/2$. We also have

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

so $\mathrm{N}(\gamma) \le B$ and $(\gamma) = (\alpha_j)$ for one of the α_j fixed above. Thus $\gamma/\alpha_j \in \mathcal{O}_K^\times$ is a unit, and

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

satisfies $\|g - \ell\| = \|\operatorname{Log}(\alpha_j)\| \le M/2$. We then have

$$\|h - \ell\| \le \|h - g\| + \|g - \ell\| \le M$$

as desired (by the triangle inequality for the sup-norm). □

Dirichlet's unit theorem follows immediately from Proposition 15.9.

Theorem 15.10 (Dirichlet's 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 lattice Λ_K in the trace-zero hyperplane $\mathbb{R}_0^{r+s}$, which has dimension $r + s - 1$. □

Example 15.11. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \ne 1$ squarefree. If $d < 0$ then $r = 0$ and $s = 1$, in which case the unit group $\mathcal{O}_K^\times$ has rank 0 and $\mathcal{O}_K^\times = (\mathcal{O}_K^\times)_{\mathrm{tors}}$ is finite.

If $d > 0$ then $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$ is a real quadratic field with $r = 2$ and $s = 0$, and the unit group $\mathcal{O}_K^\times$ has rank 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 the *fundamental unit* of $\mathcal{O}_K$ (and of K). To explicitly determine ϵ, let $D = \operatorname{disc} \mathcal{O}_K$ (so $D = d$ if $d \equiv 1 \bmod 4$ 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 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

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

15.3 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 15.9, 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 15.12. 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 value of R_K does not depend on the choice of π, we use the projection to normalize the Haar measure on $\mathbb{R}_0^{r+s}\simeq\mathbb{R}^{r+s-1}$. 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 15.13. 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

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

The 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 is the same in both cases, and since we have require the fundamental unit to satisfy $\epsilon>1$ (which forces a choice of embedding), the regulator of K is simply $R_K=\log\epsilon$.

References

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

18.785 Number Theory I
Fall 2016