Algebraic Number Theory, Math 421
Instructor: Sreekar M. Shastry
Notes on the ideal class group and the unit group

1. Finiteness of the Class Group

We use the usual notation, $K, L/K, G, \mathscr{O}_K, \mathscr{O}_L, P, Q, \ldots$

Theorem 1. *Given K, there is a positive real number λ, depending only on K such that every nonzero ideal $I \subset \mathscr{O}_K$ contains a nonzero element α with*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \lambda \|I\|.$$

Proof. Let $\{\alpha_i\}_{i=1}^n$ be an integral basis for $\mathscr{O}_K$ and $\{\sigma_j\}_{j=1}^n$ be the set of embeddings $K \hookrightarrow \mathbb{C}$. We will show that

$$\lambda := \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

will do the job.

For an ideal I, let m be the unique positive integer such that

$$m^n \leq \|I\| < (m+1)^n$$

and consider the $(m+1)^n$ elements of $\mathscr{O}_K$:

$$\left\{ \sum_{j=1}^{n} m_j \alpha_j : m_j \in \mathbb{Z}, 0 \leq m_j \leq m \right\}$$

(we are secretly using the fact that $\mathrm{char}(K) = 0$). Two elements of this set must be congruent mod I since the set has cardinality greater than $\|I\|$; we take their difference and obtain a nonzero element of I of the form

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j \text{ s.t. } m_j \in \mathbb{Z}, |m_j| \leq m.$$

The following chain of inequalities completes the proof:

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j |\sigma_i(\alpha_j)| \leq m^n \lambda \leq \|I\| \lambda.$$

■

Corollary 2. *Every ideal class of $\mathscr{O}_K$ contains an ideal J with $\|J\| \leq \lambda$ (the same λ as above).*

Proof. Given an ideal class C, fix a representative I of C^{-1} and choose $\alpha \in I$ as in the theorem. We have $I \supset (\alpha)$ so that $(\alpha) = IJ$ for some J (by [Mar77, Theorem 15,p.57] and its proof). Then J is in the class of C. Now we use the theorem to the effect that

$$\|(\alpha)\| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$$

to see that

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \|(\alpha)\| = \|I\|\|J\| \leq \lambda \|I\|.$$

■

Corollary 3. *The class group, $\mathrm{Cl}(\mathscr{O}_K)$, is finite.*

Proof. If $J = \prod P_i^{n_i}$ then $\|J\| = \prod \|P_i\|^{n_i}$. Thus only finitely many *ideals* can satisfy $\|J\| \leq \lambda$ since this inequality implies the same inequality for every $P|J$ and thus places bounds on the powers to which they can occur. ■

Example 4. Let us use the above to show that $\mathbb{Z}[\sqrt{2}]$ is a PID or in other words that $\mathrm{Cl}(\mathbb{Z}[\sqrt{2}]) = \{1\}$.

The integral basis is $\{1, \sqrt{2}\}$ (since $2 \equiv 2 \pmod 4$!) and the above proof produces $\lambda = (1+\sqrt{2})^2 = 1 + 2\sqrt{2} + 2$. This number is between 5 and 6 and therefore every ideal class contains an ideal J with $\|J\| \leq 6$. Thus the support of J must be contained in the set of primes lying over $2, 3, 5$. We factor each of $2.\mathscr{O}_K, 3.\mathscr{O}_K, 5.\mathscr{O}_K$: $2.\mathscr{O}_K = \left(\sqrt{2}\right)^2$ while $3.\mathscr{O}_K$ and $5.\mathscr{O}_K$ are inert because 2 is a quadratic nonresidue mod 3 and 5 (see [Mar77, Theorem 25,p.74]). Therefore the only ideals J with $\|J\| \leq 5$ are $\mathscr{O}_K$, $\left(\sqrt{2}\right)$, and $2.\mathscr{O}_K$. It follows that every ideal in $\mathscr{O}_K$ is principle.

2. Minkowski's Theorem

5. We now seek to improve the constant λ. We will accomplish this by embedding $\mathscr{O}_K$ into $\mathbb{R}^n$ and applying general geometric results.

Let $\{\sigma_1, \ldots, \sigma_r\}$ be the embeddings $K \hookrightarrow \mathbb{R}$ and $\{\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s\}$ be the embeddings $K \hookrightarrow \mathbb{C}$ which do not factor through $\mathbb{R} \subset \mathbb{C}$. Thus $r + 2s = n = [L : K]$. We obtain a map $\iota : K \to \mathbb{R}^n$ by

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1, (\alpha)) \ldots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha))).$$

Observe that it is a homomorphism of abelian groups with trivial kernel.

Theorem 6. *The mapping $\iota : K \to \mathbb{R}^n$ sends $\mathscr{O}_K$ isomorphically (as abelian groups) onto a lattice in $\mathbb{R}^n$. A fundamental domain for this lattice has volume*

$$\frac{1}{2^s}\sqrt{|\mathrm{disc}(\mathscr{O}_K)|}.$$

Proof. Let us see that $\iota(\mathscr{O}_K)$ is a lattice Λ in $\mathbb{R}^n$ (a lattice is by definition the $\mathbb{Z}$-span of an $\mathbb{R}$-basis for $\mathbb{R}^n$). To see this let $\{\alpha_i\}_{i=1}^n$ be an integral basis for $\mathscr{O}_K$. These generate $\mathscr{O}_K$ over $\mathbb{Z}$ and therefore their images in $\mathbb{R}^n$ generate Λ over $\mathbb{Z}$. We must show that this generating set is linearly independent over $\mathbb{R}$. Consider the $n \times n$ matrix the ith row of which is $\iota(\alpha_i)$ (recall that $n = r + 2s$):

$$A := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \mathrm{Re}(\tau_1(\alpha_1)) & \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Re}(\tau_s(\alpha_1)) & \mathrm{Im}(\tau_s(\alpha_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \mathrm{Re}(\tau_1(\alpha_n)) & \mathrm{Im}(\tau_1(\alpha_n)) & \cdots & \mathrm{Re}(\tau_s(\alpha_n)) & \mathrm{Im}(\tau_s(\alpha_n)) \end{pmatrix}.$$

Elementary column operations transform this matrix into

$$B := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \overline{\tau}_1(\alpha_1) & \tau_1(\alpha_1) & \cdots & \overline{\tau}_s(\alpha_1) & \tau_s(\alpha_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \overline{\tau}_1(\alpha_n) & \tau_1(\alpha_n) & \cdots & \overline{\tau}_s(\alpha_n) & \tau_s(\alpha_n) \end{pmatrix}$$

so that we have

$$\det(A) = \frac{1}{(2i)^s}\det(B).$$

Now, $\det(B)$ is the discriminant of the number field K (in particular it is nonzero by [Mar77, Theorem 7,p.25]). On the other hand, the volume of the fundamental domain in question is $|\det(A)|$. ∎

7. Let us define a fundamental domain for a lattice in Euclidean space with $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$ to be

$$\left\{\sum_{i=1}^n a_i v_i : a_i \in [0, 1) \subset \mathbb{R}\right\}.$$

From linear algebra, we know that the volume of the fundamental domain is the determinant of the matrix with rows $\{v_i\}$. This volume is moreover the volume (with respect to the Riemannian metric induced by pushforward from $\mathbb{R}^n$) of the compact torus $\mathbb{R}^n/\Lambda$.

For a sublattice $\Lambda' \subset \Lambda$, the group Λ/Λ' is finite and we have

$$\mathrm{vol}(\mathbb{R}^n/\Lambda') = \mathrm{vol}(\mathbb{R}^n/\Lambda)|\Lambda/\Lambda'|.$$

We apply this to an ideal $I \subset \mathscr{O}_K$ to obtain

$$\mathrm{vol}(\mathbb{R}^n/\Lambda_I) = \mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})|\Lambda_{\mathscr{O}_K}/\Lambda_I| = \frac{1}{2^s}(|\mathrm{disc}(\mathscr{O}_K)|)^{1/2}\|I\|.$$

We now define a "norm" on $\mathbb{R}^n$ for $x = (x_1, \ldots, x_n)$ by

$$\mathrm{N}(x) := x_1 \cdots x_r \underbrace{(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)}_{s \text{ factors}}$$

where $n = r + 2s$. Thus we have

$$\mathrm{N}(\iota(x)) = \mathrm{N}_{K/\mathbb{Q}}(x)$$

Theorem 8. *Every lattice $\Lambda \subset \mathbb{R}^n$ contains a nonzero point x such that*

$$|\mathrm{N}(x)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Corollary 9. *A nonzero ideal $I \subset \mathscr{O}_K$ contains a nonzero element α such that*

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \|I\|\sqrt{|\mathrm{disc}(\mathscr{O}_K)|}.$$

Proof. Apply the above theorem with $\Lambda = \Lambda_I$, use the earlier result that

$$\mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K}) = 2^{-s}|\mathrm{disc}(\mathscr{O}_K)|^{1/2},$$

and the fact that $\mathrm{vol}(\mathbb{R}^n/\Lambda_I) = \|I\|\mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})$. ■

Corollary 10. *Each ideal class of $\mathscr{O}_K$ has a representative J with*

$$\|J\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathscr{O}_K)|}.$$

Proof. Given an ideal class C choose an ideal $I \in C^{-1}$ and find an α as in the previous corollary. Now, there is a J in C such that $(\alpha) = IJ$ so that the previous corollary gives

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| = \|I\|\|J\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \|I\|\sqrt{|\mathrm{disc}(\mathscr{O}_K)|},$$

as required. ■

11. The factor $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$ is called Minkowski's constant and it decays quickly with respect to n. As an example of its use, let us show that $\mathbb{Q}[e^{2\pi i/5}]$ is has trivial class group. Every ideal class contains a J with $\|J\| \leq \frac{15\sqrt{5}}{2\pi^2} < 2$. Thus every ideal class contains $\mathscr{O}_K$ itself, or in other words, every ideal class divides the trivial ideal class.

We now begin the the proof of the theorem.

Lemma 12 (Blichtfeldt's Lemma)**.** *Let Λ be an n-dimensional lattice in $\mathbb{R}^n$ and let E be a convex, measurable, centrally symmetric subset of $\mathbb{R}^n$ such that*

$$\mathrm{vol}(E) > 2^n\mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Then E contains a nonzero point of Λ. If E is also compact, then the strict inequality can be weakened to $\geq$.

(Recall that a subset of $\mathbb{R}^n$ is convex if for any x, y in it and $\alpha \in [0,1]$, $\alpha x + (1-\alpha)y$ is also in it. Centrally symmetric means $-E = E$.)

Proof. Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is the disjoint union of the translates $x+F, x \in \Lambda$. Thus we have

$$\tfrac{1}{2}E = \coprod_{x\in\Lambda} \tfrac{1}{2}E \cap (x+F).$$

Under the hypothesis of strict inequality, we have

$$\begin{aligned}\mathrm{vol}(F) &< 2^{-n}\mathrm{vol}(E)\\ &= \mathrm{vol}\left(\tfrac{1}{2}E\right)\\ &= \sum_{x\in\Lambda} \mathrm{vol}\left(\tfrac{1}{2}E \cap (x+F)\right)\\ &= \sum_{x\in\Lambda} \mathrm{vol}\left(\left(\tfrac{1}{2}E - x\right) \cap F\right).\end{aligned}$$

On the other hand, if the sets $(\frac{1}{2}E - x) \cap F$ were all pairwise disjoint then the last equation sum would be at most $\mathrm{vol}(F)$. Thus there exist $x, y \in \Lambda$ such that $\frac{1}{2}E - x$ and $\frac{1}{2}E - y$ intersect. Then $x - y \in \Lambda \smallsetminus \{0\}$.

Now, convexity and central symmetry imply that $0 \in E$, $\frac{1}{2}E \subset E$, and $E = \frac{1}{2}E + \frac{1}{2}E$ (the set of all possible sums). Let $z = e' - x = e'' - y$ where $e', e'' \in \frac{1}{2}E$. Then $x - y = -z + e' - (-z + e'') = e' + e'' \in E$. This completes the proof under the strict inequality hypothesis.

Next, suppose that E is compact hence closed and bounded and now weaken the hypothesis to $\mathrm{vol}(E) \geq 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$. For each $m = 1, 2, \ldots$ the first part of the theorem ensures that $(1+1/m)E$ contains some nonzero point $x_m \in \Lambda$. The x_m are all in $2E$ and since the sequence $\{x_m\}$ is discrete, it consists of only finitely many distinct points. Thus one of them, say x_{m_0}, is in infinitely many of the $(1+1/m)E$ and thus is in $\overline{E} = E$. ∎

Corollary 13 (of the lemma)**.** *Suppose there is a compact, convex, centrally symmetric set A of positive volume with the property*

$$a \in A \Rightarrow |\mathrm{N}(a)| \leq 1.$$

Then every n-dimensional lattice Λ contains a nonzero point x with

$$|\mathrm{N}(x)| \leq \frac{2^n}{\mathrm{vol}(A)}\mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Proof. Apply the lemma with $E = tA$ where

$$t^n = \frac{2^n}{\mathrm{vol}(A)}\mathrm{vol}(\mathbb{R}^n/\Lambda).$$

∎

Proof of Theorem 8. Let us get warmed up by proving a weaker result. Let A be the set defined by the inequalities

$$|x_1| \leq 1, \ldots, |x_r| \leq 1, \underbrace{x_{r+1}^2 + x_{r+2}^2 \leq 1, \ldots, x_{n-1}^2 + x_n^2 \leq 1.}_{s \text{ inequalities}}$$

Then $\mathrm{vol}(A) = 2^r\pi^s$ and we deduce from the previous corollary that every Λ contains a nonzero x with

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^s \mathrm{vol}(\mathbb{R}^n/\Lambda).$$

Let us now proceed with the proof of the theorem as stated. Define A by

$$|x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n.$$

We show that this set is convex. Quite generally, let $f(x_1, \ldots, x_n)$ be a continuous and nonnegative function $\mathbb{R}^n \to \mathbb{R}_{\geq 0}$ and consider a set $E := \{x : f(x) \leq \alpha\} = f^{-1}([0, \alpha])$. If the condition

$$x, y \in E \Rightarrow (x + y)/2 \in E \qquad (*)$$

holds, then E is convex. This follows from the continuity of f and the density in $\mathbb{R}$ of the dyadic rationals (verify this). Thus, to show that A is convex, it suffices to show that $(*)$ holds for A. This in turn follows from a combination of the triangle inequalities for $\mathbb{R}$ and $\mathbb{R}^2$:

$$|r + s| \leq |r| + |s|$$
$$\sqrt{(a+b)^2 + (c+d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}.$$

(The last equality is just $\|x + y\| \leq \|x\| + \|y\|$ if $x = (a, b), y = (c, d), \|(a, b)\| = \sqrt{a^2 + b^2}$.)

Recall the AM-GM ineqality for a finite sequence of nonnegative real numbers:

$$(a_1 a_2 \cdots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Now, the condition $a \in A \Rightarrow |\mathrm{N}(a)| \leq 1$ follows from applying AM-GM to the set of nonnegative real numbers

$$\left\{|x_1|, \cdots, |x_r|, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \cdots \sqrt{x_{n-1}^2 + x_n^2}, \sqrt{x_{n-1}^2 + x_n^2}\right\}$$

(note well the repetition). Namely, the GM is $|N(a)|^{1/n}$ and the AM is at most 1.

Let us now show that

$$\mathrm{vol}(A) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s.$$

Combining the above with the previous lemma and its corollary will complete the proof of the theorem. First note that the case $s = 0, r = n$ of the computation of $\mathrm{vol}(A)$ is direct[1] and therefore we assume $s > 0$ henceforth.

In general, let $V_{r,s}(t)$ be the volume of the subset of $\mathbb{R}^{r+2s}$ defined by

$$|x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq t$$

so that

$$V_{r,s}(t) = t^{r+2s} V_{r,s}(1).$$

We claim that

$$V_{r,s}(1) = \frac{1}{(r+2s)!} 2^r \left(\frac{\pi}{2}\right)^s.$$

For $r > 0$ we have:

$$\begin{aligned} V_{r,s}(1) &= 2\int_0^1 V_{r-1,s}(1-x)dx \\ &= 2V_{r-1,s}(1)\int_0^1 (1-x)^{r-1+2s} dx \\ &= \frac{2}{r+2s} V_{r-1,s}(1). \end{aligned}$$

[1] In greater detail, one starts with the n-dimensional cube defined by $\{x : \max |x_i| \leq n\}$ which clearly has volume $2^n n^n$. Now, $n!$ is the number of permutations σ of $\{1, \ldots, n\}$. We cover the set A with the $n!$ disjoint (up to sets of measure zero) and isometric sets

$$A_\sigma := \{|x_{\sigma(1)}| \leq \cdots \leq |x_{\sigma(n)}|\};$$

the permutation corresponding to $x \in A$ is obtained by simply ordering the coordinates of x which shows that the A_σ cover A.

Repeated application gives

$$V_{r,s}(1) = \frac{2^r}{(r+2s)(r+2s-1)\cdots(2s+1)} V_{0,s}(1).$$

Now $s > 0$, and we define[2] $V_{0,1}(1) := \pi/4$. We have

$$V_{0,s}(1) = \int_{\{x^2+y^2 \leq 1/4\}} V_{0,s-1}\left(1 - 2\sqrt{x^2+y^2}\right) dxdy.$$

Changing to polar coordinates we compute[3]

$$\begin{aligned} V_{0,s}(1) &= \int_0^{2\pi} \int_0^{1/2} V_{0,s-1}(1-2\rho)\rho d\rho d\theta \\ &= 2\pi \int_0^{1/2} (1-2\rho)^{2(s-1)} \rho V_{0,s-1}(1) d\rho \end{aligned}$$

where we have used $V_{r,s}(t) = t^{r+2s} V_{r,s}(1)$. Thus,

$$\begin{aligned} V_{0,s}(1)/V_{0,s-1}(1) &= \frac{\pi}{2} \int_0^1 u^{2(s-1)}(1-u) du \\ &= \frac{\pi}{2} \left(\frac{1}{2s-1} - \frac{1}{2s} \right) \\ &= \frac{\pi}{2} \frac{1}{2s(2s-1)} \end{aligned}$$

and we obtain

$$V_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{1}{(2s)!}.$$

The demonstrates our claim on the value of $\mathrm{vol}(A)$ and completes the proof of the theorem. ∎

3. Dirichlet's Unit Theorem

Theorem 14. *Write $U := \mathscr{O}_K^\times$ and $r, 2s$ for the number of real, resp. complex embeddings of K. Then U_K is a finitely generated abelian group and we have a direct product decomposition*

$$U = U_{\mathrm{tors}} U_{\mathrm{free}}.$$

Here U_{tors} coincides with the finite group of roots of unity of K and U_{free} is a free abelian group of rank $r+s-1$ with $\mathbb{Z}$-basis $\{u_i\}$ also known as a fundamental system of units.

Proof. We have a sequence

$$U \subset \mathscr{O}_K - \{0\} \to \Lambda_{\mathscr{O}_K} - \{0\} \xrightarrow{\log} \mathbb{R}^{r+s}$$

where log is defined in this context as follows. For $(x_1, \ldots, x_n) \in \Lambda_{\mathscr{O}_K} - \{0\}$

$$\log(x_1, \ldots, x_n) := (\log|x_1|, \ldots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \ldots, \log(x_{n-1}^2 + x_n^2)).$$

This is well defined since all of the arguments to the classical logs are positive real numbers. We will also write log for the composites $U \to \mathbb{R}^{r+s}$ and $\mathscr{O}_K - \{0\} \to \mathbb{R}^{r+s}$. The target, $\mathbb{R}^{r+s}$ shall be called the logarithmic space.

The following properties are immediate:

(1) $\log(\alpha\beta) = \log\alpha + \log\beta$ for $\alpha, \beta \in \mathbb{R} - \{0\}$,

(2) $\log U \subset H$ where $H \subset \mathbb{R}^{r+s}$ is the hyperplane defined by $y_1 + \cdots + y_{r+s} = 0$ — this is because the norm of a unit is ± 1. The hyperplane H is also called the "trace zero hyperplane,"

[2] Of course, one should check that this is compatible with the earlier computation...

[3] There is a serious typo at this point in [Mar77].

(3) any bounded set in the logarithmic space has a finite preimage in U — this is because preimage under log of a bounded set is still a bounded set and $\Lambda_{\mathscr{O}_K}$ is a lattice in the Euclidean space in question.

The first two properties show that $\log : U \to H$ is a group homomorphism where U is written multiplicatively and H is written additively being a real vector space. The third property shows that the kernel in U is equal to the set of roots of unity of K; namely, an element of the kernel has finite order and is thus a root of unity and a root of unity lies on the unit circle and is sent to zero by log. Moreover, we use the fact that every finite subgroup of the circle is cyclic[4] to deduce that the kernel is a cyclic group.

The third property also implies that the image $\log(U)$ is a discrete subgroup of the logarithmic space. This is a general fact valid for subgroups of a real vector space such that every bounded subset is finite[5].

The discrete subgroup $\Lambda_U := \log(U)$ is contained in H and thus is a free abelian group of rank $d \leq r + s - 1$.

To see that U is a direct product $U_{\text{tors}} \cdot U_{\text{free}}$, we note that we have already seen that U is generated by U_{tors} and representatives of the d basis elements of Λ_U. Thus U is a finitely generated abelian group which therefore splits into the direct sum of its torsion subgroup and a free part. Moreover, that free part is generated by a splitting of the exact sequence

$$0 \to U_{\text{tors}} \to U \to \Lambda_U \to 0.$$

Thus $U_{\text{free}} :=$ the image of Λ_U under the splitting.

It remains to show that $d = r + s - 1$. We will do this by producing $r + s - 1$ units whose log vectors are $\mathbb{R}$-linearly independent. We need a lemma first.

Lemma A. Fix k with $1 \leq k \leq r + s$. For each nonzero $\alpha \in \mathscr{O}_K$ there exists a nonzero $\beta \in \mathscr{O}_K$ with

$$|\mathrm{N}_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathscr{O}_K)|}$$

such that if

$$\log(\alpha) = (a_1, \cdots, a_{r+s})$$
$$\log(\beta) = (b_1, \cdots, b_{r+s})$$

then $b_i < a_i$ for all $i \neq k$.

To see this, we use Blichtfeldt's Lemma (also called Minkowski's Lemma). Let E be the subset of $\mathbb{R}^n$ defined by the inequalities

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r$$
$$x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \ldots, x_{n-1}^2 + x_n^2 \leq c_{r+s}$$

---

[4]Proof: if $x, y \in S^1$ are of finite order, then $x' = 2\pi/a, y' = 2\pi/b$ are lifts of x, y in $\mathbb{R}$, for some $a, b \in \mathbb{Z}_{>0}$. Then the group generated by x and y is the cyclic group on a generator whose lift is $2\pi/\mathrm{lcm}(a, b)$. This is because we may obtain any common multiple of a and b in the denominator by adding suitable multiples of x' and y'.

Thus the set of roots of unity in a number field is a finite cyclic group.

[5]Proof: Choose a bounded neighborhood of zero in the subgroup in question. It is finite hence the topology on it induced from the ambient Euclidean space is discrete. Hence 0 is both open and closed in this subgroup and thus it is discrete.

Warning: what is called a "lattice" on [Mar77, p.143] is not the current terminology. Lattice means discrete and cocompact subgroup, and what Marcus calls "lattice" simply means discrete subgroup. Compare with the terminology in [Mil09].

The discussion on [Mar77, p.143] says, in modern terminology, that an $\mathbb{R}$-independent set in a Euclidean space gives rise, by taking integer linear combinations, to a discrete subgroup, but on the other hand, a $\mathbb{Z}$-independent set need not generate a discrete subgroup.

where the c_i are chosen to satisfy $0 < c_i < e^{a_i}$ for all $i \neq k$ and

$$c_1 c_2 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathscr{O}_K)|}.$$

Then $\mathrm{vol}(E) = 2^r \pi^s c_1 \cdots c_{r+s} = 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda_{\mathscr{O}_K})$. Blichtfeldt then tells us that E contains a nonzero point of $\Lambda_{\mathscr{O}_K}$ and one verifies that β can be taken to be the corresponding element of $\mathscr{O}_K$. ///

Using Lemma A we can show that distinguished units exist.

Lemma B. Fix k with $1 \leq k \leq r+s$. Then there exists $u \in U$ such that if

$$\log(u) = (y_1, \ldots, y_{r+s})$$

then $y_i < 0$ for all $i \neq k$.

Starting with a nonzero $\alpha_1 \in \mathscr{O}_K$ we apply Lemma A repeatedly to get a sequence $\alpha_1, \alpha_2, \ldots$ of nonzero elements of $\mathscr{O}_K$ with the property that for each $i \neq k$ and for each $j \geq 1$ the ith coordinate of $\log(\alpha_{j+1})$ is strictly less than that of $\log(\alpha_j)$ and moreover that the numbers $|\mathrm{N}_{K/\mathbb{Q}}(\alpha_j)|$ are bounded. Then the $\|(\alpha_j)\|$ are bounded. This implies (as in the proof of the finiteness of class groups) that there are only finitely many distinct ideals (α_j). Fixing any $j < h$ such that $(\alpha_j) = (\alpha_h)$, we have $\alpha_h = \alpha_j u$ for some $u \in U$. This is the sought element. ///

Lemma B shows that there are units $u_1, \ldots, u_{r+s}$ such that all coordinates of $\log(u_i)$ are negative except the kth. Since $\log(u_i) \in H$ it follows that the kth coordinate is positive. We form the $(r+s) \times (r+s)$ matrix having $\log(u_i)$ as its ith row. We claim that this matrix has rank $r+s-1$ and hence that there are $r+s-1$ $\mathbb{R}$-linearly independent rows. This will complete the proof of the unit theorem.

Lemma C. Let $A = (a_{ij})$ be an $m \times m$ real matrix such that $a_{ii} > 0$ for all i and $a_{ij} < 0$ for all $i \neq j$ and such that, moreover, each row-sum is 0

$$\sum_{j=1}^{m} a_{ij} = 0.$$

Then A has rank $m-1$.

Let us see that the first $m-1$ columns are linearly independent. Suppose not so that $t_1 v_1 + \cdots + t_{m-1} v_{m-1} = 0$ where the v_j are the column vectors and the t_j are real numbers, not all 0. Without loss we may assume that some $t_k = 1$ and that all other $t_j \leq 1$ (divide by the coefficient with maximum absolute value). Consider the kth row:

$$0 = \sum_{j=1}^{m-1} t_j a_{kj} \geq \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^{m} a_{kj} = 0,$$

a contradiction. ///

This completes the proof of Dirichlet's unit theorem. ■

Examples 15. (a) Let K be imaginary quadratic. Then $r + s - 1 = 0$ and $U = K^\times_{\mathrm{tors}}$ = the finite group of roots of 1 in K.

(b) Let K be real quadratic. Then $U = \{\pm u^k\}_{k \in \mathbb{Z}}$ is isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}$. In this case, u is called a fundamental unit in $\mathscr{O}_K$.

References

[Mar77] Daniel A. Marcus. *Number Fields.* Springer-Verlag, 1977. Universitext.

[Mil09] James S. Milne. Algebraic number theory (v3.02), 2009. Available at `www.jmilne.org/math/`.