9. Dirichlet's Theorem.

The main result of this section is the Dirichlet Unit theorem (P. Lejeune Dirichlet, German mathematician 1805–1859). We give a proof by means of Minkowski's convex body theorem.

Proposition 9.1. *Let F be a number field of degree n. Let ε be in the unit group O_F^* of the ring of integers of F. Then the following are equivalent*
(a) ε has finite order in O_F^*. In other words, it is a root of unity.
(b) For $i = 1, \ldots, n$ we have $|\phi_i(\varepsilon)| = 1$.

Proof. Suppose that ε is a root of unity. Then we have $\varepsilon^m = 1$ for some $m > 0$. It follows that for each $i = 1, \ldots, n$ we have $\phi_i(\varepsilon)^m = 1$ so that $|\phi_i(\varepsilon)|^m = 1$ and hence $|\phi_i(\varepsilon)| = 1$. Conversely, if for $i = 1, \ldots, n$ we have $|\phi_i(\varepsilon)| = 1$, then for each $k \in \mathbf{Z}$ the unit ε^k is in the lattice $O_F \subset F_{\mathbf{R}}$ as well as in the bounded set $B = \{(z_i) \in F_{\mathbf{R}} : |z_i| \leq 1 \text{ for } i = 1, \ldots, n\}$. Since the intersection $O_F \cap B$ is finite, so is $\{\varepsilon^k : k \in \mathbf{Z}\}$. This shows that ε has finite order in O_F^*

Corollary 9.2. *Let F be a number field. Then the group μ_F of roots of unity in F is a finite cyclic group.*

Proof. Roots of unity are algebraic integers. Therefore we have $\mu_F \subset O_F^*$. In the notation of the proof of part (b) of Proposition 9.1 the group μ_F is contained in the finite set $O_F \cap B$. Therefore μ_F is a finite group. Since O_F is a domain, the group μ_F is cyclic. This proves the corollary.

Let

$$\mathrm{Log} : F_{\mathbf{C}}^* \longrightarrow F_{\mathbf{C}}$$

be the homomorphism defined by

$$\mathrm{Log}(z_1, \ldots, z_n) = (\log|z_1|, \ldots, \log|z_n|)| \in F_{\mathbf{C}} = \prod_{i=1}^{n} \mathbf{C}.$$

The image of the Log-map is contained in the subalgebra $\prod_{i=1}^n \mathbf{R}$. The image of $F_{\mathbf{R}}^*$ is the subalgebra $F_{\mathbf{R}}^0$ of elements of $\prod_{i=1}^n \mathbf{R}$ for which any two coordinates corresponding to a complex embedding and its complex conjugate, are equal. It has real dimension $r_2 + r_2$. The image of the subgroup of elements of $F_{\mathbf{R}}^*$ whose norms are ± 1 is the subspace of elements of $F_{\mathbf{R}}^0$ of trace zero. Equivalently, it is the orthogonal complement of the element 1. It is denoted by $F_{\mathbf{R}}^{\perp}$. The dimension of $F_{\mathbf{R}}^{\perp}$ is $r = r_1 + r_2 - 1$. Since units have norm ± 1, the group $\mathrm{Log}|O_F^*|$ is contained in $F_{\mathbf{R}}^{\perp}$.

Lemma 9.3. *The kernel of the homomorphism* $\mathrm{Log} : O_F^* \longrightarrow F_{\mathbf{R}}^{\perp}$ *is the subgroup μ_F of roots of unity. Its image is a discrete subgroup of $F_{\mathbf{R}}^{\perp}$.*

Proof. The kernel consists of units ε for which $|\phi_i(\varepsilon)| = 1$ for $i = 1, \ldots, n$. By Prop. 9.1 this means that ε is a root of unity. To prove the second statement, let $R > 0$ and let $B \subset F_{\mathbf{R}}$ be the subset

$$\{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in F_{\mathbf{R}} : |x_i| < R \text{ and } |z_i| < R \text{ for all } i\}.$$

Then B is bounded and hence $B \cap F_{\mathbf{R}}^{\perp}$ is a bounded subset of $F_{\mathbf{R}}^{\perp}$. Suppose that the logarithmic image of $\varepsilon \in O_F^*$ is in B. This means that $|\phi_i(\varepsilon)| < e^R$ for all $i = 1, \ldots, n$. Since O_F is a lattice in $F_{\mathbf{R}}$ and since the group of roots of unity μ_F is finite, there are only finitely many units ε with this property. It follows that the image $\mathrm{Log}|O_F^*|$ is discrete subgroup of $F_{\mathbf{R}}^{\perp}$.

Corollary 9.4. *Let F be a number field of degree n. Then its unit group O_F^* is a finitely generated group of rank at most r.*

Proof. Indeed, let W be the subvector space of $F_{\mathbf{R}}^{\perp}$ spanned by $\mathrm{Log}|O_F^*|$. By Proposition 6.6 (c), the group $\mathrm{Log}|O_F^*|$ is a lattice in W. Since the dimension of $F_{\mathbf{R}}^{\perp}$ is r, the rank of $\mathrm{Log}|O_F^*|$ is at most r.

To prove that the rank of O_F^* is *equal* to r is more difficult. Let F be a number field of degree n and discriminant Δ_F. We write δ for the covolume $\sqrt{|\Delta_F|}$ of $O_F \subset F_{\mathbf{R}}$. We have inclusions

$$F_{\mathbf{R}}^{\perp} \ \subset \ F_{\mathbf{R}}^{0} \ \subset \ F_{\mathbf{R}}.$$

Let $\pi : F_{\mathbf{R}}^{0} \longrightarrow F_{\mathbf{R}}^{\perp}$ be the orthogonal projection on $F_{\mathbf{R}}^{\perp}$. It is given by

$$\pi(x) \ = \ x - \frac{Tr(x)}{n} \cdot 1, \qquad \text{for } x \in F_{\mathbf{R}}^{0}.$$

We let $\lambda : F_{\mathbf{R}}^{*} \longrightarrow F_{\mathbf{R}}^{\perp}$ denote the homomorphism that is the composition of the Log-map $F_{\mathbf{R}}^{*} \to F_{\mathbf{R}}^{0}$ and the orthogonal projection on $F_{\mathbf{R}}^{\perp}$. Explicitly we have

$$\lambda(x) \ = \ \pi(\mathrm{Log}|x|) \ = \ \mathrm{Log}|x| - \frac{Tr(\mathrm{Log}|x|)}{n} \cdot 1 \ = \ \mathrm{Log}|\frac{x}{N(x)^{1/n}}|.$$

There are only finitely many non-zero principal ideals of O_F with norm at most δ. Let $\alpha_1, \ldots, \alpha_t \in O_F$ be generators of these ideals. For each $i = 1, \ldots, t$ let B_i denote the closed ball with center $\lambda(\alpha_i)$ and radius $\log \delta$:

$$B_i = \{z \in F_{\mathbf{R}}^{\perp} : \|z - \lambda(\alpha_i)\| \leq \log \delta\}.$$

We put

$$L \ = \ \mathrm{Log}|O_F^*|.$$

This is a subgroup of $F_{\mathbf{R}}^{+}$. Since $|N(\varepsilon)| = 1$ for every $\varepsilon \in O_F^*$ it is contained in $F_{\mathbf{R}}^{\perp}$.

Proposition 9.5. *We have*

$$F_{\mathbf{R}}^{\perp} = \{y + z : y \in L \text{ and } z \in \bigcup_{i=1}^{n} B_i\}.$$

Proof. Let $x = (x_\phi)$ be an arbitrary element of $F_{\mathbf{R}}^{\perp}$. By e^x we denote the element (e^{x_ϕ}) of $F_{\mathbf{R}}^{*}$. The box

$$B \ = \ \{(z_\phi) \in F_{\mathbf{R}} : |z_\phi| \leq \delta^{1/n} \text{ for all embeddings } \phi\}.$$

is convex and symmetric and has has volume $2^{r_1}\sqrt{2\pi}^{r_2}\delta \geq 2^n\delta$. We multiply B by e^x. The result is another convex and symmetric box

$$e^x B \;=\; \{(z_\phi) \in F_{\mathbf{R}} : |z_\phi| \leq e^x \delta^{1/n} \text{ for all embeddings } \phi\}.$$

Since the trace of x is zero, the norm of e^x is 1. It follows that the volume of the box $e^x B \subset F_{\mathbf{R}}$ is equal to the volume of B and is hence at least $2^n\delta$. By Minkowski's convex body theorem there exists therefore a non-zero vector in $O_F \cap e^x B$. In other words, there is a non-zero $a \in O_F$ for which

$$|\phi(a)| \leq e^{x_\phi}\delta^{1/n}, \qquad \text{for all embeddings } \phi.$$

This implies that $|N(a)| \leq \delta$. Therefore the principal ideal generated by a is one of the principal ideals (α_i) with $1 \leq i \leq t$ that were enumerated above. This means that $a = \varepsilon\alpha_i$ for some unit $\varepsilon \in O_F^*$. Put $y = \mathrm{Log}(\varepsilon) = \lambda(\varepsilon)$. Then we put

$$z = x - y.$$

To show that $z = x - \mathrm{Log}(\varepsilon)$ is in B_i, we check that $\|z - \lambda(\alpha_i)\|$ is at most $\log\delta$. We have $z - \lambda(\alpha_i) = x - \lambda(a)$ and the inequalities

$$\lambda(a)_\phi = \log\left|\frac{\phi(a)}{N(a)^{1/n}}\right| \;\leq\; \log|\phi(a)| \leq x_\phi + \frac{1}{n}\log\delta, \qquad \text{for all embeddings } \phi.$$

Here we used the fact that $|N(a)| \geq 1$. Since the sum over all ϕ of $\lambda(a)_\phi$ and of x_ϕ is zero, the lemma below applies to the real numbers $\lambda(a)_\phi - x_\phi$. We get

$$\|z - \lambda(a_i)\|^2 = \|\lambda(a) - x\|^2 \;=\; \sum_{\phi\in\Phi}(\lambda(a)_\phi - x_\phi)^2 \leq \frac{n(n-1)}{n^2}\log^2\delta \;<\; \log^2\delta,$$

as required.

Corollary 9.6. *(Dirichlet's unit theorem) The group L is a lattice inside $F_{\mathbf{R}}^{\perp}$.*

Proof. Since each ball B_i is compact and since the composite map

$$\bigcup_{i=1}^{t} B_i \;\hookrightarrow\; F_{\mathbf{R}}^{\perp} \;\longrightarrow F_{\mathbf{R}}^{\perp}/L$$

is continuous and surjective, Lemma 9.5 implies that $F_{\mathbf{R}}^{0}/L$ is compact and we are done.

The covolume of the lattice $\mathrm{Log}|O_F^*|$ in the Euclidean space $F_{\mathbf{R}}^{\perp}$ is an invariant of the number field F. To compute it we choose generators ε_i for $i = 1, \ldots, r$ of O_F^*/μ_F and complete the vectors

$$\begin{pmatrix} \log|\phi_1(\varepsilon_1)| \\ \vdots \\ \log|\phi_n(\varepsilon_1)| \end{pmatrix}, \ldots, \begin{pmatrix} \log|\phi_1(\varepsilon_r)| \\ \vdots \\ \log|\phi_n(\varepsilon_r)| \end{pmatrix} \qquad \text{in } F_{\mathbf{R}} \qquad (*)$$

to a basis of $F_{\mathbf{R}}$ by adding vectors of $F_{\mathbf{R}}$ that are orthogonal to one another and to $F_{\mathbf{R}}^{\perp}$.

More precisely, we add the vector $1 \in F \subset F_{\mathbf{R}}$. It has length $\sqrt{n}$. Moreover, for each of the r_2 pairs of complex conjugate embeddings $\phi, \overline{\phi} : F \hookrightarrow \mathbf{C}$ we add the vector $e_{\phi,\overline{\phi}}$ whose coordinates corresponding to ϕ and $\overline{\phi}$ are equal to $+1$ and -1 respectively, while all other coordinates are zero. It is orthogonal to $F_{\mathbf{R}}^{\perp}$ because $|\phi(a)| = |\overline{\phi}(a)|$ for each $a \in F$. The length of $e_{\phi,\overline{\phi}}$ is $\sqrt{2}$. The covolume of $\mathrm{Log}|O_F^*|$ is

$$\frac{1}{\sqrt{2^{r_2} n}} |\det M|$$

where M is the $n \times n$-matrix whose columns are the $r = r_1 + r_2 - 1$ vectors listed in $(*)$, the r_2 vectors $e_{\phi,\overline{\phi}}$ and the vector 1. It is closely related to the classical *regulator* R. We have

$$\mathrm{covol}\, \mathrm{Log}|O_F^*| = \sqrt{\frac{n}{2^{r_2}}} R.$$

Example 9.8. We compute the unit group O_F^* of the field $F = \mathbf{Q}(\sqrt{67})$. We have $r_1 = 2$ and $r_2 = 0$. Since F admits embeddings into $\mathbf{R}$, the group of roots of unity in F is $\{\pm 1\}$. By Prop. 3.4 the ring of integers of F is $O_F = \mathbf{Z}[\sqrt{67}]$. By Dirichlet's Unit Theorem the group O_F^* is isomorphic to $\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. In other words, the ring O_F contains a unit ε for which we have

$$O_F^* = \{\pm\varepsilon^k : k \in \mathbf{Z}\}.$$

We compute such a *fundamental unit* by exhibiting a principal ideal of O_F that is generated by an element $u \in O_F$ and also by some other element $v \in O_F$.The quotient u/v is then in O_F^*. We begin by factoring some principal ideals of O_F into products of prime ideals Recall that for $k \in \mathbf{Z}$ the norm of the element $k - \sqrt{67} \in O_F$ is equal to $k^2 - 67$. We compute the factorizations of some ideals generated by elements β of the form $\beta = \sqrt{67} - k$ that have small norms.

Table 9.9.

	k	β	$N(\beta) = k^2 - 67$	(β)
(i)	5	$\sqrt{67} - 5$	$-42 = -2 \cdot 3 \cdot 7$	${\mathfrak{p}_2}^2\mathfrak{p}_3'\mathfrak{p}_7$
(ii)	6	$\sqrt{67} - 6$	-31	$\mathfrak{p}_{31}$
(iii)	7	$\sqrt{67} - 7$	$-18 = -2 \cdot 3^2$	$\mathfrak{p}_2\mathfrak{p}_3^2$
(iv)	8	$\sqrt{67} - 8$	-3	$\mathfrak{p}_3$
(v)	9	$\sqrt{67} - 9$	$14 = 2 \cdot 7$	$\mathfrak{p}_2\mathfrak{p}_7'$
(vi)	10	$\sqrt{67} - 10$	$33 = 3 \cdot 11$	$\mathfrak{p}_3\mathfrak{p}_{11}$

In this example only the prime ideals of norm ≤ 7 play a role. They divide the prime numbers $p \leq 7$. By Theorem 7.1 the factorization of the primes $p \leq 7$ is determined by the factorization of the polynomial in irreducible factors in the ring $\mathbf{F}_p[X]$. The results are listed in Table 9.10 below.

Table 9.10.

p	$X^2+67 \pmod p$	factorization	prime ideals
2	$(X-1)^2$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2=(2,\sqrt{(67)}-1)$
3	$(X-1)(X+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$	$\mathfrak{p}_3=(3,\sqrt{67}-1)$ and $\mathfrak{p}_3'=(3,\sqrt{67}+1)$
5	X^2-2	(5)	
7	$(X-2)(X+2)$	$\mathfrak{p}_7\mathfrak{p}_7'$	$\mathfrak{p}_7=(7,\sqrt{67}-2)$ and $\mathfrak{p}_7'=(7,\sqrt{67}+2)$

Even if our goal is to compute the unit group of F, note that the Minkowski constant of F is equal to

$$\frac{2!}{2^2}\sqrt{4\cdot 67}\leq 8.5.$$

Therefore the class group is generated by the prime ideals of norm at most 7. Lines (iii) and (v) of Table 9.9 show that Cl_F is actually generated by the primes lying over 3. Since these are principal by line (iv), the class group of O_F is trivial and O_F is a PID.

Lines (iii) and (iv) of Table 9.9 show that

$$\frac{(\alpha-8)^2(\alpha-7)}{9}=-221+27a$$

is an element of O_F of norm 2. Therefore both its square and the number 2 generate the ideal (2). It follows that

$$\varepsilon=\frac{1}{2}(-221+27a)^2=48842-5967\sqrt{67}$$

is a unit of O_F.

It remains to show that ε and -1 *generate* the group O_F^* or, equivalently, that ε generates the cyclic group $O_F^*/\{\pm1\}$. This can be done by a search among small elements of O_F as follows. Any element $a\in O_F$ can be written as $a=X+Y\sqrt{67}$ for certain integers X and Y. Therfore the square of the length of an element $a\in O_F$ is given by

$$\|a\|^2=\phi_1(a)^2+\phi_2(a)^2=2(X^2+67Y^2).$$

If ε does not generate $O_F^*/\{\pm1\}$, then $\varepsilon=\pm\eta^k$ for some generator η and $|k|\geq 2$. Since $|\phi_1(\varepsilon)|=97683.99\ldots$ and $|\phi_2(\varepsilon)|=0.00001\ldots$. We see that $|\phi_1(\eta)|\leq|\phi_1(\varepsilon)|^{1/2}=312.54$ while $|\phi_2(\eta)|\leq 1$. Writing $\eta=X+Y\sqrt{67}$, this means that

$$\|\eta\|^2=2(X^2+67Y^2)\leq 312.54^2+1\leq 97685.$$

Since $N(\eta)=X^2-67Y^2$ is equal to ±1 this implies $4\cdot 67Y^2\leq 97687$ and hence $|Y|\leq 19$. It is a finite computation to check that only for $Y=0$ there is an $X\in\mathbf{Z}$ for which $X^2-67Y^2=\pm1$. Indeed, these values of X and Y correspond to $\eta=\pm1$, contradicting the fact that ε is a power of η. It follows that ε is a generator of $O_F^*/\{\pm1\}$.

The final finite, lengthy computation can be considerably shortened by proving that if $\varepsilon=\pm\eta^k$ for some $k\in\mathbf{Z}$, then $|k|$ must be considerably larger than 2. This can be done by excluding prime divisors p of k. In this example we show that k is not divisble by 2 or 3.

This implies $|k| \geq 5$ and hence $|\phi_1(\eta) \leq |\phi_1(\varepsilon)|^{1/5} = 9.96$ while $|\phi_2(\eta) \leq 1$. It follows that $\|\eta\|^2 = 2(X^2 + 67Y^2) \leq 100.1$. This implies at once $Y = 0$ and hence $X = \pm 1$. AS before it follows that ε is a generator of $O_F^*/\{\pm 1\}$.

We first show that k is not even. For if k were even, then one of $\pm\varepsilon$ would be a square. Since $\phi_1(\varepsilon)$ is positive, $-\varepsilon$ cannot be a square. We show that ε is not a square either by showing that it is not a square modulo a suitably chosen prime ideal $\mathfrak{p}$ of O_F. We take the small prime ideal $\mathfrak{p} = \mathfrak{p}_3$. The residue field $O_F/\mathfrak{p}_3$ is $\mathbf{F}_3$. The image of $\varepsilon = 48842 - 5967\sqrt{67}$ in $O_F/\mathfrak{p}_3$ is 2, which is not a square in $\mathbf{F}_3$. Therefore ε is not a square in O_F either. This shows that k must be odd.

Similarly, k is not divisible by 3. Since -1 is a cube in O_F, the exponent k is divisible by 3 if and only if ε is a cube. This time we choose a prime ideal $\mathfrak{p}$ for which $\#(O_F/\mathfrak{p})^*$ is divisible by 3. We take $\mathfrak{p} = \mathfrak{p}_7$. It has residue field $\mathbf{F}_7$ and the subgroup of cubes is $\{\pm 1\}$. Since $\sqrt{67} \equiv 2 \pmod{\mathfrak{p}_7}$, the image of $\varepsilon = 48842 - 5967\sqrt{67}$ in $O_F/\mathfrak{p}_7$ is $3 - 3 \cdot 2 = 4$, which is not a cube in $\mathbf{F}_7$. Therefore ε is not a cube in O_F.

This completes the computation. The covolume of the lattice $\mathrm{Log}|O_F^*|$ is

$$\frac{1}{\sqrt{2}} \det \begin{pmatrix} 1 & \log|\phi_1(\varepsilon)| \\ 1 & \log|\phi_2(\varepsilon)| \end{pmatrix} = \sqrt{2} \log(48842 + 5967\sqrt{67}),$$

which is indeed $\sqrt{2}$ times the usual regulator.

Exercises.

9.1 Let $n > 1$ and $M \in \mathbf{R}$. Suppose that $x_1, \ldots, x_n \in \mathbf{R}$ satisfy

$$x_i \leq M \text{ for } i = 1, \ldots, n \qquad \text{and} \qquad \textstyle\sum_{i=1}^n x_i \geq 0.$$

Prove the inequality $\sum_{i=1}^n x_i^2 \leq n(n-1)M^2$.

9.2 Let F be a number field of degree n. The *regulator* R_F is defined as follows. Let r_1 and r_2 be as usual. So we have $r_1 + 2r_2 = n$. Put $r = r_1 + r_2 - 1$. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a $\mathbf{Z}$-basis of the unit group O_F^* modulo roots of unity.
Let $\phi_1, \ldots, \phi_{r_1}$ denote the embeddings $F \longrightarrow \mathbf{C}$ whose image is in $\mathbf{R}$ and $\phi_{r_1}, \ldots, \phi_{r_1+r_2}$ embeddings $F \longrightarrow \mathbf{C}$ that are mutually non-conjugate. Put $r = r_1 + r_2 - 1$. Then

$$R_F = |\det(M)|$$

where M is the $r \times r$-matrix whose rows are vectors of the form $\log(\phi_i|\varepsilon_1|'), \ldots), \log(\phi_i|\varepsilon_r|')$. Here i runs through the indices $1, \ldots, r$ except one. The absolute value $|x|'$ is the usual one on the real coordinates, but its square on the complex ones.

(a) Show that the regulator R_F is well defined, i.e. it does not depend on the choice of the embedding $\phi_i : F \to \mathbf{C}$ that was left out.

(b) Show that $R_F = \sqrt{\frac{2^{r_2}}{n}} \cdot \mathrm{covol}\,\mathrm{Log}|O_F^*|$.

9.3 Let $f(T)$ be a monic polynomial in $\mathbf{Z}[T]$. Show: if $\mathrm{Disc}(f) = 1$, then f is linear or $f(T) = (T-k)(T-k-1)$ for some $k \in \mathbf{Z}$.

9.4 Show that if the rank of the unit group O_F^* of a number field F is 1, then $[F : \mathbf{Q}] = 2$, 3 or 4.

9.5 (*Pell's equation.*) Show that for every positive integer d the equation

$$X^2 - dY^2 = 1$$

has solutions $X, Y \in \mathbf{Z}_{>0}$.

9.6 Let $f(T) \in \mathbf{Z}[T]$ be a polynomial all of whose roots in $\mathbf{C}$ are on the unit circle. Show that all roots of f are roots of unity.

9.7 Let $\eta \in \mathbf{C}$ be a sum of roots of unity. Show that if $|\eta| = 1$, then η is a root of unity.