LECTURE APRIL 15: SOME MORE ALGEBRAIC NUMBER THEORY

1. Algebraic number theory: the basics

Definition 1.1. *A complex number $\alpha \in \mathbf{C}$ is* integral *if it is the root of a* monic *polynomial with* integer coefficients*. Then α is called an* algebraic integer*, as opposed to a* rational integer*, which refers to elements of $\mathbf{Z}$. We let $\overline{\mathbf{Z}}$ denote the set of algebraic integers.*

Example of an algebraic integer: $\sqrt{2}$ is a root of $x^2 - 2$.

Not an algebraic integer: $\alpha = 1/2$. If $1/2$ were the root of $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbf{Z}$, then the rational root theorem says that $2|1$, which is false. In fact $\overline{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$.

Theorem 1.2. *$\overline{\mathbf{Z}} \subset \mathbf{C}$ is a subring.*

To prove this theorem, we need to review some facts about finitely generated abelian groups. A finitely generated abelian group is a group M which is abelian, such that there exist elements $\alpha_1, \ldots, \alpha_n \in M$ which generate M. Example: $\mathbf{Z}^4$, or $\mathbf{Z} \oplus \mathbf{Z}/6$. An abelian group is *torsion-free* if for all nonzero $\alpha \in M$, the elements $2\alpha, 3\alpha, \ldots$ are also nonzero.

If a finitely generated abelian group is torsion-free, then it is free. Free means that there exist elements $\alpha_1, \ldots, \alpha_n$ such that

$$M = \mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n \cong \mathbf{Z}^n.$$

(If $M = \mathbf{Q}$, then M is torsion-free, but not free. The problem is that this group is not finitely generated.)

We are often going to consider finitely generated subgroups $M \subset \mathbf{C}$ (under addition). These are automatically free, because they are torsion-free and finitely generated. For instance $M = \mathbf{Z} \oplus \mathbf{Z}i = \mathbf{Z}[i]$.

Theorem 1.3. *The following are equivalent, for a complex number α.*

1. *α is an algebraic integer.*
2. *There exists a finitely generated subgroup $M \subset \mathbf{C}$ such that $\alpha M \subset M$.*

Proof. Assume that α is the root of an irreducible polynomial with integer coefficients:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

with $a_i \in \mathbf{Z}$.

Let M be the subgroup of $\mathbf{C}$ generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Can check that $\alpha M \subset M$. This really just comes down to checking that $\alpha \cdot \alpha^{n-1}$ belongs to M, but

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0 \cdot 1 \in M.$$

Conversely, suppose that there exists a finitely generated subgroup $M \subset \mathbf{C}$ such that $\alpha M \subset M$. Choose a basis for M:

$$M = \mathbf{Z}\alpha_1 \oplus \mathbf{Z}\alpha_2 \oplus \cdots \oplus \mathbf{Z}\alpha_n,$$

for $\alpha_i \in \mathbf{C}$. This means that $\alpha\alpha_i \in M$ for $i = 1, \ldots, n$. Let's spell this out:

$$\begin{aligned}
\alpha\alpha_1 &= a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n \\
\alpha\alpha_2 &= a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n \\
\vdots\; &\;\vdots \\
\alpha\alpha_n &= a_{n1}\alpha_1 + a_{n2}\alpha_2 + \cdots + a_{nn}\alpha_n
\end{aligned}$$

with $a_{ij} \in \mathbf{Z}$. If I let $A = (a_{ij})$, and $v = (\alpha_1, \dots, \alpha_n)^t$ (a column vector), then $Av = \alpha v$. In other words, A has an eigenvector v with value α. This means that α is the root of the characteristic polynoimal $f(t) = \det(tI - A)$. Then $f(t)$ is a monic polynomial with integer coefficients!! Therefore $\alpha \in \overline{\mathbf{Z}}$. $\square$

We can now prove that $\overline{\mathbf{Z}} \subset \mathbf{C}$ is a subring. We just need to check that $\overline{\mathbf{Z}}$ is closed under addition and multiplication.

Let $\alpha, \beta \in \overline{\mathbf{Z}}$. Then there exist finitely generated abelian subgroups $M, N \subset \mathbf{C}$ such that $\alpha M \subset M$ and $\beta N \subset N$. Let MN be the abelian group generated by all products of elements of M and N. Then MN is still finitely generated (check this!). We have

$$(\alpha + \beta)MN = \alpha MN + \beta MN \subset MN + M\beta N \subset MN + MN = MN.$$

Similarly,

$$\alpha\beta MN = (\alpha M)(\beta N) \subset MN,$$

so that $\alpha + \beta$ and $\alpha\beta$ are both in $\overline{\mathbf{Z}}$.

Next time: we'll compute $\overline{\mathbf{Z}} \cap K = \mathcal{O}_K$ for various values of K, where $K/\mathbf{Q}$ is finite.

2. Examples: Quadratic fields

Given a finite extension $K/\mathbf{Q}$, we can define

$$\mathcal{O}_K = K \cap \overline{\mathbf{Z}},$$

the *ring of integers* of K.

If $[K : \mathbf{Q}] = 2$, then $K = \mathbf{Q}(\sqrt{m})$. We can assume that m is an integer, and even a squarefree integer, other than 1. What is $\mathcal{O}_K$?

If $a + b\sqrt{m} \in K$ (with $a, b \in \mathbf{Q}$), when does it belong to $\mathcal{O}_K$? The characteristic polynomial of $\alpha = a + b\sqrt{m}$ is

$$x^2 - \mathrm{tr}(\alpha)x + N(\alpha),$$

in order for α to belong to $\mathcal{O}_K$, we need $\mathrm{tr}(\alpha), N(\alpha) \in \mathbf{Z}$, that is:

$$\begin{aligned} 2a &\in \mathbf{Z} \\ a^2 - mb^2 &\in \mathbf{Z} \end{aligned}$$

Certainly these conditions are satisfied if $a, b \in \mathbf{Z}$; thus $\mathbf{Z}[\sqrt{m}] \subset \mathcal{O}_K$. But it may be possible that $a = \frac{1}{2}a_0$, where a_0 is odd. This forces $b = \frac{1}{2}b_0$, where b_0 is odd (exercise). Then

$$a_0^2 - mb_0^2 \equiv 0 \pmod 4$$

This means that $1 - m \equiv 0 \pmod 4$, so that $m \equiv 1 \pmod 4$.

Theorem 2.1. *The ring of integers $\mathcal{O}_K$ is*

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{m}] & m \equiv 2, 3 \pmod 4 \\ \mathbf{Z}[\frac{-1+\sqrt{m}}{2}] & m \equiv 1 \pmod 4 \end{cases}$$

In the second case, let $\eta = \frac{-1+\sqrt{m}}{2}$. Then η has minimal polynomial $x^2 + x - (m-1)/4$, and then $\mathcal{O}_K = \mathbf{Z}[\eta]$. One observation here is that $\mathcal{O}_K$ is always a free abelian group of rank 2. In the first case, $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\sqrt{m}$, and in the second case, $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\eta$.

Thus the ring of integers in $\mathbf{Q}(\sqrt{5})$ is $\mathbf{Z}[\phi]$, $\phi = (-1 + \sqrt{5})/2$, whereas $\mathbf{Q}(\sqrt{-5})$ has ring of integers $\mathbf{Z}[\sqrt{-5}]$.

3. The structure of $\mathcal{O}_K$ as an abelian group

Theorem 3.1. *Let $[K : \mathbf{Q}] = n$. Then $\mathcal{O}_K$ is a free abelian group of rank n.*

We have that $K = \mathbf{Q}(\alpha)$, where α is the root of an irreducible polynomial of degree n. There are exactly n conjugates of α in $\mathbf{C}$. We can therefore define n homomorphisms $\sigma_1, \dots, \sigma_n \colon K \to \mathbf{C}$. These are *embeddings*.

Let $\alpha_1, \dots, \alpha_n$ be a basis for $K/\mathbf{Q}$. Define a matrix

$$M(\alpha_1, \dots, \alpha_n) = (\sigma_i(\alpha_j)).$$

This is an $n \times n$ matrix. In fact it is invertible!

Theorem 3.2. *The determinant* $(\det M(\alpha_1, \dots, \alpha_n))^2$ *is a nonzero rational number.*

Proof. The elements $\sigma_i(\alpha_j)$ all belong to the splitting field of K in $\mathbf{C}$, call it E. Let $G = \mathrm{Gal}(E/\mathbf{Q})$. Elements of G have the effect of *permuting* the embeddings σ_i, and therefore they permute the columns of the matrix $M(\alpha_1, \dots, \alpha_n)$. This has the effect of changing the determinant by a sign, and therefore doesn't change the squared determinant at all. $\square$

Theorem 3.3. *Let $\alpha \in K$. Then there exists a rational integer M, such that $M\alpha \in \mathcal{O}_K$.*

(Exercise)

We can therefore find a basis $\alpha_1, \dots, \alpha_n$ for $K/\mathbf{Q}$ consisting of elements of $\mathcal{O}_K$. Then we have

$$\det M(\alpha_1, \dots, \alpha_n)^2 \in \overline{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$$

is a nonzero rational integer.

By the well-ordered property of the natural numbers, there exists a basis $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ for $K/\mathbf{Q}$, which makes

$$\left|\det M(\alpha_1, \dots, \alpha_n)^2\right|$$

as small as possible.

I now claim that

$$\mathcal{O}_K = \mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n.$$

Let $\alpha \in \mathcal{O}_K$ not belong to $\mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n$. This means we can write α as a linear combination

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

where $c_i \in \mathbf{Q}$ are not all integers. WLOG, $c_1 \notin \mathbf{Z}$. By replacing α with $\alpha - m\alpha_1$ we can also assume $0 < c_1 < 1$. Then we have a new basis for $K/\mathbf{Q}$ given by $\alpha, \alpha_2, \alpha_3, \dots, \alpha_n$. We have

$$\det M(\alpha, \alpha_2, \dots, \alpha_n) = \det M(c_1\alpha_1, \alpha_2, \dots, \alpha_n) = c_1 \det(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Since $c_1^2 < 1$, this contradicts the minimality of $\det M(\alpha_1, \dots, \alpha_n)^2$.

Definition 3.4. *Let $[K : \mathbf{Q}] = n$, and let $\alpha_1, \dots, \alpha_n$ be any $\mathbf{Z}$-basis for the free abelian group $\mathcal{O}_K$. The integer*

$$D = \det M(\alpha_1, \dots, \alpha_n)^2 \in \mathbf{Z}$$

is called the discriminant *of $K/\mathbf{Q}$.*

Example 3.5. *What is the discriminant of $\mathbf{Q}(i)$? A $\mathbf{Z}$-basis would be $1, i$. The discriminant is*

$$D = \det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}^2 = -4$$

Example 3.6. *The fields $\mathbf{Q}(\sqrt{-3}), \mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{-7}), \mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{-2})$ have discriminants $-3, -4, 5, -7, 8, -8$, respectively.*

4. Units

The group of units in $\mathcal{O}_K$ is an interesting group.

Example 4.1. $\mathbf{Z}[i]^\times = \{1, -1, i, -i\}$

Example 4.2. *$\mathbf{Z}[\phi]^\times$ is an infinite group, generated by -1 and ϕ. Thus $\mathbf{Z}[\phi]^\times \cong \mathbf{Z} \times \mathbf{Z}_2$.*

Let K be an algebraic number field (i.e., $K/\mathbf{Q}$ is a finite extension).

Definition 4.3. *Let $\sigma_1, \ldots, \sigma_n \colon K \to \mathbf{C}$ be the embeddings of K into $\mathbf{C}$. The* norm *of an element $\alpha \in K$ is*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Then $N(\alpha) \in \mathbf{Q}$. Note that $N(\alpha\beta) = N(\alpha)N(\beta)$. Thus $N \colon K^\times \to \mathbf{Q}^\times$ is a group homomorphism.

Example 4.4. *Let $m \neq 1$ be a squarefree integer, and let $K = \mathbf{Q}(\sqrt{m})$. A typical element of K is $\alpha = a + b\sqrt{m}$, where $a, b \in \mathbf{Q}$. Then*

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

Thus in $\mathbf{Q}(i)$, we have

$$N(a + bi) = a^2 + b^2.$$

Lemma 4.5. *Let $\alpha \in \mathcal{O}_K$. Then $N(\alpha) \in \mathbf{Z}$.*

Proof. If α is an algebraic integer, then so are its conjugates, and then $N(\alpha)$, being the product of these, must also lie in $\overline{\mathbf{Z}}$. But also $N(\alpha) \in \mathbf{Q}$, and therefore $N(\alpha) \in \mathbf{Z}$. $\square$

Theorem 4.6. *Let $\alpha \in \mathcal{O}_K$. Then $\alpha \in \mathcal{O}_K^\times$ if and only if $N(\alpha) = \pm 1$.*

Proof. Suppose α is a unit, so that $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. Then $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. Since $N(\alpha), N(\beta) \in \mathbf{Z}$, we must have $N(\alpha) = \pm 1$.

Conversely, suppose $N(\alpha) = \pm 1$. Then

$$\alpha \prod_{i=2}^{n} \sigma_i(\alpha) = \pm 1.$$

Let $\beta = \prod_{i=2}^{n} \sigma_i(\alpha)$, so that $\alpha\beta = \pm 1$. Then $\beta \in K$, but also $\beta \in \overline{\mathbf{Z}}$, and so $\beta \in \mathcal{O}_K$. Then $\pm\beta$ is the inverse of α. $\square$

Let's try to find $\mathcal{O}_K^\times$ when $K = \mathbf{Q}(\sqrt{m})$.

Example 4.7. *If $m = -1$, then $N(a + bi) = a^2 + b^2$. This is always positive, so $a + bi \in \mathbf{Z}[i]$ is a unit if and only if $a^2 + b^2 = 1$. This clearly has only four solutions $\alpha = \pm 1, \pm i$.*

Example 4.8. *Let $K = \mathbf{Q}(\sqrt{2})$, so that $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$. An element $a + b\sqrt{2} \in \mathcal{O}_K$ is a unit if and only if*

$$a^2 - 2b^2 = \pm 1.$$

This is a Diophantine equation. A few solutions are $(1, 0), (1, 1), (3, 2), (7, 5)$..... Consider first the solution $(1, 1)$, which corresponds to $\epsilon = 1 + \sqrt{2}$. Its powers are

$$\begin{aligned} \epsilon^2 &= 3 + 2\sqrt{2} \\ \epsilon^3 &= 7 + 5\sqrt{2} \end{aligned}$$

In fact, all solutions appear this way, and $\mathbf{Z}[\sqrt{2}]^\times$ is generated by -1 and ϵ. Thus $\mathbf{Z}[\sqrt{2}]^\times \cong \mathbf{Z}_2 \times \mathbf{Z}$.

The Diophantine equation

$$a^2 - mb^2 = 1$$

is called *Pell's equation*, and it has a very long history. First of all, m should be positive to have any chance of their being an integer solution.

Theorem 4.9. *Let $m > 1$ be square free. Then Pell's equation $a^2 - mb^2 = 1$ has infinitely many solutions. The group of units $\mathcal{O}_K^\times$ ($K = \mathbf{Q}(\sqrt{m})$) is generated by -1 and one* fundamental unit *ϵ.*

Proof. At least, we'll try to come up with one nontrivial solution to $a^2 - mb^2 = 1$. Nontrivial means $b \neq 0$. If (a, b) is a solution with $a, b > 0$, then

$$(a - b\sqrt{m})(a + b\sqrt{m}) = 1.$$

This means that $a - b\sqrt{m}$ is kind of small. I'm getting at the fact that a/b is close to $\sqrt{m}$. $\square$

Let's talk about *rational approximations to irrational numbers.* Given an irrational number α, when is a fraction p/q a good rational approximation?

Theorem 4.10. *Let α be irrational, and let $N \geqslant 1$. There exists a fraction p/q with $q \leqslant N$, such that*

$$\left|\frac{p}{q} - \alpha\right| \leqslant \frac{1}{qN}$$

Proof. Recall the floor function: $[\pi] = 3$. The fractional part is everything else:

$$\{\pi\} = .14159... = \pi - [\pi].$$

Thus $0 < \{\alpha\} < 1$. Let $N \geqslant 1$, and consider the numbers $\{q\alpha\}$ for $q = 1, \dots, N$. Chop up the interval $(0, 1)$ into N parts:

$$(0, 1/N), (1/N, 2/N), \dots, ((N-1)/N, 1).$$

If one of the $\{qN\}$ lies in the first or last interval, we're done. Assume not: then our n numbers land in $n-1$ intervals, and therefore two of them must end up in the same interval: there exist $q_1 < q_2 \leqslant N$, such that

$$|\{q_2\alpha\} - \{q_1\alpha\}| = |(q_2 - q_1)\alpha - [q_2\alpha] - [q_1\alpha]| < 1/N.$$

Let $q = q_2 - q_1$, and let $p = [q_2\alpha] + [q_1\alpha]$; then

$$|q\alpha - p| < 1/N,$$

and so

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{qN}.$$

$\square$

The theorem shows that there exist infinitely many "good" approximations to α, where good means that

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^2}.$$

Let's apply this to $\alpha = \sqrt{m}$. If p/q is a good approximation to $\sqrt{m}$, then

$$\left|p - q\sqrt{m}\right| < \frac{1}{q}.$$

On the other hand

$$\left|p + q\sqrt{m}\right| = \left|(p - q\sqrt{m}) + 2q\sqrt{m}\right| < 3q\sqrt{m}$$

Multiplying, we get

$$\left|p^2 - mq^2\right| \leqslant \frac{1}{q}3q\sqrt{m} = 3\sqrt{m}.$$

In other words, we have found an infinite collection of elements $p + q\sqrt{m} \in \mathbf{Z}[\sqrt{m}]$ with norm bounded by some constant.

Consider the infinite sequence of ideals $I = (p + q\sqrt{m})$ generated by these elements. The norm of $p + q\sqrt{m}$ has absolute value bounded by $M = 3\sqrt{m}$. Now, I contains this norm $n = p^2 - mq^2$.

The set of ideals of $\mathbf{Z}[\sqrt{m}]$ containing a particular integer n is in bijection with the set of ideals of $\mathbf{Z}[\sqrt{m}]/n$. The latter ring is a finite ring (of order n^2), and so there are only finitely many ideals in it.

We find that the infinite sequence of ideals I ranges through a finite set. Thus two of these ideals must be the same: $(\alpha) = (\beta)$. Then α/β must be a unit in $\mathbf{Z}[\sqrt{m}]$.

5. The unit group and the class number

Last time we showed that if $m > 1$ is a square-free integer, then Pell's eqution $a^2 - mb^2 = 1$ has a nontrivial solution (nontrivial means not $(\pm 1, 0)$). In terms of algebraic number theory, this means that if $K = \mathbf{Q}(\sqrt{m})$, and $\mathcal{O}_K$ is the ring of integers, then the unit group $\mathcal{O}_K^\times$ contains at least one element other than ± 1. This element has to be of infinite order.

Let's now finish the job:

Theorem 5.1. *Let $K = \mathbf{Q}(\sqrt{m})$, where $m > 1$ is a square-free integer. Then $\mathcal{O}_K^\times \cong \mathbf{Z}_2 \times \mathbf{Z}$. That is, it is generated by -1 and one unit ϵ of infinite order.*

The unit ϵ is called the *fundamental unit* of K.

Proof. First I claim that there is at least one unit ϵ which is > 1. We already know that there's a unit $\epsilon \neq \pm 1$.

Given an element $\alpha = a + b\sqrt{m} \in \mathbf{Q}(\sqrt{m})$, I let $\overline{\alpha} = a - b\sqrt{m}$. We have $N(\alpha) = \alpha\overline{\alpha}$. Given a unit ϵ, we have $\epsilon\overline{\epsilon} = N(\epsilon) = \pm 1$. Replacing ϵ with one of $-\epsilon, 1/\epsilon, -1/\epsilon$, we can assume that $\epsilon > 1$.

I want to choose ϵ to be the *least* unit which is greater than 1. I have to justify why I can do this. I claim that there are only finitely many units in any interval $(1, N)$. It's enough to show this for units which have norm 1. If ϵ has norm 1, then $\overline{\epsilon} = 1/\epsilon$. If $\epsilon \in (1, N)$, then $\overline{\epsilon} \in (1/N, 1)$.

We find that

$$\operatorname{tr}(\epsilon) = \epsilon + \overline{\epsilon} \in (1 + 1/N, N + 1).$$

But $t = \operatorname{tr}(\epsilon)$ is a rational integer, and we know there are only finitely many integers in a given bounded interval. We assumed that $N(\epsilon) = 1$, so ϵ has minimal polynomial $x^2 - tx + 1$. This assumes only finitely many values, and therefore there are only finitely many possible values of ϵ.

We can now say that there exists a unit $\epsilon > 1$ which is least for this property.

I claim that if α is another unit, then $\alpha = \pm\epsilon^n$ for some $n \in \mathbf{Z}$. WLOG assume that $\alpha > 1$. The powers $\epsilon, \epsilon^2, \epsilon^3, \ldots$ are unbounded. If α is not a power of ϵ, there exists n such that

$$\epsilon^n < \alpha < \epsilon^{n+1}.$$

Divide by ϵ^n to obtain

$$1 < \alpha\epsilon^{-n} < \epsilon.$$

This contradicts the minimality of ϵ as a unit greater than 1. ☐

What can we say about the structure of the unit group in general?

Example 5.2. *Let $K = \mathbf{Q}(\theta)$, where $\theta^3 = 2$. The ring of integers is $\mathcal{O}_K = \mathbf{Z}[\theta]$. What are the units $\mathbf{Z}[\theta]^\times$?*

We have

$$1 + \theta + \theta^2 = \frac{\theta^3 - 1}{\theta - 1} = \frac{1}{\theta - 1}$$

Thus $\theta - 1$ is a unit. In fact $\mathcal{O}_K^\times \cong \mathbf{Z}_2 \times \mathbf{Z}$, generated by -1 and $\theta - 1$.

Example 5.3. *Let $K = \mathbf{Q}(\theta)$, where $\theta^4 = 2$. We have*

$$1 + \theta + \theta^2 + \theta^3 = \frac{1}{\theta - 1},$$

and so $\theta - 1$ is a unit. But also K contains $\mathbf{Q}(\sqrt{2})$, since $\theta^2 = \sqrt{2}$. So the unit group of $\mathcal{O}_K$ must also contain $\theta^2 - 1 = \sqrt{2} - 1$. In fact, $\mathcal{O}_K^\times$ is generated by $-1, \theta - 1, \theta^2 - 1$. We have

$$\mathcal{O}_K^\times \cong \mathbf{Z}_2 \times \mathbf{Z} \times \mathbf{Z}.$$

Let $K/\mathbf{Q}$ be an algebraic number field. We must have $K = \mathbf{Q}(\alpha)$, where α is a root of an irreducible polynomial $f(x) \in \mathbf{Q}[x]$. This polynomial has some number of real roots, say r_1. The number of complex roots is even, say $2r_2$. We have $r_1 + 2r_2 = [K : \mathbf{Q}]$.

Theorem 5.4 (Dirichlet's unit theorem). *The group of units $\mathcal{O}_K^\times$ is a finitely generated abelian group. It is isomorphism to*

$$\mathcal{O}_K^\times \cong W \times \mathbf{Z}^{r_1+r_2-1},$$

where W is a finite cyclic group.

So for a real quadratic field, $r_1 = 2$, $r_2 = 0$, and $r_1 + r_2 - 1 = 1$.

But for $\mathbf{Q}(\sqrt[4]{2})$, we had $r_1 = 2$, $r_2 = 1$, so that $r_1 + r_2 - 1 = 2$.

Finding the group of units is a subtle matter.

Next we turn to the class number of an algebraic number field. Given an algebraic number field K, we might be interested in the structure of ideals of $\mathcal{O}_K$.

The best possible scenario is that $\mathcal{O}_K$ is a *principal ideal domain*, which means that every ideal is principal. It follows from this that element of $\mathcal{O}_K$ can be uniquely factored into irreducible elements, up to units.

The *class number* h of K is a positive integer measuring how far $\mathcal{O}_K$ is from being a principal ideal domain. If $h = 1$, then $\mathcal{O}_K$ is a PID.

Definition 5.5. *Let I and J be two nonzero ideals of $\mathcal{O}_K$. We say that I and J are* equivalent *if there exist $\alpha, \beta \in \mathcal{O}_K$ nonzero such that*

$$(\alpha)I = (\beta)J.$$

An ideal being equivalent to the unit ideal (1) just means that the ideal is principal.

Theorem 5.6. *The set of equivalence classes of nonzero ideals of $\mathcal{O}_K$ forms a group H_K under multiplication of ideals.*

For existence of inverses: Given a nonzero ideal I, you can find an integer $n \in I$ which is nonzero (think about norms). And then $(n) = IJ$ for some ideal J (there's a nontrivial result). Then the class of J is inverse to the class of I in H_K.

Theorem 5.7. *H_K is a finite abelian group.*

Let $h = \#H_K$ be its order, this is called the *class number* of K.

Open problem: Prove that there exist infinitely many algebraic number fields K with $h = 1$.

There are amazing analytic formulas for the class number, but often they involve the group of units as well.

For example, let $K = \mathbf{Q}(\sqrt{p})$, where $p \equiv 1 \pmod 4$ is a positive prime. There is a fundamental unit ϵ and a class number h.

Theorem 5.8 (Dirichlet's class number formula).

$$\epsilon^h = \prod_{a=1}^{(p-1)/2} \sin\left(\frac{2\pi a}{p}\right)^{-\left(\frac{a}{p}\right)}$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Exercise in Galois theory: prove that the right-hand side actually belongs to $\mathbf{Q}(\sqrt{p})$.

For instance if $p = 5$, the RHS is $(1 + \sqrt{5})/2$, the fundamental unit of $\mathbf{Q}(\sqrt{5})$.