Algebraic number theory **LTCC 2008**

Lecture notes, Part 2

5. The ideal class group

Let K be an algebraic number field and R_K the ring of integers of K. It is useful to generalise the notion of an ideal of R_K as follows.

Definition 5.1. A subset $A \subseteq K$ is called a *fractional ideal* of R_K if there exists $\gamma \in R_K \setminus \{0\}$ such that the set $\gamma A = \{\gamma\alpha : \alpha \in A\}$ is an ideal of R_K (so in particular $\gamma A \subseteq R_K$).

The product of two fractional ideals is defined in the same way as the product of two ideals. The product of two fractional ideals is again a fractional ideal. The following theorem generalises Theorem 4.7.

Theorem 5.2. *Let $I(K)$ be the set of non-zero fractional ideals of R_K. Then $I(K)$ is an abelian group with respect to multiplication of fractional ideals. Every fractional ideal $A \in I(K)$ can be expressed in the form $A = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$ where the P_i are distinct prime ideals of R_K and $e_i \in \mathbb{Z}$, and this representation is unique (more precisely it's unique up to the order of the factors and including factors with exponent zero).*

Proof. See for example [1, Theorems 2 and 3]. □

If $\alpha \in K$ then the set $(\alpha) := \{\lambda\alpha : \lambda \in R_K\}$ is a fractional ideal of R_K. It is called the *principal fractional ideal* generated by α. Let $P(K)$ denote the set of non-zero principal fractional ideals of R_K. We note that $(1) = R_K$, $(\alpha)^{-1} = (\alpha^{-1})$ and $(\alpha) \cdot (\beta) = (\alpha\beta)$, hence $P(K)$ is a subgroup of $I(K)$.

Definition 5.3. The *ideal class group* $\mathrm{Cl}(K)$ of an algebraic number field K is defined to be $\mathrm{Cl}(K) = I(K)/P(K)$.

Example 5.4. We want to compute $\mathrm{Cl}(\mathbb{Q})$. Let $A \in I(\mathbb{Q})$, i.e. A is a non-zero fractional ideal of $R_{\mathbb{Q}} = \mathbb{Z}$. Then there exists $\gamma \in \mathbb{Q} \setminus \{0\}$ such that γA is a non-zero ideal of $\mathbb{Z}$. By Lemma 4.5 there exists $\alpha \in \mathbb{Z}$ such that $\gamma A = (\alpha)$. Hence $A = \gamma^{-1}(\alpha) = (\gamma^{-1}\alpha)$ is a principal fractional ideal, i.e. $A \in P(\mathbb{Q})$. Therefore $I(\mathbb{Q}) = P(\mathbb{Q})$ which shows that the ideal class group $\mathrm{Cl}(\mathbb{Q}) = I(\mathbb{Q})/P(\mathbb{Q})$ is trivial.

Example 5.5. We now give an example of a non-principal ideal. Let $K = \mathbb{Q}(\sqrt{-6})$. By Lemma 3.6 we have $R_K = \mathbb{Z} + \mathbb{Z}\sqrt{-6}$. We will show that the ideal $A = (2, \sqrt{-6})$ of the ring R_K is not principal and that therefore the ideal class group $\mathrm{Cl}(K)$ is non-trivial.

First we define the norm $N\alpha$ of an element $\alpha \in K$ by $N\alpha = \alpha\tau(\alpha)$ where τ is the automorphism of K defined in Lemma 2.9. The norm satisfies $N(\alpha\beta) = N\alpha \cdot N\beta$ for all $\alpha, \beta \in K$ because we have (using that τ is an automorphism) $N(\alpha\beta) = \alpha\beta\tau(\alpha\beta) = \alpha\tau(\alpha) \cdot \beta\tau(\beta) = N\alpha \cdot N\beta$. If $\alpha = a + b\sqrt{-6}$ with $a, b \in \mathbb{Q}$ then

$$N\alpha = a^2 + 6b^2. \tag{1}$$

From this we see that $N\alpha \in \mathbb{N}$ if $\alpha \in R_K \setminus \{0\}$.

Now suppose for a contradiction that A is principal, so $A = (\alpha)$ for some $\alpha \in R_K$. Since $2 \in A$ we have $2 = \lambda\alpha$ for some $\lambda \in R_K$, and taking norms gives $N(2) = N\lambda \cdot N\alpha$, hence $N\alpha \mid N(2) = 4$. Similarly $\sqrt{-6} \in A$ implies $N\alpha \mid N(\sqrt{-6}) = 6$. It follows that $N\alpha = 1$ or $N\alpha = 2$. Equation (1) shows that the case $N\alpha = 2$ is impossible. In the case $N\alpha = 1$ equation (1) shows that $\alpha = \pm 1$ and therefore $1 \in (\alpha) = A = (2, \sqrt{-6})$. But then there exist $a, b, c, d \in \mathbb{Z}$ such that $1 = (a +$

$b\sqrt{-6})\cdot 2+(c+d\sqrt{-6})\cdot\sqrt{-6}=(2a-6d)+(2b+c)\sqrt{-6}$ which implies $1=2a-6d$. As this is impossible, it follows that the case $N\alpha=1$ is also impossible. Hence the ideal A is not principal.

Theorem 5.6. *Let K be an algebraic number field. Then the ideal class group $\mathrm{Cl}(K)$ is finite.*

Proof. See for example [1, Theorem 31, p. 155]. □

Definition 5.7. Let K be an algebraic number field. The *class number* h_K of K is defined to be the order of the ideal class group of K, i.e. $h_K=|\mathrm{Cl}(K)|$.

6. Units

We first recall the definition of a unit of a commutative ring.

Definition 6.1. Let R be a commutative ring. An element $\alpha\in R$ is called a *unit* if there exists a $\beta\in R$ such that $\alpha\beta=1$. The set of units of R is denoted by $R^\times$.

Lemma 6.2. *Let R be a commutative ring. Then $R^\times$ is an abelian group (with respect to multiplication).*

Proof. Clear. □

Now let K be an algebraic number field. We want to determine the structure of the group $R_K^\times$. First we consider the torsion subgroup of $R_K^\times$, i.e. the subgroup consisting of all elements of finite order. A *root of unity* in K is an element $\zeta\in K$ such that $\zeta^e=1$ for some $e\in\mathbb{N}$. We let μ_K denote the set of roots of unity in K,

$$\mu_K=\{\zeta\in K:\zeta^e=1\text{ for some }e\in\mathbb{N}\}.$$

It is easy to see that μ_K is a group with respect to multiplication.

Lemma 6.3. *Let K be an algebraic number field. The torsion subgroup of $R_K^\times$ is equal to the group μ_K of roots of unity in K. Furthermore μ_K is a finite cyclic group.*

Proof. If α is a torsion element in $R_K^\times$, then $\alpha^e=1$ for some $e\in\mathbb{N}$, so α is a root of unity in K. Conversely if $\alpha\in\mu_K$, then $\alpha\in R_K$ (because α satisfies a polynomial equation of the form $X^e-1=0$ for some $e\in\mathbb{N}$), and $\alpha^e=1$ implies that α is a unit (with inverse α^{e-1}) and has finite order.

Next we show that the group μ_K is finite. Assume for a contradiction that μ_K is infinite. Then μ_K must contain elements of arbitrary large order because for every $e\in\mathbb{N}$ the equation $X^e=1$ has at most e solutions in the field K. Now if $\zeta\in\mu_K$ then $\mathbb{Q}(\zeta)\subseteq K$ and therefore $[K:\mathbb{Q}]\geq[\mathbb{Q}(\zeta):\mathbb{Q}]$. However one can show that if ζ is a root of unity of order e then $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(e)$ where φ denotes Euler's φ-function (see for example [2, VI, Theorem 3.1]). But $\varphi(e)\to\infty$ as $e\to\infty$, therefore $[K:\mathbb{Q}]=\infty$ which contradicts the definition of an algebraic number field.

Finally the cyclicity of the group μ_K follows from the general fact that any finite subgroup of $K^\times$ is cyclic (this is true for any field K and not only for algebraic number fields, see for example [2, IV, Theorem 1.9]). □

Example 6.4. If $m>1$ is square-free and $K=\mathbb{Q}(\sqrt{m})$ (so K is a real quadratic field) then $\mu_K=\{1,-1\}$. Here the inclusion $\mu_K\supseteq\{1,-1\}$ is obvious. Conversely if $\zeta\in\mu_K$ then we can consider ζ as an element of $\mathbb{R}^\times$ because $K\subset\mathbb{R}$ (where $\mathbb{R}$ denotes the field of real numbers). But the only elements of finite order in $\mathbb{R}^\times$ are 1 and -1, hence $\zeta\in\{1,-1\}$ as claimed.

Example 6.5. If $K=\mathbb{Q}(\sqrt{-1})$ then $\mu_K=\{1,-1,\sqrt{-1},-\sqrt{-1}\}$. Here the inclusion $\mu_K\supseteq\{1,-1,\sqrt{-1},-\sqrt{-1}\}$ is clear; the inclusion $\mu_K\subseteq\{1,-1,\sqrt{-1},-\sqrt{-1}\}$ is left as an exercise.

The next aim is to determine the structure of the torsion free group $R_K^\times/\mu_K$. For this we must consider embeddings σ of K into $\mathbb{C}$, i.e. injective homomorphisms $\sigma : K \to \mathbb{C}$.

Lemma 6.6. *Let K be an algebraic number field of degree n over $\mathbb{Q}$. Then there exist precisely n distinct embeddings of K into $\mathbb{C}$.*

Sketch of proof. There exists an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. This element α satisfies an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n. In the field $\mathbb{C}$ the polynomial $f(x)$ has n distinct roots $r_1, \dots, r_n \in \mathbb{C}$. Then for each $i = 1, \dots, n$ there exists a unique homomorphism $K \to \mathbb{C}$ which sends α to r_i. $\square$

Let $\sigma : K \to \mathbb{C}$ be an embedding. If $\sigma(K) \subseteq \mathbb{R}$ we call σ a *real embedding*, otherwise we call σ a *complex embedding*. We let r be the number of real embeddings of K and $\sigma_1, \dots, \sigma_r$ the list of real embeddings. Complex embeddings come in pairs, because if $\sigma : K \to \mathbb{C}$ is a complex embedding then the map $\overline{\sigma}$ which is defined by $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ (i.e. the complex conjugate of $\sigma(\alpha)$) is again a complex embedding different from σ. So in particular the number of complex embeddings is even. We let $2s$ be the number of complex embeddings of K and $\sigma_{r+1}, \dots, \sigma_{r+s}, \sigma_{r+s+1} = \overline{\sigma_{r+1}}, \dots, \sigma_{r+2s} = \overline{\sigma_{r+s}}$ the list of complex embeddings. By Lemma 6.6 the total number of embeddings is equal to the degree of K over $\mathbb{Q}$, so

$$r + 2s = [K : \mathbb{Q}].$$

Lemma 6.7. *Let K be an algebraic number field of degree n over $\mathbb{Q}$, and let $\sigma_1, \dots, \sigma_n$ be the list of embeddings of K into $\mathbb{C}$. Then for every positive real number B the set*

$$\{\alpha \in R_K : |\sigma_i(\alpha)| \leq B \textit{ for all } i = 1, \dots n\}$$

is finite.

Sketch of proof. Let $\alpha \in R_K$ be such that $|\sigma_i(\alpha)| \leq B$ for all $i = 1, \dots n$. We define a polynomial $f(X) \in \mathbb{C}[X]$ by $f(X) = \prod_{i=1}^n (X - \sigma_i(\alpha))$. Then the coefficients of $f(X)$ are symmetric functions in $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$. This implies that the coefficients are rational numbers (this follows easily from Galois theory) and integral over $\mathbb{Z}$ (because $\alpha \in R_K$ implies that all $\sigma_i(\alpha)$ are integral over $\mathbb{Z}$), hence by Lemma 3.3 they are integers. Furthermore since all $|\sigma_i(\alpha)|$ are bounded by B it follows that all coefficients of $f(X)$ are bounded by a constant depending on B (but independent of α). It is also easy to see that α is a root of $f(X)$.

We have shown that α is a root of a polynomial of degree n with bounded integer coefficients. As there are only finitely many such polynomials and each such polynomial has only finitely many roots, it follows that there are only finitely many α in the set. $\square$

Define a map $\lambda : R_K^\times \to \mathbb{R}^{r+s}$ by

$$\lambda(x) = \big(\log|\sigma_1(x)|, \dots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \dots, 2\log|\sigma_{r+s}(x)|\big).$$

Since $\log|\sigma_i(xy)| = \log|\sigma_i(x)| + \log|\sigma_i(y)|$ for all $x, y \in R_K^\times$ and all $i = 1, \dots, r+s$, the map λ is a homomorphism from the multiplicative group $R_K^\times$ to the additive group $\mathbb{R}^{r+s}$.

Lemma 6.8. $\ker(\lambda) = \mu_K$

Proof. If $\zeta \in \mu_K$ then $\zeta^e = 1$ for some $e \in \mathbb{N}$. It follows that $e \cdot \lambda(\zeta) = \lambda(\zeta^e) = \lambda(1) = (0, \dots, 0)$, hence $\lambda(\zeta) = (0, \dots, 0)$, i.e. $\zeta \in \ker(\lambda)$.

Conversely, if $\zeta \in \ker(\lambda)$ then $\log|\sigma_i(\zeta)| = 0$ and thus $|\sigma_i(\zeta)| = 1$ for all $i = 1, \dots, r+s$. This implies that $|\sigma_i(\zeta)| = 1$ also for $i = r+s+1, \dots, r+2s$ because $|\sigma_{r+s+1}(\zeta)| = |\overline{\sigma_{r+1}(\zeta)}| = |\sigma_{r+1}(\zeta)| = 1$ etc. The same argument applies to all powers ζ^i. This shows that all ζ^i for $i \in \mathbb{Z}$ lie in the finite set of Lemma 6.7 (with

$B = 1$). Hence there exist integers $i < j$ such that $\zeta^i = \zeta^j$, i.e. $\zeta^{j-i} = 1$. Thus $\zeta \in \mu_K$ as claimed. $\square$

It follows from Lemma 6.8 that $R_K^\times/\mu_K$ is isomorphic to the image of λ. The next lemma will be used to show that the image of λ lies in the hyperplane

$$H = \{(x_1, \ldots, x_{r+s}) \in \mathbb{R}^{r+s} : x_1 + \cdots + x_{r+s} = 0\}.$$

Lemma 6.9. *Let $\alpha \in R_K$. Then α is a unit if and only if the product*

$$N(\alpha) := \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_{r+2s}(\alpha)$$

is equal to 1 *or* -1.

Sketch of proof. Let $\alpha \in R_K^\times$. Since $\alpha \in R_K$ the $\sigma_i(\alpha)$ are integral over $\mathbb{Z}$ for all i. Hence the product $N(\alpha) = \sigma_1(\alpha)\cdots\sigma_{r+2s}(\alpha)$ is integral over $\mathbb{Z}$. But using Galois theory it is easy to see that $N(\alpha)$ lies in $\mathbb{Q}$, therefore $N(\alpha) \in \mathbb{Z}$. Similarly $N(\alpha^{-1}) := \sigma_1(\alpha^{-1})\cdots\sigma_{r+2s}(\alpha^{-1}) \in \mathbb{Z}$ because $\alpha^{-1} \in R_K$. But clearly $N(\alpha)\cdot N(\alpha^{-1}) = 1$, hence $N(\alpha) = \pm 1$ as claimed.

Conversely, if $\sigma_1(\alpha)\cdots\sigma_{r+2s}(\alpha) = \pm 1$ then $\pm\sigma_1^{-1}\big(\sigma_2(\alpha)\cdots\sigma_{r+2s}(\alpha)\big)$ is an inverse of α in R_K, and thus α is a unit. $\square$

Lemma 6.10. *The image of λ is a full lattice in $H \subset \mathbb{R}^{r+s}$, i.e. $\lambda(R_K^\times)$ is a discrete subgroup of H with rank equal to the dimension of H.*

Proof. Let $\alpha \in R_K^\times$. Then

$$\lambda(\alpha) = \big(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \ldots, 2\log|\sigma_{r+s}(\alpha)|\big).$$

Now for $1 \le i \le s$ we have $2\log|\sigma_{r+i}(\alpha)| = \log|\sigma_{r+i}(\alpha)| + \log|\sigma_{r+s+i}(\alpha)|$, hence

$$\begin{aligned}
\log|\sigma_1(\alpha)| + \cdots + \log|\sigma_r(\alpha)| + 2\log|\sigma_{r+1}(\alpha)| &+ \cdots + 2\log|\sigma_{r+s}(\alpha)| \\
&= \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_{r+2s}(\alpha)| \\
&= \log\big|\sigma_1(\alpha)\cdots\sigma_{r+2s}(\alpha)\big| \\
&= \log|\pm 1| \\
&= 0.
\end{aligned}$$

This shows that $\lambda(R_K^\times) \subseteq H$.

If W is any bounded region of H and $\alpha \in R_K^\times$ is such that $\lambda(\alpha) \in W$ then $\log|\sigma_i(\alpha)|$ is bounded for $i = 1, \ldots, r+s$. It follows that $|\sigma_i(\alpha)|$ is bounded for all $i = 1, \ldots, r+2s$ and Lemma 6.7 therefore implies that α must lie in a finite set. This shows that $\lambda(R_K^\times) \cap W$ is finite. Hence $\lambda(R_K^\times)$ is a discrete subgroup of H.

The most difficult step is to show that $\lambda(R_K^\times)$ has rank equal to $\dim_{\mathbb{R}} H = r+s-1$. This requires constructing $r+s-1$ many units in R_K such that their images under λ are linearly independent over $\mathbb{R}$. For details see for example [1, IV.(4.7)]. $\square$

We have a short exact sequence of abelian groups

$$\{1\} \longrightarrow \ker(\lambda) \longrightarrow R_K^\times \xrightarrow{\lambda} \lambda(R_K^\times) \longrightarrow 0.$$

By Lemma 6.10 we know that $\lambda(R_K^\times)$ is a full lattice in the $(r+s-1)$-dimensional vector space H. Therefore $\lambda(R_K^\times) \cong \mathbb{Z}^{r+s-1}$, so in particular the short exact sequence splits (non-canonically), i.e. there exists an isomorphism

$$R_K^\times \cong \ker(\lambda) \times \lambda(R_K^\times).$$

We also know that $\ker(\lambda) = \mu_K$ by Lemma 6.8. Hence we obtain the following theorem.

Theorem 6.11 (Dirichlet's unit theorem)**.** *Let K be an algebraic number field. Let r be the number of real embeddings $K \to \mathbb{R}$ and let $2s$ be the number of complex embeddings $K \to \mathbb{C}$. Then $R_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$.*

Units $\alpha_1, \ldots, \alpha_{r+s-1} \in R_K^\times$ with the property that $\lambda(\alpha_1), \ldots, \lambda(\alpha_{r+s-1})$ are a $\mathbb{Z}$-basis of the lattice $\lambda(R_K^\times)$ are called a system of *fundamental units* for $R_K^\times$. If ζ is a generator of the cyclic group μ_K and $\alpha_1, \ldots, \alpha_{r+s-1}$ is a system of fundamental units for $R_K^\times$, then every unit can be expressed uniquely in the form $\zeta^i \alpha_1^{e_1} \cdots \alpha_{r+s-1}^{e_{r+s-1}}$ where $0 \le i < |\mu_K|$ and $e_1, \ldots, e_{r+s-1} \in \mathbb{Z}$.

Definition 6.12. Let K be an algebraic number field and let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K and $\sigma_{r+1}, \ldots, \sigma_{r+s}$ half of the complex embeddings of K as above. Let $\alpha_1, \ldots, \alpha_{r+s-1}$ be a system of fundamental units of $R_K^\times$. Then the *regulator* $\mathrm{Reg}_K \in \mathbb{R}$ of K is defined to be the absolute value of any $(r+s-1)\times(r+s-1)$-minor of the matrix

$$\begin{pmatrix} \log|\sigma_1(\alpha_1)| & \ldots & \log|\sigma_1(\alpha_{r+s-1})| \\ \vdots & & \vdots \\ \log|\sigma_r(\alpha_1)| & \ldots & \log|\sigma_r(\alpha_{r+s-1})| \\ 2\log|\sigma_{r+1}(\alpha_1)| & \ldots & 2\log|\sigma_{r+1}(\alpha_{r+s-1})| \\ \vdots & & \vdots \\ 2\log|\sigma_{r+s}(\alpha_1)| & \ldots & 2\log|\sigma_{r+s}(\alpha_{r+s-1})| \end{pmatrix}.$$

This definition does not depend on any of the choices.

Example 6.13. Let $m > 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{m})$. Then the field K has two real embeddings (given by $\sigma_1(a + b\sqrt{m}) = a + b\sqrt{m}$ and $\sigma_2(a + b\sqrt{m}) = a - b\sqrt{m}$) and no complex embeddings, so $r = 2$, $s = 0$. Since $\mu_K = \{1, -1\}$ (by Example 6.4) it follows from Dirichlet's unit theorem that $R_K^\times \cong \{1, -1\} \times \mathbb{Z}$. If $\alpha \in R_K^\times$ is a fundamental unit then the regulator of K is the absolute value of any 1×1-minor of the matrix

$$\begin{pmatrix} \log|\sigma_1(\alpha)| \\ \log|\sigma_2(\alpha)| \end{pmatrix},$$

hence $\mathrm{Reg}_K = \big|\log|\sigma_1(\alpha)|\big| = \big|\log|\sigma_2(\alpha)|\big|$.

To give an explicit example, we consider $K = \mathbb{Q}(\sqrt{2})$. Then one can show that $\alpha = 1 + \sqrt{2}$ is a fundamental unit of K (it is clear that α is a unit because $\alpha^{-1} = -1 + \sqrt{2} \in R_K$, but to see that α is in fact a fundamental unit requires some additional arguments). Hence $\mathrm{Reg}_K = \big|\log|\sigma_1(\alpha)|\big| = \big|\log(1 + \sqrt{2})\big| = 0.88137\ldots$.

References

[1] A. Fröhlich, M.J. Taylor, *Algebraic number theory*, CUP, 1991.
[2] S. Lang, *Algebra*, 3rd edition, Springer, 2002.