## 8. Algebraic numbers: The class group and the class number

**Theorem 8.29** *Let $D$ be Dedekind ring. Unique factorization into irreducibles holds in $D$ if and only if every ideal of $D$ is principal.*

For the proof we will need one simple statement which we formulate as an exercise.

**Exercise 8.15** Let $D$ be a Dedekind ring which is a unique factorisation domain. Then for every irreducible $p \in D$ the principal ideal $(p)$ is prime and hence maximal.

**Proof of Theorem 8.29** If $D$ is principal ideal domain, then we know it has unique factorisation property. Suppose factorisation in $D$ is unique. We need to show that every ideal $I$ in $D$ is principal. Since every ideal is a product of prime ideals, it is sufficient to prove this when $I$ is prime, hence maximal. The quotient ring $D/I$ is a finite field. Let $q$ be the characteristic of this field, then $qa = 0$ for every $a$ in this quotient, which means that $qx \in I$ for all $x \in D$. In particular, $q = q \cdot 1 \in I$. As we know $q$ is prime in $\mathbb{Z}$ but in $D$ it may have a non-trivial factorisation

$$q = p_1 \cdots p_m,$$

where $p_i$'s are primes in $D$. We have $(q) = (p_1) \dots (p_m)$ and by Exercise 8.15 each ideal $(p_i)$ is maximal. By Theorem 8.28 $I|(p_j)$ for some $j$ which forces $I = (p_j)$ since both are maximal. Hence $I$ is principal. □

---

The following definition plays a major role in algebraic number theory. Two ideals $I, J \subset D$ of $F$ are *equivalent*, $I \sim J$, if there exist nonzero $\alpha, \beta \in D$ such that $(\alpha)I = (\beta)J$.

**Exercise 8.16** *Let $[I]$ denotes the equivalence class of the ideal $I$. Show that for every principal ideal $I$ of $D$ we have $I = [D]$.* □

The equivalence classes are called *ideal classes* of $D$. The *class number* $h_F$ of the field $F$ is the number of ideal classes in $D$. The *class number* of the field is a measure of non-uniqueness of its prime factorisation.

**Lemma 8.30** *We have $h_F = 1$ if and only if $D$ is a principal ideal domain (and hence a unique factorisation domain).*

**Proof.** Let $h_F = 1$ and let $J$ be an ideal. Since $J \sim D$, we have $(\alpha)J = (\beta)D = (\beta)$ for non-zero $\alpha, \beta \in D$, which implies that $\beta/\alpha \in D$ and $J = (\beta/\alpha)$. The converse is easy. □

Ideal classes can be multiplied: if $[I]$ denotes the equivalence class of the ideal $I$, then the multiplication $[I][J] = [IJ]$ is well-defined and commutative.

**Theorem 8.31** *The ideal classes of $D$ form a group $C_F$, which is called the ideal class group of $F$.*

**Proof.** The class $[D]$ which consists of principal ideals is obviously the identity element of this group: $[I][D] = [ID] = [I]$. All we need to show is that every ideal class $[I]$ has an inverse. Let us take an arbitrary $a \in I$ and consider the prime ideal factorisation of the principal ideal $(a)$:

$$(a) = \pi_1 \cdots \pi_r.$$

Since $I$ divides $(a)$ and the factorisation is unique, we will have (wolog) $I = \pi_1 \cdots \pi_s$. Then $J = \pi_{s+1} \cdots \pi_r$ and $[J]$ will be the inverse of $[I]$. □

One of the main results of classical algebraic number theory states

**Theorem 8.32** *The class number of an algebraic number field is finite.* □

We will not prove this theorem here. We end the topic with an example of a non-trivial class group.

**Example 8.33** Since $-5 \not\equiv 1 (\text{mod } 4)$ the ring $D = \mathbb{Z}[\sqrt{-5}]$ is the ring of integers of $\mathbb{Q}(\sqrt{-5})$. It does not possess unique factorisation; in fact the class group $C_F$ is cyclic of order 2. Indeed, the ideal $J = (2, 1 + \sqrt{-5})$ is not principal, which can be proved by contradiction as follows. If $J$ were generated by an element $x$ of $D$, then $x$ would divide both 2 and $1 + \sqrt{-5}$. Then the norm $N(x)$ of $x$ would divide both $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, so $N(x)$ would divide 2. We are assuming that $x$ is not a unit of $D$, so $N(x)$ cannot be 1. It cannot be 2 either, because $D$ has no elements of norm 2 because the equation $b^2 + 5c^2 = 2$ has no solutions in integers. One also computes that $J^2 = (2)$, which is principal, so the class of $J$ in the ideal class group has order two. Showing that there aren't any other ideal classes requires more effort. The fact that this $J$ is not principal is also related to the fact that the element 6 has two distinct factorisations into primes: $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

For $d < 0$, where $d$ is square-free, the only quadratic fields $\mathbb{Q}(\sqrt{d})$ with class number 1 are those for $-d = 1, 2, 3, 7, 11, 18, 43, 67, 163$. Gauss conjectured that for $d > 0$ there are infinitely many such fields but this is still unproven.

**Exercise 8.17** *Let $D$ be a Dedekind ring. Prove the following cancellation property for the ideals of $D$: if $I, J, H$ are any three ideals of $D$ satisfying $IH = JH$, then $I = J$.*

**Exercise 8.18** *Let $D$ be a Dedekind ring and $I$ be an ideal of $D$. Prove that $I^k$ is principal for some positive integer $k$.*

**Exercise 8.19** *If $I \subset J \subset D$ are ideals, then there is an ideal $K \subset D$ such that $I = JK$.*