IDEALS, PART I

In these notes we discuss some theorems from the theory of ideals, several of which are not covered in detail in the texts.

Throughout, let d be a squarefree integer, let $K = \mathbb{Q}(\sqrt{d})$, and let R be the ring of algebraic integers of K. As we have noted, the ring of integers R can be described explicitly as follows:

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \mod 4 \end{cases}$$

Definition 1 *If $d \equiv 2,3 \mod 4$ let $d_K = 4d$. If $d \equiv 1 \mod 4$ let $d_K = d$. We call d_K the discriminant of K.*

The ring of algebraic integers R can also be written in the form:

$$R = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right].$$

Note that when $d_K = 4d$, this is simply equal to $Z[\sqrt{d}]$.

Definition 2 *An Ideal I of R is a subset of R with the following properties:*

1. *If a, $b \in I$, then $a + b \in I$.*
2. *If $a \in I$ and $r \in R$, then $ra \in R$.*

For example, $I = \{0\}$ is an ideal, and $I = R$ is also an ideal. If $\alpha \in R$, then the set

$$(\alpha) = \{r\alpha | r \in R\}.$$

is an ideal generated by a single element. We call such an ideal a *principal* ideal. If the elements α_1, $\alpha_2 \ldots \alpha_n \in R$ then we can form the ideal

$$I = (\alpha_1, \ldots, \alpha_n) = \{r_1\alpha_1 + \ldots r_n\alpha_n | r_i \in R\}.$$

One can prove that for the rings R we are considering (and more generally for the ring of integers of any number field), any ideal can be generated by at most two elements.

Definition 3 *Let I and J be two ideals in R. We define the product IJ to be the ideal generated by all elements of the form ab, with $a \in I$ and $b \in J$.*

Note that if $a, a' \in I$ and $b, b' \in J$, then $ab + a'b' \in IJ$, and this element can not necessarily be written as an element of I times an element of J.

Definition 4 *An ideal I of R is prime if $I \neq R$ and if the following property is satisfied: for all a, $b \in R$ such that $ab \in I$, either $a \in I$ or $b \in I$.*

Example. All ideals of $R = \mathbb{Z}$ are principal. Equivalently, any ideal of R is equal to one of the form $I = (m)$. This follows from the following result: the ideal $I = (m_1, m_2, \ldots m_k)$ is equal to (m), where m is the gcd of $m_1, \ldots m_k$. The product of two ideals $I = (n)$ and $J = (m)$ is $IJ = (nm)$. The prime ideals are the principal ideals $I = (p)$ when p prime, and the ideal $I = (0)$ (exercise: check this is prime).

Theorem 0.1 *Let I be a non-zero proper ideal of R (so I is neither (0) or R). Then I can be uniquely factored into prime ideals.*

This theorem generalizes the classical theorem that positive integers can be uniquely factored into prime numbers. The following example shows why we need to talk about ideals at all:
Example. Let $d = -5$. We see that $d_K = -20$, and $R = \mathbb{Z}[\sqrt{-5}]$. Suppose we tried to factor the number "6". Note that

$$6 = (1 + \sqrt{-5}) \times (1 - \sqrt{-5}) = 2 \times 3.$$

Suppose that R had unique factorization. Let p be a prime divisor of 6. One property that primes have is the following: if $p|ab$ then $p|a$ or $p|b$. Thus $p|2$ or $p|3$, and $p|1 + \sqrt{-5}$ or $p|1 - \sqrt{-5}$. There are various cases to consider, but they are similar. Suppose that $p|2$ and $p|1 + \sqrt{-5}$. Taking norms (if $p|\alpha$ then $p\overline{p}|\alpha\overline{\alpha} = N(\alpha)$) we see that $N(p)|N(2) = 4$ and $N(p)|N(1 + \sqrt{-5}) = 6$. Thus $N(p)|2$, and hence $N(p) = \pm 1$ or ± 2. Yet if $p = x + y\sqrt{-5}$ then $N(p) = x^2 + 5y^2$, and thus $p = \pm 1$. Clearly this is not a prime, so R does not have unique factorization. One should think of this example as follows. The numbers 2 and $(1 + \sqrt{-5})$ have no common factor, but "morally" they should both be divisible by a common prime. The solution is to take the ideal $I = (2, 1 + \sqrt{-5})$. This ideal is not principal, but it plays the role of the gcd of 2 and $(1 + \sqrt{-5})$. One can show easily that $I^2 = (2)$. If $J = (3, 1 + \sqrt{-5})$ and $J' = (3, 1 - \sqrt{-5})$ then $JJ' = (3)$, and $6 = I^2JJ'$.

Here are some more constructions with ideals.

Definition 5 *The norm of an ideal $N(I)$ is equal to the greatest common divisor of the norms of every element of I.*

Note that if I is principal, then $I = (\alpha)$. Since every element if I is divisible by α, the norm of every element of I is divisible by $N(\alpha)$. However, the norm if I is by definition positive, and $N(\alpha)$ can be negative, thus $N(I) = |N(\alpha)|$.

Theorem 0.2 *If I and J are two ideals, then $N(IJ) = N(I)N(J)$.*

Exercise. If I is a prime ideal, then $N(I) = p^k$, where p is a prime number. (Hint: first prove that the integer $N(I)$ actually lies inside I. Then if $N(I) = ab$ use the fact that $a \in I$ or $b \in I$.

Definition 6 *Let R be the ring of integers of a quadratic number field. For any ideal I, we define the conjugate ideal $\overline{I}$ as follows:*

$$\overline{I} = \{\overline{\alpha} | \alpha \in I\}.$$

(recall that α is the conjugate of α).

Thus for example if $I = (\alpha)$, then $\overline{I} = (\overline{\alpha})$. A useful result is the following:

Lemma 0.1 *If $N(I) = m$, then $I\overline{I} = (m)$.*

Proof. If $I = (\alpha)$ is principal, this is easy to see, since $\alpha\overline{\alpha} = N(\alpha)$. To prove the result in general we show that $(m) \subseteq I\overline{I}$ and $II \subseteq (m)$. First we prove that $(m) \subseteq I\overline{I}$. The ideal $I\overline{I}$ contains the norms of every element of I. These norms are integers, and their gcd is by definition equal to $N(I) = m$; moreover we can write m as a linear combination of these integers. Thus $m \in I\overline{I}$. Now we show that $I\overline{I} \subseteq (m)$. Elements of $I\overline{I}$ are sums of elements of the form $\alpha\overline{\beta}$, where α, $\beta \in I$. Thus if we prove that $\alpha\overline{\beta}$ is a multiple of m, it will follow that any element of $I\overline{I}$ is a multiple of m, and we will be done. let $\alpha, \beta \in I$. Let $\gamma = \alpha\overline{\beta}$. Since norms of elements of I are divisible by m, the numbers $N(\alpha)$, $N(\beta)$ and $N(\alpha + \beta)$ are divisible by m. Thus so is

$$(\alpha + \beta)(\overline{\alpha} + \overline{\beta}) - \alpha\overline{\alpha} - \beta\overline{\beta} = \alpha\overline{\beta} + \overline{\alpha}\beta = \gamma + \overline{\gamma}.$$

In particular, if $\gamma = \alpha\overline{\beta}$, then $m|\text{Trace}(\gamma)$. Moreover,

$$N(\gamma) = \gamma\overline{\gamma} = N(\alpha)N(\beta)$$

is divisible by m^2. Thus γ satisfies a quadratic equation of the form

$$x^2 + amx + bm^2 = 0,$$

where a, b are integers. If $\gamma' := \gamma/m$, then γ' satisfies the quadratic equation $x^2 + ax + b = 0$. This equation also has integral coefficients, and therefore γ' is an algebraic integer, and so lies in R. Thus $\gamma = m\gamma'$ is a multiple of m, and $I\overline{I} = (m)$.

Definition 7 *We form an equivalence relation on ideals as follows. Let $I \sim J$ if there exist α, $\beta \in R$ such that $(\alpha)I = (\beta)J$ and $N(\alpha\beta) > 0$. We call the set of ideals modulo this relation the narrow class group. If we relax the condition that $N(\alpha\beta) > 0$, we get the class group.*

Let us explain why the class group is actually a group. The zero element in the class group is the set of principal ideals. The zero element in the narrow class group is the set of principal ideals (α) with $N(\alpha) > 0$. It is clear how to multiply ideals, and it is clear that if $I \simeq J$ and $I' \simeq J'$, then $II' \simeq JJ'$. Thus it suffices to show why inverses exist. Given an ideal I, we must find an ideal J such that IJ is principal. From the lemma above we may take $J = \overline{I}$, since $I\overline{I} = (N(I))$ is principal. Thus the class of $\overline{I}$ is inverse to I in the class group (and the ideal class group, since $N(m) = m^2 > 0$. A major result in algebraic number theory is the following: I. We have the following:

Theorem 0.3 *The Class group (denoted* $\mathrm{Cl}(K)$*) and the Narrow Class group* $\mathrm{Cl}^+(K)$ *are finite abelian groups.*

Relevant to our discussion of binary quadratic forms is the following.

Theorem 0.4 *There is a one to one correspondence between elements of the Narrow class group of* K *and classes of binary quadratic forms of discriminant* d_K*.*

If $d_K < 0$, then the narrow class group is equal to the class group. Moreover, since the number of reduced binary quadratic forms of discriminant d_K is finite, this provides another proof of the finiteness of the class group in this case.