IDEALS, PART II

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.

Let $I \subseteq R$ be an ideal. If we forget about multiplication and only remember how to add elements of R, then I and R can be considered as abelian groups. As an abelian group, the ring R is isomorphic to the free abelian group on two generators, or $\mathbb{Z}^2$. Generators for R can be given by 1 and $(d_K + \sqrt{d_K})/2$. Since $I \subseteq R$, I is a subgroup of $\mathbb{Z}^2$. Up to isomorphism, the only subgroups of $\mathbb{Z}^2$ are the trivial group, free groups on one generator, (which are isomorphic to $\mathbb{Z}^1$) and free groups on two generators, which are isomorphic to $\mathbb{Z}^2$. Suppose that $I = \mathbb{Z}^1$. Then I would be generated by a single element α, and every element in I would be of the form $n\alpha$, with $n \in \mathbb{Z}$. Since ideals are closed under multiplication by elements of R, however, we see that $\sqrt{d}\alpha \in I$. Thus I cannot be isomorphic to $\mathbb{Z}^1$. We see that I always contains $0 \in R$. Then either $I = (0)$, or I is abstractly isomorphic to $\mathbb{Z}^2$, and can thus be generated by two elements α, β.

Definition 1 *If I is generated as an abelian group by α and β, we write $I = [\alpha, \beta]$. If $I = [\alpha, \beta]$, then all elements of I can uniquely be written in the form $\alpha x + \beta y$, with $x, y \in \mathbb{Z}$.*

If one can write $I = (\alpha, \beta)$ as an ideal, it does not necessarily follow that $I = [\alpha, \beta]$. For example, if $I = (2 + \sqrt{-1}, 2 - \sqrt{-1})$, then $I = \mathbb{Z}[\sqrt{-1}]$ is the trivial ideal. However, 1 cannot be written as an integer combination of $2 + \sqrt{-1}$ and $2 - \sqrt{-1}$ since the integral part of any such sum is even.

Definition 2 *If $I = [\alpha, \beta]$ we say that the pair (α, β) is correctly ordered if*

$$\frac{\alpha\overline{\beta} - \overline{\alpha}\beta}{\sqrt{d}} > 0.$$

If (α, β) is not correctly ordered, then (β, α) is.

We can now describe the correspondence between ideal classes and binary quadratic forms. Let $I = [\alpha, \beta]$ be an ideal, and suppose that (α, β) is correctly ordered. Then the binary quadratic form associated to $[\alpha, \beta]$ is

$$\frac{N(\alpha x + \beta y)}{N(I)} = \frac{\alpha\overline{\alpha}x^2 + (\alpha\overline{\beta} + \overline{\alpha}\beta)xy + \beta\overline{\beta}y^2}{N(I)}.$$

since $I\overline{I} = (N(I))$ (see the last set of notes), we see that the coefficients of this modular form have integral coefficients. Denote this binary quadratic form by $f([\alpha, \beta])$.
The binary quadratic form $f([\alpha, \beta])$ depends on our choice of basis for I. However, we are only really interested in the *class* of the quadratic form f.

Lemma 0.1 *Let $[f(I)] = [f([\alpha, \beta])]$ denote the class of the binary quadratic form $f([\alpha, \beta])$. Then $[f(I)]$ only depends on I.*

If $[\gamma, \delta]$ is another basis for I, then

$$\gamma = a\alpha + b\gamma, \qquad \delta = c\alpha + d\delta.$$

Moreover, α and β can themselves be written as a linear combination of γ and δ. It follows that

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is an invertible matrix, and thus $M \in \mathrm{GL}_2(\mathbb{Z})$. If γ and δ are also correctly ordered, then M actually has determinant 1, and $M \in \mathrm{SL}_2(\mathbb{Z})$. Since

$$N(\gamma x + \delta y) = N((a\alpha + b\gamma)x + (c\alpha + d\delta)y) = N((ax + by)\alpha + (cx + dy)\delta),$$

we see that $f([\gamma, \delta]) = M \circ f([\alpha, \beta])$ and thus $[f(I)]$ is well defined.

Lemma 0.2 *If $I \sim J$ in the Narrow class group, then $[f(I)] = [f(J)]$.*

It suffices to prove that if $J = (\gamma)I$ with $N(\gamma) > 0$, then $[f(J)] = [f(I)]$. Let $I = [\alpha, \beta]$, with (α, β) correctly ordered. We find that $J = [\gamma\alpha, \gamma\beta]$, $N(J) = N(\gamma)N(I)$, and

$$f(J) = \frac{\gamma\alpha\overline{\gamma\alpha}x^2 + (\gamma\alpha\overline{\gamma}\overline{\beta} + \overline{\gamma\alpha}\gamma\beta)xy + \gamma\beta\overline{\gamma}\overline{\beta}y^2}{N(\gamma)N(I)} = f([\alpha, \beta]).$$

Thus $[f(J)] = [f(I)]$.

To finish establishing the correspondence between the Narrow class group and the set of classes of binary quadratic forms, it suffices to show that any binary quadratic form of discriminant d_K arises from at least one ideal class. We can prove this explicitly as follows.

Lemma 0.3 *Let $f = ax^2 + bxy + cy^2$ be a primitive binary quadratic form of discriminant d (if $d < 0$ assume that $a > 0$). Let*

$$I = \begin{cases} \left[a, \frac{b-\sqrt{d}}{2}\right] & a > 0, \\ \left[a\sqrt{d}, \frac{b-\sqrt{d}}{2} \cdot \sqrt{d}\right] & a < 0. \end{cases}$$

Then $[f(I)] = [f]$.