More Factorization in Rings

Here we continue our study of factorization in rings of the form

$$R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Z}\}.$$

Here d is a fixed integer which is not a perfect square (so that $\sqrt{d}$ is irrational). For any $r = a + b\sqrt{d} \in R$, we define the *conjugate* of r as

$$\overline{r} = a - b\sqrt{d} \in R.$$

(If $d < 0$ then $\overline{r}$ is in fact the usual complex conjugate of r; but if $d > 0$ then all elements of R are real so this notion of conjugation is different than complex conjugation. To avoid confusion, the expression $\overline{r}$ we have defined may be called the *algebraic conjugate* of r.) Also define the *norm* of r as

$$N(r) = r\overline{r} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}.$$

Proposition. *For all $x, y \in R$ we have*
(a) $\overline{x + y} = \overline{x} + \overline{y}$;
(b) $\overline{xy} = \overline{x}\cdot\overline{y}$;
(c) $N(xy) = N(x)N(y)$.

Proof. Write $x = a + b\sqrt{d}$ and $y = u + b\sqrt{d}$ where $a, b, u, v \in \mathbb{Z}$. Then

$$\begin{aligned}
\overline{x + y} &= \overline{(a + b\sqrt{d}) + (u + v\sqrt{d})} = \overline{(a + u) + (b + v)\sqrt{d}} \\
&= (a + u) - (b + v)\sqrt{d} = (a - b\sqrt{d}) + (u - v\sqrt{d}) = \overline{x} + \overline{y}; \\
\overline{xy} &= \overline{(a + b\sqrt{d})(u + v\sqrt{d})} = \overline{(au + dbv) + (av + bu)\sqrt{d}} \\
&= (au + dbv) - (av + bu)\sqrt{d} = (a - b\sqrt{d})(u - v\sqrt{d}) = \overline{x}\cdot\overline{y}.
\end{aligned}$$

This proves (a) and (b). Now the proof of (c) is easy:

$$N(xy) = xy\cdot\overline{xy} = xy\cdot\overline{x}\cdot\overline{y} = x\overline{x}\cdot y\overline{y} = N(x)N(y).$$

□

(As an exercise, check that $N(x + y)$ is *not* the same as $N(x) + N(y)$.) The norm function is very useful in the study of factorization in R: for classifying units, for deciding irreducibility, and for factorization. We proceed with some examples of this.

Determining Units

We first use the norm to help classify units. Recall that by definition, $u \in R$ is a *unit* iff there exists $v \in R$ such that $uv = vu = 1$.

Theorem. *Let $x \in R = \mathbb{Z}[\sqrt{d}]$. Then x is a unit iff $N(x) = \pm 1$.*

Proof. First suppose that $x \in R$ is a unit, so that $xy = 1$ for some $y \in R$; then $N(x)N(y) = N(xy) = N(1) = 1$. Since $N(x)$ and $N(y)$ are integers, this forces $N(x) = N(y) = \pm 1$.

Conversely, suppose that $N(x) = \pm 1$; then $x\overline{x} = \pm 1$ so that $x(\pm\overline{x}) = 1$ and so x is a unit. □

The set of units in R is denoted $R^\times$. As a first example, let us find the units of $\mathbb{Z}[\sqrt{-5}]$: An element $u = a + b\sqrt{-5}$ is a unit iff $N(u) = a^2 + 5b^2 = \pm 1$. Clearly the only integer solutions of this relation are $a \in \{1, -1\}$ and $b = 0$; thus the only units of $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1. We therefore have $\mathbb{Z}[\sqrt{-5}] = \{1, -1\}$.

The ring $\mathbb{Z}[\sqrt{5}]$ is interesting: here the units $u = a + b\sqrt{5}$ correspond to solutions of $a^2 - 5b^2 = \pm 1$. This equation has infinitely many integer solutions! First note that $(a, b) = (2, 1)$ is a solution, so $2 + \sqrt{5}$ is a unit with $(2 + \sqrt{5})(-2 + \sqrt{5}) = 1$. Also $\pm(2 + \sqrt{5})^k$ is a unit for every integer k, since

$$\left[\pm(2 + \sqrt{5})^k\right]\left[\pm(-2 + \sqrt{5})^k\right] = 1.$$

This gives infinitely many units in $\mathbb{Z}[\sqrt{5}]$:

$$\pm 1,\ \pm 2 \pm \sqrt{5},\ 9 \pm 4\sqrt{5},\ \pm 38 \pm 17\sqrt{5},\ \pm 161 \pm 72\sqrt{5},\ 682 \pm 305\sqrt{5}, \ldots.$$

With a little more work, it may be shown that these are the *only* units in $\mathbb{Z}[\sqrt{5}]$, so that in fact

$$\mathbb{Z}[\sqrt{5}]^\times = \{\pm(2 + \sqrt{5})^k \,:\, k \in \mathbb{Z}\}.$$

However, to justify this would require more technical work than we care to indulge in at this early stage in our investigation of rings.

A more difficult case would be to find the units of $\mathbb{Z}[\sqrt{61}]$, for which we must solve $a^2 - 61b^2 = 1$. Again, there are infinitely many solutions; but aside from the trivial solutions $(a, b) = (\pm 1, 0)$, it will be very difficult to find any solutions by inspection. The units of $\mathbb{Z}[\sqrt{61}]$ are in fact

$$\begin{aligned}\mathbb{Z}[\sqrt{61}]^\times &= \{\pm(29718 + 3805\sqrt{61})^k \,:\, k \in \mathbb{Z}\} \\ &= \{\pm 1,\ \pm 29718 \pm 3805\sqrt{61},\ \pm 1766319049 \pm 226153980\sqrt{61},\ \ldots\}.\end{aligned}$$

The task of determining the units of $\mathbb{Z}[\sqrt{d}]$ is equivalent to the problem of finding the integer solutions of $a^2 - db^2 = 1$. The latter equation is known as *Pell's equation*; and an

algorithm for its solution, using continued fractions, is a standard topic in number theory courses, including our Math 4550. We will not digress further on this topic here.

Factoring and Verifying Irreducibility

Consider the problem of factoring 369 into irreducible factors in $R = \mathbb{Z}[\sqrt{-5}]$. We may begin by factoring $369 = 3{\cdot}3{\cdot}41$. The factor 3 is irreducible, which we verify as follows: Suppose $3 = xy$ where $x, y \in R$; then $N(x)N(y) = N(3) = 9$. However $N(x)$ and $N(y)$ are non-negative integers (recall that $N(a + b\sqrt{-5}) = a^2 + 5b^2$) so the only possibilities for the factorization $N(x)N(y) = 9$ are $9 \times 1 = 9$, $3 \times 3 = 9$ or $1 \times 9 = 9$. If $N(x) = 1$ then x is a unit; and if $N(y) = 1$ then y is a unit. The only other possibility is that $N(x) = N(y) = 3$; but this is impossible since $a^2 + 5b^2 = 3$ has no integer solutions. Thus 3 is irreducible in R as claimed. However, factoring 41 is a different story: if $41 = xy$ then $N(x)N(y) = N(41) = 41^2$ which has a nontrivial solution with $N(x) = N(y) = 41$. This requires us to solve $a^2 + 5b^2 = 41$, and we quickly find solutions $(a, b) = (\pm 6, \pm 1)$. This yields the factorization

$$369 = 3{\cdot}3{\cdot}(6 + \sqrt{-5})(6 - \sqrt{-5}).$$

All four factors here are irreducible in $\mathbb{Z}[\sqrt{-5}]$; for example if $6 + \sqrt{-5} = xy$ then $N(x)N(y) = N(6 + \sqrt{-5}) = 41$ so either $N(x) = 1$ or $N(y) = 1$, whence either x or y is a unit.

Other factorizations of 41 are available in $\mathbb{Z}[\sqrt{-5}]$; for example,

$$369 = (2 + \sqrt{-5})(2 - \sqrt{-5})(6 + \sqrt{-5})(6 - \sqrt{-5}).$$

We verify the irreducibility of all four factors here, using the norm map as we did above for 3 and $6 \pm \sqrt{-5}$. This factorization is *essentially different* from the factorization of 369 given above (i.e. the irreducible factors $2 \pm \sqrt{-5}$ are not associates of 3). Here we have further confirmation that the ring $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization. (We have already encountered this when factoring $6 = 2{\cdot}3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.)