TheNumbersBook.com 2010

Stewart: # 5.3, 5.4, 5.5, 5.8, 5.10, 5.13

5.3 Calculate the norms of ideals mentioned in Exercise 2 and check multiplicativity.

Recall that $P = \langle 2, 1+\sqrt{-5}\rangle, Q = \langle 3, 1+\sqrt{-5}\rangle$ and $R = \langle 3, 1-\sqrt{-5}\rangle$ and, by Theorem 3.2, $O_K = \mathbb{Z}[\sqrt{-5}]$.

First, consider P. We will show that any element in $\mathbb{Z}[\sqrt{-5}]$ is either in P or $1+P$ (that is $1+x$ for some $x \in P$). Let $a + b\sqrt{-5} = r \in \mathbb{Z}[\sqrt{-5}]$. If $r \in P$, then we're done. Therefore, suppose that $r \notin P$. Rewriting, we get

$$r = (a-b) + b(1+\sqrt{-5}) = (a-b) + x$$

for $x \in P$. If $a-b$ is even, then $r \in P$, a contradiction. Thus, $a-b$ is odd, and so we have

$$\begin{aligned} r &= (a-b) + x \\ &= 2n + 1 + x \text{ (for some } n \in \mathbb{Z}) \\ &= 1 + (2n + x) \\ &= 1 + x' \text{ (for } x' \in P) \\ &\in 1 + P \end{aligned}$$

Thus, any element of $\mathbb{Z}[\sqrt{-5}]$ is either in P or $1+P$. Thus, $O_K/P = \{P, 1+P\}$ and, by definition of norm, we have

$$N(P) = |O_K/P| = 2$$

Now consider Q. We show that any element in $\mathbb{Z}[\sqrt{-5}]$ is in $Q, 1+Q, 2+Q$. Let $a + b\sqrt{-5} = r \in \mathbb{Z}[\sqrt{-5}]$. If $r \in Q$, then we're done. Therefore, suppose that $r \notin Q$. Rewriting, we get

$$r = (a-b) + b(1+\sqrt{-5}) = (a-b) + x$$

for $x \in Q$. There are three possibilities: $a - b = 3n, 3n+1$ or $3n+2$ for $n \in \mathbb{Z}$. If $a - b = 3n$, then $r = a - b + x \in Q$, a contradiction. Thus, $a-b$ is either $3n+1$ or $3n+2$ and so we have

$$\begin{aligned} r &= (a-b) + x & \qquad r &= (a-b) + x \\ r &= 3n + 1 + x & r &= 3n + 2 + x \\ r &= 1 + x' & r &= 2 + x' \text{ (for some } x' \in Q) \\ &\in 1 + Q & &\in 2 + Q \end{aligned}$$

Thus any element of $\mathbb{Z}[\sqrt{-5}]$ is in $Q, 1+Q$ or $2+Q$. Thus,

$$N(Q) = |O_K/Q| = |\{Q, 1+Q, 2+Q\}| = 3$$

Now consider R. We show that any element in $\mathbb{Z}[\sqrt{-5}]$ is in $R, 1+R, 2+R$. Let $a + b\sqrt{-5} = r \in \mathbb{Z}[\sqrt{-5}]$. If $r \in R$, then we're done. Therefore, suppose that $r \notin R$. Rewriting, we get

$$r = (a+b) + b(1-\sqrt{-5}) = (a+b) + x$$

for $x \in R$. There are three possibilities for $a+b$: $a+b = 3n, 3n+1$ or $3n+2$ for $n \in \mathbb{Z}$. If $a+b = 3n$, then $r = a+b+x \in Q$, a contradiction. Thus, $a+b$ is either $3n+1$ or $3n+2$ and so we have

$$\begin{aligned} r &= (a+b)+x & \qquad r &= (a+b)+x \\ r &= 3n+1+x & r &= 3n+2+x \\ r &= 1+x' & r &= 2+x' \text{ (for some } x' \in R) \\ &\in 1+R & &\in 2+R \end{aligned}$$

Thus any element of $\mathbb{Z}[\sqrt{-5}]$ is in $R, 1+R$ or $2+R$. Thus,

$$N(R) = |O_K/R| = |\{R, 1+R, 2+R\}| = 3$$

Finally, we check multiplicativity. Note that $N(\langle 2\rangle) = 4, N(\langle 3\rangle) = 9$ and $N(\langle 1+\sqrt{-5}\rangle) = N(\langle 1-\sqrt{-5}\rangle) = (1+\sqrt{-5})(1-\sqrt{-5}) = 6$. Thus,

$$\begin{aligned} N(P^2) &= N(P)^2 = 4 = N(\langle 2\rangle) \\ N(QR) &= N(Q)N(R) = 9 = N(\langle 3\rangle) \\ N(PQ) &= N(P)N(Q) = 6 = N(\langle 1+\sqrt{-5}\rangle) \\ N(PR) &= N(P)N(R) = 6 = N(\langle 1-\sqrt{-5}\rangle) \\ N(P^2QR) &= N(P)^2N(Q)N(R) = 36 = N(\langle 6\rangle) \end{aligned}$$

so multiplicativity works out. ■

5.4 Prove that the ideals P, Q, R of Exercise 2 cannot be principal.

From 5.3, we established that $N(P) = 2$ and $N(Q) = N(R) = 3$. Suppose, by way of contradiction, that P is principal. That is, $P = \langle a + b\sqrt{-5}\rangle$ for some $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. By Corollary 5.10, we have

$$\begin{aligned} 2 &= N(P) \\ &= N(\langle a+b\sqrt{-5}\rangle) \\ &= N(a+b\sqrt{-5}) \\ &= (a+b\sqrt{-5})(a-b\sqrt{-5}) \text{ (definition of norm)} \\ &= a^2 + 5b^2 \end{aligned}$$

This, however, is a contradiction as there are no integer solutions to $a^2 + 5b^2 = 2$. Thus, P is not principal.

Now, suppose by way of contradiction that Q is principal: $Q = \langle a + b\sqrt{-5} \rangle$ for some $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Using the same approach as above, we have $3 = a^2 + 5b^2$, a contradiction since there are no integer solutions. Thus, Q is not principal.

Finally, suppose by way of contradiction that R is principal: $R = \langle a + b\sqrt{-5} \rangle$ for some $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Using the same approach as above, we have that $3 = a^2 + 5b^2$, a contradiction. Thus, R is not principal. ■

5.5 Show the principal ideals $\langle 2 \rangle, \langle 3 \rangle$ in Exercise 2 are generated by irreducible elements but the ideals are not prime.

We show that 2 and 3 are irreducible in $\mathbb{Z}[\sqrt{-5}]$. First, suppose that 2 factors into $(a + b\sqrt{-5}), (c + d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$. Taking the norm, we have

$$\begin{aligned} N(2) &= N((a + b\sqrt{-5})(c + d\sqrt{-5})) \\ 4 &= N(a + b\sqrt{-5})N(c + d\sqrt{-5}) \\ 4 &= (a^2 + 5b^2)(c^2 + 5d^2) \end{aligned}$$

Since 4 factors into 4×1 or 2×2 (up to reordering), we have that $4 = a^2 + 5b^2, 1 = c^2 + 5d^2$ or $2 = a^2 + 5b^2 = c^2 + 5d^2$. From this, the only possibility is $a = 2, b = 0, c = 1, d = 0$ which implies that 2 factors into 2×1. Thus, 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Now suppose that $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Taking the norm, we have

$$\begin{aligned} N(3) &= N((a + b\sqrt{-5})(c + d\sqrt{-5})) \\ 9 &= N(a + b\sqrt{-5})N(c + d\sqrt{-5}) \\ 9 &= (a^2 + 5b^2)(c^2 + 5d^2) \end{aligned}$$

Since 9 factors into 9×1 or 3×3, we have that $9 = a^2 + 5b^2, 1 = c^2 + 5d^2$ or $3 = a^2 + 5b^2 = c^2 + 5d^2$. From this, the only possibilities are $a = 3, b = 0, c = 1, d = 0$ or $a = 2, b = 1, c = 1, d = 0$. The latter possibility implies $3 = 2 + \sqrt{-5}$, which is impossible. Thus, the only factorization of 3 is 3×1, implying that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Now note that $P = \langle 2, 1 + \sqrt{-5} \rangle \not\subseteq \langle 2 \rangle$ since $1 + \sqrt{-5} \notin \langle 2 \rangle$. By Proposition 5.7, this implies that $\langle 2 \rangle \nmid P$. However, Exercise 5.5.2 showed that $\langle 2 \rangle = P^2$ and so $\langle 2 \rangle | P^2$. We've just shown that $\langle 2 \rangle | PP$ but $\langle 2 \rangle \nmid P$. Thus, $\langle 2 \rangle$ is not prime.

Finally, note that $Q = \langle 3, 1 + \sqrt{-5} \rangle \not\subseteq \langle 3 \rangle$ (because $1 + \sqrt{-5} \notin \langle 3 \rangle$) and $R = \langle 3, 1 - \sqrt{-5} \rangle \not\subseteq \langle 3 \rangle$. By Proposition 5.7, this means that $\langle 3 \rangle \nmid Q$ and $\langle 3 \rangle \nmid R$. However, by Exercise 5.5.2, we have that $\langle 3 \rangle | QR$. Thus, $\langle 3 \rangle$ is not prime because we've just shown that $\langle 3 \rangle | QR$ but $\langle 3 \rangle \nmid Q$ or R. ■

5.8 Suppose P, Q are distinct prime ideals in O_K. Show $P + Q = O_K$ and $P \cap Q = PQ$.

Assume that P and Q are nonzero. By Theorem 5.3(d), P and Q are maximal. Now note that $P + Q \subseteq O_K$ is an ideal because

(1) $P + Q$ consists of elements of the form $p + q$ for $p \in P, q \in Q$. Note that $(p + q) + (p' + q') = (p + p') + (q + q') \in P + Q$ and

(2) For any $r \in O_K$,

$$\begin{aligned} r(p + q) &= rp + rq \\ &= p' + q' \text{ (because } P, Q \text{ are ideals)} \\ &\in P + Q \end{aligned}$$

Moreover, P is properly contained in $P + Q$ since we can choose any $0 \neq \alpha \in Q$ and get an element outside of P. Thus, $P \subset P + Q \subseteq O_K$ and since P is maximal (by Theorem 5.3d) and not equal to $P + Q$, it must be that $P + Q = O_K$.

Now consider $P \cap Q$. First, note that for $r, r' \in P \cap Q$, we have $r + r' \in P \cap Q$ because $r + r' \in P$ and $r + r' \in Q$ (because P, Q are ideals). Similarly, for any $\alpha \in O_K$, $\alpha r \in P \cap Q$ because $\alpha r \in P$ and $\alpha r \in Q$. Thus, $P \cap Q$ is an ideal of O_K.

Since P is an ideal, then $Pr \subseteq P$ for any $r \in O_K$. Specifically, $PQ \subseteq P$. At the same time, $PQ \subseteq Q$ because Q is also an ideal. Thus, $PQ \subseteq P \cap Q$. On the other hand, $P \cap Q \subseteq P$ and $P \cap Q \subseteq Q$ which by Proposition 5.7, implies $P | P \cap Q$ and $Q | P \cap Q$. Now, by Theorem 5.6, $P \cap Q$ can be written as a product of prime ideals, two of which are P and Q. Call the product of remaining ideals R. Then we have the following equality:

$$P \cap Q = PQR$$

This immediately implies that $PQ | P \cap Q$, or equivalently $P \cap Q \subseteq PQ$. The results of this paragraph imply that $P \cap Q = PQ$. ∎

5.10 Find all fractional ideals of $\mathbb{Z}$ and of $\mathbb{Z}[\sqrt{-1}]$.

By Example 5.4, all fractional ideals of $\mathbb{Z}$ are of the form $r\mathbb{Z}$ for $r \in \mathbb{Q}$.

Since $-1 \equiv 3 \not\equiv 1 (\mod 4)$, $\mathbb{Z}[i]$ is its own ring of integers by Theorem 3.2(a). We know from class that $\mathbb{Z}[i]$ is a UFD so Theorem 5.21 guarantees that every ideal of $\mathbb{Z}[i]$ is principal. Consider any ideal $\langle a + bi \rangle \subseteq \mathbb{Z}[i]$ for $a, b \in \mathbb{Z}$. By Theorem 5.3(a), the fractional ideals are of the form $\alpha \langle a + bi \rangle$ where $\alpha \in \mathbb{Q}[i]$ (the field of fractions of $\mathbb{Z}[i]$). ∎

5.13 Find all the ideals in $\mathbb{Z}[\sqrt{2}]$ with norm 18.

By Theorem 3.2a, $O_K = \mathbb{Z}[\sqrt{2}]$. Theorem 4.19 asserts that $\mathbb{Z}[\sqrt{2}]$ is Euclidean, and so a UFD. By Theorem 5.21, every ideal in $\mathbb{Z}[\sqrt{2}]$ is principal.

Since any ideal in $\mathbb{Z}[\sqrt{2}]$ is principal, let $I = \langle a + b\sqrt{2} \rangle$ be any ideal. By Corollary 5.10,

$$\begin{aligned} N(I) &= |N(a + b\sqrt{2})| \\ &= |(a + b\sqrt{2})(a - b\sqrt{2})| \\ &= |a^2 - 2b^2| \end{aligned}$$

so a necessary condition for I to have norm 18 is that $a^2 - 2b^2 = \pm 18$.

At this point, there are several directions we can take. One possibility is to note that $a^2 - 2b^2 = 18$ is a curve. One integer point is $(6, 3)$. Similarly, $a^2 - 2b^2 = -18$ is a curve. One integer point is $(0, 3)$. One way, of course, is to look for integer points on these curves. Another characterization of the solutions is the recursive system:

$$\begin{aligned} a_{n+1} &= 3a_n + 4b_n \\ b_{n+1} &= 2a_n + 3b_n \end{aligned}$$

We prove by induction that a_{n+1}, b_{n+1} is a solution. Let $n = 0$: $a_1 = 6, b_1 = 3$ is one solution. Now suppose that (a_n, b_n) is a solution. Plugging in a_{n+1}, b_{n+1}, we get

$$\begin{aligned} a_{n+1} - 2b_{n+1} &= (3a_n + 4b_n)^2 - 2(2a_n + 3b_n)^2 \\ &= 9a_n^2 + 24a_nb_n + 16b_n^2 - 2(4a_n^2 + 12a_nb_n + 9b_n^2) \\ &= a_n^2 - 2b_n^2 \end{aligned}$$

which, by induction, we know must equal ±18. Thus, the above recursive formula provides infinitely many solutions. ■