Math 361 lecture for Friday, Week 6

Operations on ideals

Our next big goal: let $\mathfrak{O}_K$ be the ring of integers in a number field. We have seen in homework that elements of $\mathfrak{O}_K$ do not necessarily have uniquely factor into primes. However, it turns that ideals in $\mathfrak{O}_K$ uniquely factor into prime ideals (which we define below). Thus, for instance, if $\alpha \in \mathfrak{O}_K$ does not factor into primes, its corresponding principal ideal (α) will.

Let R be a ring (commutative, with 1). Recall that a nonempty subset $I \subseteq R$ is an *ideal* if it is closed under addition ($a, b \in I \Rightarrow a + b \in I$) and "inside-out" multiplication ($r \in R, a \in I \Rightarrow ra \in I$). Equivalently, I is an R-submodule of R.

An ideal I is *finitely generated* if it is finitely generated as an R-module. This means that there exist $a_1, \ldots, a_k \in R$ for some k such that

$$I = (a_1, \ldots, a_k) := \{\textstyle\sum_{i=1}^{k} r_i a_i : r_1, \ldots, r_k \in R\}.$$

Definition 1. The *sum* and *product* of ideals I and J of R are defined as follows:

$$I + J = \{a + b : a \in I \text{ and } b \in J\},$$
$$IJ = \{\textstyle\sum_{i=1}^{k} a_i b_i : k \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \text{ for all } i\}.$$

The proof that $I + J$ and IJ are ideals and the proof of the following proposition are left as straightforward exercises.

Proposition 2. Let I, J and K be ideals of R, and let $a, b \in R$.

1. $I(J + K) = IJ + IK$,
2. $(IJ)K = I(JK)$,
3. $IJ = JI$,
4. $I(0) = (0)$,
5. $I(1) = I$,
6. $(a_1, \ldots, a_k) + (b_1, \ldots, b_\ell) = (a_i + b_j : 1 \le i \le k, 1 \le j \le \ell)$,
7. $(a_1, \ldots, a_k)(b_1, \ldots, b_\ell) = (a_i b_j : 1 \le i \le k, 1 \le j \le \ell)$,
8. $(a) \subseteq (b)$ if and only if $b|a$, and
9. if R is a domain, then $(a) = (b)$ if and only if $a = ub$ for some unit u.

Definition 3. Let P be an ideal of R. Then

1. P is *prime* if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$, and

2. P is *maximal* if $P \neq R$ and if whenever Q is an ideal of R and $P \subsetneq Q$, then $Q = R$.

Proposition 4.

1. P is prime if and only if for all ideals I and J such $IJ \subseteq P$, we have $I \subseteq P$ or $J \subseteq P$.
2. If P is maximal, then P is prime.
3. P is prime if and only if R/P is a domain.
4. P is maximal if and only if R/P is a field.

Proof.

1. Homework.
2. Suppose that P is maximal. Let $ab \in P$ with $a \notin P$. Then $P \subsetneq (a) + P$. By maximality, $(a) + P = R$. So there exist $r \in R$ and $p \in P$ such that $1 = ra + p$. Multiplying by b, we find $b = rab + bp \in P$.
3. ($\Rightarrow$) Suppose that P is prime and that $\overline{a}\,\overline{b} = 0 \in R/P$ with $\overline{a} \neq 0$. Then $ab \in P$ and $a \notin P$. Since P is prime, $b \in P$, and hence $\overline{b} = 0 \in R/P$. We have shown that R/P is a domain.

   ($\Leftarrow$) Suppose that R/P is a domain and that $ab \in P$ with $a \notin P$. It follows that $\overline{ab} = \overline{a}\,\overline{b} = 0 \in R/P$ and $\overline{a} \neq 0$. Since R/P is a domain, $\overline{b} = 0 \in R/P$. Hence, $b \in P$. We have shown that P is prime.
4. Homework.

□

Exercise 5. In this exercise, we look at a number ring which is not a UFD. We hint at uniqueness of factorization into primes can be recovered by passing from elements to ideals. Consider the number field $K = \mathbb{Q}(\sqrt{-5})$. Since $-5 \neq 1 \bmod 4$, the number ring of K is $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$. In homework, we have seen that

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

where $2, 3, 1 \pm \sqrt{-5}$ are non-associated irreducibles. (We say a, b is a ring are *associates* if $a = ub$ for some unit u. Note that association is an equivalence relation.) Thus, $\mathfrak{O}_K$ is not a UFD. Further, none of $2, 3, 1 \pm \sqrt{-5}$ is prime. (For instance, a straightforward calculation shows that although $(1 + \sqrt{-5})$ divides $2 \cdot 3$, it divides neither 2 nor 3: we have $(1 + \sqrt{-5})(a + b\sqrt{-5}) = (a - 5b) + (a + b)\sqrt{-5} \in \mathbb{Z}$ if and only if $a + b = 0$. So in this case, $(1 + \sqrt{-5})(a + b\sqrt{-5}) = 6a$. Then $6a = 2$ and $6a = 3$ have no integer solutions.)

Define

$$P_1 = (2, 1 + \sqrt{-5}), \quad P_2 = (3, 1 + \sqrt{-5}), \quad P_3 = (3, 1 - \sqrt{-5}).$$

We claim these ideals are all primes. We will have better methods of proving this later, but for now, let's show that P_1 is prime by showing that $\mathbb{Z}[\sqrt{-5}]/P_1$ is isomorphic to the field $\mathbb{Z}/2\mathbb{Z}$. That implies that P_1 is maximal, hence prime. First note that for $a, b \in \mathbb{Z}$, working modulo P_1,

$$a + b\sqrt{-5} = (a + b\sqrt{-5}) - b(1 + \sqrt{-5}) = a - b \bmod P_1.$$

since $1 + \sqrt{-5} \in P_1$. Further, since $2 \in P_1$, we can take the value of $a - b$ modulo 2.

Define

$$\begin{aligned} \phi\colon \mathbb{Z}[\sqrt{-5}] &\to \mathbb{Z}/2\mathbb{Z} \\ a + b\sqrt{-5} &\mapsto \overline{a - b} \end{aligned}$$

We claim that ϕ is a well-defined isomorphism of rings. To show it is well-defined, we must show that $\phi(p) = \overline{0}$ for all elements $p \in P_1$. It suffices to show that the generators P_1 are sent to $\overline{0} \in \mathbb{Z}/2\mathbb{Z}$. First, we have $\phi(2) = \overline{2} = \overline{0}$. Next, we have $\phi(1 + \sqrt{-5}) = \overline{1} - \overline{1} = \overline{0}$.

We now show that ϕ preserves sums and products. Let $a, b, c, d \in \mathbb{Z}$. Then

$$\begin{aligned} \phi((a + b\sqrt{-5}) + (c + d\sqrt{-5})) &= \phi((a + c) + (b + d)\sqrt{-5}) \\ &= \overline{a + c} - \overline{b + d} \\ &= \overline{a - b} - \overline{c - d} \\ &= \phi(a + b\sqrt{-5}) + \phi(c + d\sqrt{-5}), \end{aligned}$$

and, recalling that $\overline{1} = -\overline{1}$ in $\mathbb{Z}/2\mathbb{Z}$,

$$\begin{aligned} \phi((a + b\sqrt{-5})(c + d\sqrt{-5})) &= \phi((ac - 5bd) + (ad + bc)\sqrt{-5}) \\ &= \overline{ac - 5bd} - \overline{ad + bc} \\ &= \overline{ac} + \overline{bd} + \overline{ad} + \overline{bc} \end{aligned}$$

whereas

$$\begin{aligned} \phi(a + b\sqrt{-5})\phi(c + d\sqrt{-5}) &= (\overline{a - b})(\overline{c - d}) \\ &= \overline{ac} + \overline{bd} + \overline{ad} + \overline{bc}. \end{aligned}$$

. Since $\phi(0) = \overline{0}$ and $\phi(1) = \overline{1}$, we see that ϕ is surjective. To show injectivity, suppose that $\phi(a + b\sqrt{-5}) = \overline{a - b} \bmod 2$. So $a = b + 2k$ for some $k \in \mathbb{Z}$. We must show that $a + b\sqrt{-5} \in P_1$. We have

$$a + b\sqrt{-5} = (b + 2k) + b\sqrt{-5} = 2k + b(1 + \sqrt{-5}) \in P_1 = (2, 1 + \sqrt{-5}).$$

We now want to consider factoring the principal ideal (6) in $\mathfrak{O}_K$. We leave it to reader to check the following calculations:

$$P_1^2 = (2), \quad P_2P_3 = (3), \quad P_1P_2 = (1 + \sqrt{-5}), \quad P_1P_3 = (1 - \sqrt{-5}).$$

We may factor (6) into prime ideals as

$$(6) = (2)(3) = (P_1)^2(P_2P_3) = P_1^2P_2P_3.$$

or

$$(6) = (1+\sqrt{-5})(1-\sqrt{-5}) = (P_1P_2)(P_1P_3) = P_1^2P_2P_3.$$

To recap: $2, 3, 1 \pm \sqrt{-5}$ are irreducible but not prime in $\mathfrak{O}_K$. Their corresponding principal ideals factor into prime ideals, and when we do that, we get two corresponding factorizations of (6) into prime ideals. These two factorizations are, in fact, the same! This example illustrates the general phenomenon of unique factorization of ideals into primes in a number field.