M3P8 LECTURE NOTES 3: FACTORIZATION

In these notes R always denotes an integral domain.

1. Divisibility, Units, Associates, and Irreducibles

Let r, s be elements of R. We say r divides s (notation: $r \mid s$) if there exists $r' \in R$ with $rr' = s$ (or, equivalently, s lies in the principal ideal generated by r). An element of r that divides 1_R is called a *unit* of R; the set of units in R forms a group under multiplication denoted $R^\times$.

For any element r of R, and any unit u of R, both u and ur divide r. The set of elements of R of the form ur, with $r \in R^\times$ are called *associates* of R. Note that the principal ideals $\langle r \rangle$ and $\langle r' \rangle$ are equal if, and only if, r and r' are associates.

A nonzero element r of R is called *irreducible* if r is not a unit and the only elements of R that divide r are the units and the associates of r.

2. Unique Factorization Domains

An interesting question is when elements of rings admit unique factorizations into irreducibles. To that end we define a *Unique Factorization Domain* (UFD for short) to be a ring R in which:

(1) every nonzero element of r admits a factorization as a finite product of irreducibles in R, and
(2) if $r = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ are two factorizations of r as products of irreducibles, then $k = \ell$ and, after permuting the q_i, each q_i is an associate of p_i.

There are certainly domains in which (1) can fail, although they are somewhat exotic. One example is to take the "rational polynomial ring" with coefficients in $\mathbb{C}$, whose entries are finite formal sums $\sum a_i t^{b_i}$ where the a_i are in $\mathbb{C}$ and the b_i are *rational numbers*; every such expression is a polynomial in $t^{\frac{1}{n}}$ for some n. The element t of this ring is not a unit, and also not a finite product of irreducibles. We will show later that a very mild "finiteness" condition on a domain R (the condition that R is *Noetherian*) actually guarantees that (1) holds.

Even if (1) holds, (2) often fails. The classic example of this is $\mathbb{Z}[\sqrt{-5}]$, in which $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducibles, none are associates of each other, yet $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Another way to interpret condition (2) is as follows: we say an element r of R is *prime* if the principal ideal $\langle r \rangle$ of R is a prime ideal; in other words, for any a, b in R, if r divides ab, then r divides a or r divides b. Note that prime elements are irreducible: if r is prime and s divides r, we can write

$r = sr'$; then since r divides sr' we have that either r divides s, (in which case r is an associate of s) or r divides r' (in which case r is an associate of r' and s is a unit). The converse is not necessarily true, but we have:

Proposition 2.1. *Let R be a domain in which condition (1) holds. Then condition (2) above holds for R if, and only if, every irreducible element of R is prime.*

Proof. First suppose condition (2) holds, and let r be an irreducible element of R. If r divides ab, we can write $rs = ab$ for some $s \in R$; expanding out s, a, and b as products of irreducibles we see that r is an associate of some irreducible dividing a or b, so r is prime.

Conversely, if every irreducible element of R is prime, and we have $p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$ products of irreducibles, then, since p_1 is prime, it divides the product $q_1 q_2 \dots q_\ell$ and is thus an associate of some q_i; we can thus cancel p_1 from the left and q_i from the ring (after introducing a unit on one side)- this is possible because R is an integral domain. Repeating the process we find that (up to reordering the terms and multiplying by units) the two expressions coincide. □

3. Principal Ideal Domains

An integral domain R is a *Principal Ideal Domain* (PID) if every ideal of R is a principal ideal.

Theorem 3.1. *Every PID is a UFD.*

Proof. We first show (1). It is true for units trivially. Fix $r = r_0 \in R$ not a unit; we first show r has an irreducible factor. If r_0 is irreducible we are done. If r_0 is not irreducible, we can choose an r_1, not a unit nor an associate of r_0, such that r_1 divides r_0. If r_1 is not irreducible we choose r_2 similarly, and repeat. If this process ever terminates we have found an irreducible divisor of r. Suppose it does not terminate. We obtain an increasing tower of ideals:

$$\langle r_0 \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_2 \rangle \subsetneq \dots$$

Let I be the *union* of all these ideals. Then I is an ideal, so it is generated by some element s. Thus s divides r_i for all i. On the other hand, s lives in some $\langle r_j \rangle$, so r_j divides s. Thus s is an associate of r_j, and therefore an associate of r_i for all $i > j$. This contradicts our construction!

Thus r has an irreducible divisor s_0. Consider rs_0^{-1}. If this is a unit we are done. If not let s_1 be an irreducible divisor of rs_0^{-1}; if $r(s_0 s_1)^{-1}$ is a unit we are done; otherwise repeat. We obtain a sequence of irreducibles $s_0, s_1, \dots$ such that $s_0 s_1 \dots s_i$ divides r for all i. If this process ever terminates we are done. Suppose it does not. Then we have a strictly increasing tower of ideals:

$$\langle r \rangle \subsetneq \langle rs_0^{-1} \rangle \subsetneq \langle r(s_0 s_1)^{-1} \rangle \subsetneq \dots$$

and arguing as above we arrive at a contradiction.

Now we show (2). It suffices to show that every irreducible is prime. Let r be irreducible, and suppose that r divides ab. Let s be a generator of the ideal $\langle r, a\rangle$ of R. Then s divides r, so either s is a unit or s is an associate of r. If s is an associate of r, then since s divides a, r divides a. On the other hand, if s is a unit, then the ideal generated by r and a is the unit ideal, so we can write $1 = xa + yr$ for x, y elements of R. We then have $b = xab + ybr$, and since r divides both ybr and xab, r divides b. □

4. Euclidean Domains

One technique for proving that rings are PIDs is Euclid's algorithm. We formalize this in an abstract setting as follows:

Definition 4.1. An integral domain R is a *Euclidean Domain* if there is a function $N : R \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$, with $b \neq 0$, there exists $q, r \in R$ such that $a = qb + r$, and either $r = 0$ or $N(r) < N(b)$.

Theorem 4.2. *Any Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain, and I an ideal of R. Let n be the smallest integer such that there exists $b \in I$ with $N(b) = n$. Then for any $a \in I$, we can write $a = qb + r$ with $N(r) < N(b)$ unless $r = 0$. But since $N(b)$ is the smallest possible norm in I, we must have $r = 0$, so $a = qb$. Thus I is generated by b and we are done. □

5. Examples

The classic example of a Euclidean domain is $\mathbb{Z}$, with $N(x) = |x|$ for $x \in \mathbb{Z}$.

The ring $\mathbb{Z}[i]$ is a Euclidean domain, with $N(z) = z\overline{z} = |z|^2$. To see this, note that given a and b in $\mathbb{Z}[i]$, we have $\frac{a}{b} = x + iy$ with $x, y \in \mathbb{Q}$. Let x' and y' be the closest integers to x and y, and set $q = x' + iy'$ in $\mathbb{Z}[i]$. Then $N(a - qb) = N(b)N(\frac{a}{b} - q) = N(b)((x - x')^2 + (y - y')^2) \leq \frac{N(b)}{2}$.

Similar arguments can be used to prove that $\mathbb{Z}[\alpha]$ is a Euclidean domain for $\alpha = \sqrt{-2}$, $\alpha = \frac{-1+\sqrt{-3}}{2}$, and $\alpha = \frac{-1+\sqrt{-7}}{2}$; beyond this one needs other tricks (and for most α unique factorization fails!).

A critical example is the polynomial ring $k[X]$ for k a field. Here we can take $N(P(X))$ to be the degree of $P(X)$. Then, given polynomials $A(X), B(X)$, we can use "polynomial long division" to write $A(X) = Q(X)B(X) + R(X)$ with the degree of R strictly less than that of B (unless B is constant, in which case we can make $r = 0$).