Factorization in Polynomial Rings

These notes are a summary of some of the important points on divisibility in polynomial rings from §17 and 18.

PIDs

Definition 1 A *principal ideal domain* (PID) is an integral domain D in which every ideal has the form $\langle a \rangle = \{ra : r \in D\}$ for some $a \in D$.

For example, $\mathbb{Z}$ is a PID, since every ideal is of the form $n\mathbb{Z}$.

Theorem 2 *If F is a field, then $F[X]$ is a PID.*

Proof We know that $F[X]$ is an integral domain. Let I be an ideal. If $I = \{0\}$, then $I = \langle 0 \rangle$.

Suppose $I \neq \{0\}$. Let $g \in I$ be a nonzero polynomial of minimal degree. We claim that $I = \langle g \rangle$. Suppose $f \in I$. By the division algorithm, there are nonzero polynomials q and r such that $f = qg + r$ and either $r = 0$ or deg(r) $<$ degg. Since $f, g \in I$, $r = f - qg \in I$. Since g is of minimal degree in I, we must have $r = 0$. Thus $f = qg \in \langle g \rangle$.

Definition 3 Let D be an integral domain. If $a \in D$ is nonzero and not a unit, we say that a is *irreducible* if whenever $b, c \in D$ and $a = bc$ then b is a unit or c is a unit.

Otherwise we say that a is *reducible*.

For example, in $\mathbb{Z}$, n is irreducible if and only if n is prime.

Suppose F is a field and $f \in F[X]$. If f has degree 1, then f is irreducible. If f has degree 2 or 3, then f is irreducible if f has no zero in F. [If $f = gh$ where neither g nor h is a unit, then one of g or h has degree 1 and has a root.]

Here are some examples

$X^2 - 2$ is irreducible in $\mathbb{Q}[X]$ but reducible in $\mathbb{R}[X]$ since $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.

$X^2 + 1$ is irreducible in $\mathbb{R}[X]$, but reducible in $\mathbb{C}[X]$ since $X^2 + 1 = (X + i)(X - i)$.

$2X + 2$ is irreducible in $\mathbb{R}[X]$, but reducible in $\mathbb{Z}[X]$ since $(2X + 2) = 2(X + 2)$ and 2 is a unit in $\mathbb{R}$, but a nonunit in $\mathbb{Z}$. This example shows we have to be more careful in $D[X]$ when D is not a field.

We recall some basic definitions from §14.

Definition 4 Let R be a commutative ring and let $I \neq R$ be an ideal of R.

I is a *prime ideal* if whenever $a, b \in R$ and $ab \in I$, then $a \in I$ or $b \in I$.

I is a *maximal ideal* if whenever J is an ideal and $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.

If R is a commutative ring with unity, then every maximal ideal is prime, but prime ideals need not be maximal. For example, in $\mathbb{R}[X, Y]$. The ideal $\langle X \rangle$ is prime (since $\mathbb{R}[X, Y]/\langle X \rangle \cong \mathbb{R}[Y]$ an integral domain), but not maximal since $\langle X \rangle \subset \langle X, Y \rangle \subset \mathbb{R}[X, Y]$.

We remind you of one key fact about prime and maximal ideals.

Theorem 5 *If R is a commutative ring with unity and I is an ideal then:*

i) I is prime if and only if R/I is an integral domain;

ii) I is maximal if and only if R/I is a field.

Proposition 6 *If D is an integral domain, and $\langle a \rangle$ is prime, then a is irredcuible.*

Proof Suppose $a = bc$. We must show that either b or c is a unit. Since $bc \in \langle a \rangle$ and $\langle a \rangle$ is a prime ideal, either $b \in \langle a \rangle$ or $c \in \langle a \rangle$. Suppose $b \in \langle a \rangle$. Then $b = ad$ for some $d \in D$. Thus $a = bc = adc$. Since D is an integral domain, $1 = dc$. Thus c is a unit. A similar argument shows that if $c \in \langle a \rangle$, then b is a unit. Thus a is irreducible.

The converse is true in $F[X]$ for F a field. Indeed, if $\langle a \rangle$ is irreducible, then $\langle a \rangle$ is maximal. The proof works just as well for all PIDs.

Theorem 7 *Let D be a PID and $a \in D$. The following are equivalent:*

i) a is irreducible;

ii) $\langle a \rangle$ is maximal;

iii) $\langle a \rangle$ is prime.

Proof

ii)⇒ iii) In any commuative ring with unity, every maximal ideal is prime.

iii) ⇒ i) This is Proposition 6

i) ⇒ ii) Suppose a is irreducible. Since a is not a unit $\langle a\rangle \neq D$. Let J be an ideal such that $\langle a\rangle \subseteq J \subseteq D$. We must show that $J = I$ or $J = D$.

Since D is a PID, there is $b \in D$ such that $J = \langle b\rangle$. Since $\langle a\rangle \subseteq J$, $a = bc$ for some $c \in D$. Since a is irreducible, either b or c is a unit.

case 1: b is a unit.

Then b has an inverse $b^{-1} \in D$. If $d \in D$, then $d = db^{-1}b \in J$. Thus $J = D$.

case 2: c is a unit.

Since $a = bc$, $b = c^{-1}a \in \langle a\rangle$. Since $b \in \langle a\rangle$, $J = \langle a\rangle$.

Corollary 8 *If F is a field and $p \in F[X]$ is irreducible, then $F[X]/\langle p\rangle$ is a field.*

Proof Since p is irreducible, $\langle p\rangle$ is maximal and $F[X]/\langle p\ >$ is a field.

UFDs

Suppose F is a field and $f \in F[X]$ is reducible. Then we can factor $f = gh$ where f and g both have lower degree. If either g or h is reducible, then we can factor again.

For example if $f = 2X^4 - 7X^3 + 8X^2 - 3X$ we see that

$$\begin{aligned} f &= X(2X^3 - 7X^2 + 8X - 3) \\ &= X(X-1)(2X^2 - 5X + 3) \\ &= X(X-1)(X-1)(2X-3) \end{aligned}$$

Proposition 9 *If F is a field and $f \in F[X]$ is nonzero and not a unit, then for some n there are irreducible polynomials $g_1, \ldots, g_n \in F[X]$ such that $f = g_1 g_2 \cdots g_n$.*

This is similar to the fact that in the natural numbers $\mathbb{N}$ we can factor every element as a product of primes. In $\mathbb{N}$ the prime factorization is unique. Is this true in $F[X]$? Not quite. For example

$$(X^2 - 1) = (X-1)(X+1) = \left(\frac{X}{2} - \frac{1}{2}\right)(2X+2).$$

Of course even in $\mathbb{Z}$ we have

$$6 = 2(3) = (-2)(-3).$$

Indeed if we have one irreducible factorization, then by multiplying by suitable units we can always get another.

The next definition gives us the right way to state uniqueness of factorization.

Definition 10 If D is a domain, we say that a and b are *associates* if there is a unit $u \in D$ such that $a = ub$.

Note that if u is a unit and $a = ub$, then $b = u^{-1}a$. Thus "being associates" is a symmetric relation.

Definition 11 If D is a domain, we say that D is a *Unique Factorization Domain* (or UFD) if:

i) if $f \in D$ is nonzero and not a unit, then there are irreducible elements $g_1, \ldots, g_n \in D$ such that $f = g_1 g_2 \cdots g_n$, and

ii) if $p_1, \ldots, p_n, q_1, \ldots, q_m \in D$ are irreducible, and $p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and there is $\sigma \in S_n$ such that p_i is an associate of $q_{\sigma(i)}$ for $i = 1, \ldots, n$.

In other words if $f = p_1 \cdots p_n = q_1 \cdots q_m$ are two factorizations of f into irreducible factors, then $n = m$ and we can renumber the q's so that p_i and q_i are associates for all i.

Suppose F is a field and

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

are irreducible factorizations of f in $F[X]$. Since p_1 is irreducible, $\langle p_1 \rangle$ is a prime ideal.

We need one easy lemma.

Lemma 12 *If D is an integral domain, $I \subset D$ is a prime ideal, $a_1, \ldots, a_n \in D$ and $a_1 a_2 \cdots a_n \in I$, then some $a_i \in I$.*

Proof We prove this by induction. If $n = 2$ this is the definition of a prime ideal. If $n > 2$ and $a_1(a_2 \cdots a_n) \in I$, then either $a_1 \in I$ and we are done, or $(a_2 \cdots a_n) \in I$. In the later case, by induction $a_j \in I$ for some $j = 2, \ldots, n$.

Since $q_1 \cdots q_m = p_1(p_2 \cdots p_n)$, there is an i such that $q_i \in \langle p_1 \rangle$. Thus $q_i = up_1$ for some i, since q_i is irreducible, u must be a unit.

Thus

$$p_1 \cdots p_n = q_1 \cdots q_m = q_1 \cdots q_{i-1}(up_1)q_{i+1} \cdots q_m.$$

Since D is an integral domain,

$$p_2 \cdots p_n = uq_1 \cdots q_{i-1}q_{i+1} \cdots q_m.$$

We have gotten rid of one irreducible from each side, but at the cost of introducing a unit. This leads us to the following lemma which gives the right induction.

Lemma 13 *Suppose F is a field, $p_1, \ldots, p_n, q_1, \ldots, q_m \in F[X]$ are irreducible, u is a unit, and $p_1 \cdots p_n = uq_1 \cdots q_m$. Then $n = m$ and we can renumber the q's so that p_i and q_i are associates for all i.*

Proof We prove this by induction on n.

Suppose $n = 1$. Then $p, q_1, \ldots, q_m$ are irreducible, u is a unit and $p = uq_1 \cdots q_m$. Since $uq_1 \ldots q_m \in \langle p \rangle$ and $\langle p \rangle$ is a prime ideal, there is q_i such that $q_i \in \langle p \rangle$. Then there is $w \in \langle p \rangle$ such that $q_i = wp$. Since q_i is irreducible and p is not a unit, w is a unit. Thus

$$p = uq_1 \cdots q_{i-1}(wp)q_{i+1} \cdots q_m$$

and, since $F[X]$ is an integral domain.

$$1 = uwq_1 \cdots q_{i-1}q_{i+1} \cdots q_m.$$

Since no q_i is a unit, we must have $m = 1$ and $p = uq_1$. Thus p and q are associates.

Suppose $n > 1$. The begining of the argument is similar. Since $uq_1 \cdots q_m \in \langle p_1 \rangle$, there is a unit w and a q_i such that $q_i = wp_1$. Then

$$p_1 \cdots p_n = uq_1 \cdots q_{i-1}(wp)q_{i+1} \cdots q_m$$

and, since $F[X]$ is an integral domain.

$$p_2 \cdots p_n = uwq_1 \cdots q_{i-1}q_{i+1} \cdots q_m.$$

By induction, $n - 1 = m - 1$ and we can renumber the q's as so that p_i and q_i are associates.

Putting together Lemma 9 Lemma 13 we prove that polynomial rings are UFDs.

Theorem 14 *If F is a field, then $F[X]$ is a unique factorization domain.*

Two Important Theorems

We won't give the proofs of these results in this course, but here are two very important theorems about PIDs and UFDs that you should know. The first is a generalization of Theorem 14. It says that every PID is a UFD.

Theorem 15 *If D is a principle ideal domain, then D is a unique factorization domain.*

Theorem 16 *If D is a unique factorization domain, then the polynomial ring $D[X]$ is also a unique factorization domain.*

Suppose D is a domain. We claim that $D[X,Y] = D[X][Y]$. Suppose

$$f(X,Y) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{i,j}X^iY^j \in D[X,Y].$$

For $j = 0,\ldots,m$ let $g_j(X) \in D[X]$ be the polynomial

$$g_j(X) = \sum_{i=0}^{n} a_{i,j}X^i.$$

Then

$$f(X,Y) = \sum_{j=1}^{m} g_j(X)Y^j \in D[X][Y].$$

Similarly if $f \in D[X][Y]$, by multiplying out we get a polynomial in $D[X,Y]$.

Similarly we can identify $D[X_1,\ldots,X_n] = D[X_1]\ldots[X_n]$. This allows us to inductively apply Theorem 16.

Corollary 17 *i) The polynomial ring $\mathbb{Z}[X_1,\ldots,X_n]$ is a unique factorization domain.*

ii) If F is a field, then the polynomial ring $F[X_1,\ldots,X_n]$ is a unique factorization domain.

Proof Since $\mathbb{Z}$ and $F[X_1]$ are unique factorization domains, Theorem 16 and induction tell us that $\mathbb{Z}[X_1,\ldots,X_n]$ and $F[X_1,\ldots,X_n]$.