POLYNOMIAL RINGS AND UNIQUE FACTORIZATION DOMAINS

RUSS WOODROOFE

1. Unique Factorization Domains

Throughout the following, we think of R as sitting inside $R[x]$ as the constant polynomials (of degree 0).

We recall that

Fact 1. *If F is a field, then $F[x]$ is a Euclidean domain, with $d(f) = \deg f$.*

but

Lemma 2. *$\mathbb{Z}[x]$ is not a PID.*

Proof. Consider the ideal $I = (2, x)$. If $I = (f)$, then since $2 \in I$ we have $2 = fg$. Since $\deg 2 = 0$, we must have $\deg f = 0$, and $f \mid 2$. Thus, the possibilities are $\pm 1, \pm 2$.

But the ideal generated by a unit is the entire ring, so $(1) = (-1) = \mathbb{Z}[x] \neq I$; and ± 2 does not divide x, so $x \notin (2)$ or (-2). It follows that I is not principal, and so that $\mathbb{Z}[x]$ is not a PID. □

This suggests

Question 3. *What structure does $\mathbb{Z}[x]$ have?*

To answer this question, we make a new definition. First, remember than an element a is *irreducible* or *prime* if $a = bc$ implies that either b or c is a unit.

Definition 4. A ring is a *unique factorization domain*, abbreviated UFD, if it is an integral domain such that

1. Every non-zero non-unit is a product of irreducibles.
2. The decomposition in part 1 is unique up to order and multiplication by units.

Thus, any Euclidean domain is a UFD, by Theorem 3.7.2 in Herstein, as presented in class.

Our goal is the following theorem.

Theorem 5. *If R is a UFD, then $R[x]$ is a UFD.*

First, we notice that if $a \in R$ is prime in R, then a is prime in $R[x]$ (as a degree 0 polynomial). For if $a = bc$ in $R[x]$, then $\deg b = \deg c = 0$, hence both b and c are in R, hence one is a unit.

This means that one class of irreducibles in $R[x]$ will be the irreducibles of R. To factor out these, we make the following definition.

Definition 6. A polynomial $f \in R[x]$ is *primitive* if $a \mid f$ for some $a \in R$ only if a is a unit.

Example 7. In $\mathbb{Z}[x]$, the polynomial $4x^2 - 2$ is not primitive, since it is divisible by 2; but $4x^2 - 3$ is primitive.

Lemma 8. *Let $f \in R[x]$ be primitive. Then f is irreducible if and only if f does not factor as a product of polynomials with positive degree.*

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) If $f = gh$ where g does not have positive degree, then $\deg g = 0$, hence $g \in R$, hence (since f is primitive) g is a unit. Thus, if the only factorizations of f have one term with degree 0, then f is irreducible. □

We give the following fact without proof:

Fact 9. *Gcds exist in UFDs.*

That gcds exist should not be too surprising: the idea is that you look at the factorizations of f and g, and take the common irreducible elements (up to units) for the gcd.

The following lemma then produces primitive polynomials for a factorization:

Lemma 10. *Let R be a UFD, and let $f \in R[x]$ be nonconstant (i.e., $\deg f > 0$). Then there is an $a \in R$ and a primitive polynomial $g \in R[x]$ such that $f = ag$.*

Proof. Let

$$f = a_0 + a_1 x + \cdots + a_n x^n,$$

and let $a = \gcd(a_0, a_1, \ldots, a_n)$. Then each $a_i = ab_i$, and if we take

$$g = b_0 + \cdots + b_n x^n$$

then $f = ag$. Furthermore, g is primitive, since if $p \in R$ divides $b_0, \ldots b_n$, then p divides $a_0, \ldots, a_n$, hence by the definition of gcd is a unit. □

Corollary 11. *Let R be a UFD. Then any non-zero non-unit in $R[x]$ is a product of irreducible elements. Each irreducible element is either an irreducible of R, or else a primitive polynomial that doesn't factor into two polynomials of positive degree.*

Proof. Induct on $\deg f$.

The base case is $\deg f = 0$. In this case, f is in R, and we are done since R is a UFD.

If $\deg f > 0$, then Lemma 10 gives $f = ag$ for $a \in R$ and g primitive. The element a factors as required (since R is a UFD), while Lemma 8 says that g is either irreducible, or else factors into two polynomials $g_0 g_1$ of smaller positive degree. By induction, g_0 and g_1 themselves factor into the desired form, hence g does, hence ag does. □

Let us review this proof on a high level. We take a polynomial $f \in R[x]$. It's possible that x has some irreducibles from R that we can factor out of it. If so, we do factor these irreducibles from R out, using Lemma 10. This leaves a primitive polynomial.

Then a primitive polynomial factors only into polynomials of smaller positive degree.

Thus, what we've done so far is:

(1) Shown that a factorization exists.
(2) Loosely described the form that this factorization takes.

Notice the similarity of part 1 with what we did with Euclidean domains – it is by looking at degree that we recognize irreducibles.

It remains to show that the factorization we've found is unique. The technique we use to do this will be to embed $R[x]$ in $F[x]$, and use the fact that $F[x]$ is a UFD (since its a Euclidean domain).

Recall that $\operatorname{Frac} R$ is the field of fractions of R, that is, all formal pairs $\frac{a}{b}$. $\operatorname{Frac} R$ is a field.

Example 12. $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$. Moreover, the construction of $\operatorname{Frac} R$ from R exactly mirrored that of $\mathbb{Q}$ from the integers!

Recall further that we think of R as sitting inside F via the embedding $a \mapsto \frac{a}{1}$. We can also think of $R[x]$ as sitting inside $F[x]$ by embedding each coefficient, that is,

$$a_0 + a_1 x + \cdots + a_n x^n \mapsto \frac{a_0}{1} + \frac{a_1}{1} x + \cdots + \frac{a_n}{1} x^n.$$

Lemma 13. *Let R be a UFD, let $f, g \in R[x]$, that f is primitive, and that $F = \operatorname{Frac} R$. If f divides g in $F[x]$, then f divides g in $R[x]$.*

Proof. If f divides g in $F[x]$, then $g = fh_F$ for some $h_F \in F[x]$. Since $h_F \in F[x]$, its coefficient of x^i has the form $\frac{a_i}{b_i}$. Let $b = \prod b_i$. Then, after cancelling, bh_F has 1 on the bottom of each coefficient, hence $bh_F \in R[x]$; and $bg = f \cdot bh_F$, so that f divides bg in $R[x]$.

Let c be the element of R with the minimal number of primes in its unique factorization such that f divides cg in $R[x]$, i.e., such that $cg = fh$ for some $h \in R[x]$. By the above argument, c exists. If c is a unit, then the proof is complete.

We will show that if c is not a unit, then we have a contradiction. For then some irreducible p in R divides c. Hence,

$$p \mid cg = fh,$$

and so p divides either f or ch. But since f is primitive, p does not divide f. And if p divides h, then $\frac{h}{p}$ is in R, hence $\frac{c}{p} g = f \frac{h}{p}$, and f divides $\frac{c}{p} g$. This contradicts the choice of c as having a minimal number of primes in its unique factorization. $\square$

Lemma 13 lets us prove a Theorem of Gauss in our general setting. Gauss's Lemma (Lemma 14) can also be found in Herstein as Theorem 3.10.1.

Corollary 14. (Gauss's Lemma)
Let R be a UFD, $F = \operatorname{Frac} R$. Suppose that $0 \neq f \in R[x]$ factors in $F[x]$ as $f = g_F h_F$. Then $f = gh$ for $g, h \in R[x]$, where $g = cg_F$ for some $c \in F$. Thus, $\deg g = \deg g_F$ and $\deg h = \deg h_F$.

Proof. We start out previously to the previous proof: let

$$g_F = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n,$$

and let $b = \prod b_i$, so that $bg_F \in R[x]$.

We then apply Lemma 10, which says that $bg_F = ag$ for some $a \in R$ and primitive $g \in R[x]$. Let $c = \frac{b}{a}$, and notice that $g = cg_F$.

Then $f = g \cdot \frac{1}{c}h_F$, i.e., g divides f in $F[x]$. Since g is primitive, Lemma 13 says that it also divides f in $R[x]$, as desired. □

We are now ready to prove our main result: that R a UFD $\implies R[x]$ a UFD.

Proof. (of Theorem 5)
Corollary 11 factors f in $R[x]$ into primes in R and irreducible primitive polynomials of positive degree, satisfying part 1 of the definition of UFD. We need to show that the factorization is unique. It suffices to show that it is unique for primitive polynomials.

Suppose that f is primitive, and factors into irreducibles as $f_1 \dots f_k$. Then each f_i is primitive, since if $c \in R$ divides f_i, then c divides f, hence c is a unit since f is primitive. Then Lemma 14 tells us that each f_i is irreducible in $F[x]$, where as usual $F = \operatorname{Frac} R$.

Since $F[x]$ is a UFD, the factorization $f = f_1, \dots f_k$ is unique in $F[x]$, hence unique in the smaller domain $R[x]$. □

Since $\mathbb{Z}$ is a UFD, we have found one answer to Question 3.

Corollary 15. *$\mathbb{Z}[x]$ is a UFD.*

We can also take polynomial rings in several variables, as discussed previously.

Corollary 16. *Let R be a UFD. Then $R[x_1, \dots, x_n]$ is also a UFD.*

Proof. Induct on n! $n = 0$ is R, which follows by hypothesis. But then $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$ by definition, and since $R[x_1, \dots, x_{n-1}]$ is a UFD by induction, Theorem 5 gives the result. □

This is especially important when R is a field or the integers.

Corollary 17. *If F is a field, then $F[x_1, \dots, x_n]$ is a UFD.*

Corollary 18. *$\mathbb{Z}[x_1, \dots, x_n]$ is a UFD.*

Remark 19. In your homework, you showed that the next stronger condition does <u>not</u> hold: $F[x_1, x_2]$ is not a PID.

2. The Eisenstein Criterion

The following Eisenstein Criterion will let us produce irreducible polynomials.

Theorem 20. (Eisenstein Criterion)
Let R be a UFD, $F = \operatorname{Frac} R$, and let $f \in R[x]$ with

$$f = a_0 + a_1 x + \cdots + a_n x^n.$$

If there is a prime $p \in R$ such that

(1) $p \nmid a_n$,
(2) $p \mid a_i$ *for* $0 \leq i < n$, *and*
(3) $p^2 \nmid a_0$,

then f is irreducible over $F[x]$.

Example 21. $3x^3 - 25x + 15$ is irreducible over $\mathbb{Q}[x]$, since 5 divides 25 and 15, but not 3; and 25 does not divide 15.

Proof. Let $\overline{R} = R/(p)$. Since (p) is a maximal ideal in R, $\bar{R}$ is a field. For $r \in R$, let $\overline{r}$ be the image of r mod (p); and for $g \in R[x]$, let $\overline{g}$ be the polynomial obtained from g by taking every coefficient mod (p). The map $g \mapsto \overline{g}$ is a homomorphism. (Check this!)

Suppose by contradiction that f factors as gh in $F[x]$. Then by Gauss's Lemma (Lemma 14), we can take $g, h \in R[x]$, where each of g and h has positive degree. Since we're in $R[x]$, we can map the factorization $f = gh$ into $\overline{R}[x]$: $\overline{f} = \overline{g}\overline{h}$.

But $\overline{f} = \overline{a_n} x^n \neq 0$, since p divides every coefficient of f except for a_n. Thus, $\overline{f}$ factors into irreducibles as $\overline{a_n} x \cdot x \cdot \cdots \cdot x$. Since $\overline{R}[x]$ is a UFD, this factorization is unique, and thus $\overline{g} = \overline{c} x^\ell$, and $\overline{h} = \overline{d} x^m$.

What are ℓ and m? We compare them with $\deg g$ and $\deg h$. It is obvious that $\ell \leq \deg g$ and $m \leq \deg h$. But then

$$\deg \overline{f} = \ell + m \leq \deg g + \deg h = \deg f$$

and since $\deg f = \deg \overline{f}$ (from above), we have that $\deg g = \ell$ and $\deg h = m$. In particular, $\ell, m > 0$.

Since the constant terms of $\overline{g}$ and $\overline{h}$ are 0, we must have that the constant terms of g and h are divisible by p. But the constant term of f is the product of the constant terms of g and h, hence divisible by p^2, giving us the desired contradiction. □

Example 22. $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Similarly for $x^n - p$, where p is a prime, etc.

Coming from the point of view of field extensions, Eisenstein's Criterion is useful because it gives us lots of irreducible polynomials over $F[x]$, hence lots of field extensions of F!

3. Face rings

Definition 23. An *(abstract) simplicial complex* Δ is a family of subsets of $[n]$ such that if $A \in \Delta$ and $B \subseteq A$, then $B \in \Delta$.

An element A of Δ is called a *face*, or an $(k-1)$-face if $|A| = k$.

Example 24. The $(n-1)$-*simplex* is the power set of $[n]$. We identify the 2-simplex with a triangle. The triangle itself (a 2-face) corresponds with [3]; its edges (1-faces) with $\{1,2\}$, $\{1,3\}$, and $\{2,3\}$; vertices with $\{1\}$, $\{2\}$, and $\{3\}$ (0-faces); and the empty set $\emptyset$ is a (-1)-face.

Similarly, we identify the 3-simplex with a tetrahedron; and n-simplexes with higher dimensional versions.

Fact 25. *An abstract simplicial complex has a "geometric realization" obtained by glueing together edges, triangles, tetrahedra, etc.*

Simplicial complexes are studied in both combinatorics and topology; in this note I will sketch a connection with ring theory. First, an easy lemma:

Lemma 26. *Let C be a non-face of Δ, that is, let $C \notin \Delta$. Then if $D \supseteq C$, then D is also a non-face of Δ.*

Proof. If D is a face, then the definition of simplicial complex tells us that C is also. □

We notice that non-faces are closed under adding elements, while ideals are closed under multiplication. We make a connection:

Definition 27. Let Δ be a simplicial complex on $[n]$. Consider $F[x_1, \ldots, x_n]$, and take the ideal

$$I = (\prod_{i \in C} x_i \,:\, C \text{ is a non-face of } \Delta).$$

Then

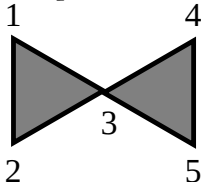
$$F[\Delta] \triangleq F[x_1, \ldots, x_n]/I$$

is the *face ring* of Δ.

Let us point out that the reason this is a good definition is: if C is a non-face, corresponding to a monomial $m_C = \prod_{i \in C} x_i$, then every product of m_C by some x_j corresponds to a larger subset, which is hence a non-face.

Remark 28. By the above discussion, I is in fact generated by the monomials corresponding to the non-faces that are minimal under inclusion.

Example 29. Let Δ be the following simplicial complex:



Then the minimal non-faces of Δ are $\{1,4\}$, $\{2,5\}$, $\{1,5\}$, $\{2,4\}$, $\{1,3,4\}$, and $\{2,3,4\}$. Thus,

$$F[\Delta] = F[x_1, \ldots, x_5]/(x_1x_4, x_2x_5, x_1x_5, x_2x_4, x_1x_3x_4, x_2x_3x_4).$$

Exercise 30. Let Δ be the simplicial complex $\{\{1\},\{2\}\}$. Show that $F[\Delta]$ is not a UFD. Is $F[\Sigma]$ a UFD for any simplicial complex Σ? Characterize such simplicial complexes.

Although we won't go far enough into either ring theory or topology to say very much about face rings, we note that many interesting properties of the topology and combinatorial geometry of Δ are encoded in the algebra of $F[\Delta]$.