Chapter 9, Additional topics for integral domains

Many times we have mentioned that theorems we proved could be done much more generally—they only required some special property like unique factorization, a division algorithm, or existence of $u,v$ such that $\gcd(m,n) = um + vn$. All of these things hold for the ring of integers and for a polynomial ring in one variable over a field. This chapter takes the idea of integral domain (commutative, no zero divisors) from Chapter 3 and adds more axioms to talk about general classes of rings which have properties like the ones above. It begins with the notion of a Euclidean domain, an integral domain in which there is some sort of division algorithm, and hence a Euclidean algorithm. For these rings, virtually everything we have done previously will still hold because most of it ultimately depended on the Euclidean algorithm. After this, we will slowly weaken the axioms and see how much still holds. With the least powerful systems of axioms, we will be particularly interested in polynomials in several variables, which we paid little attention to in Chapter 3. Other interesting examples come from subrings of the complex numbers called number rings—finitely generated rings containing the integers in which each element satisfies a monic polynomial with integer coefficients. Examples are the rings $\mathbb{Z}[\sqrt{d}]$ for $d \in \mathbb{Z}$, and in particular the Gaussian integers $\mathbb{Z}[i]$.

Throughout this chapter, $R$ denotes an integral domain. Recall the definitions of $a|b$ for $a,b$ nonzero elements of $R$, unit, associate and irreducible. (This is different than prime in general, but not in any of our more restrictive axiom systems to be looked at.)

**Definition.** $R$ is a **Euclidean domain** if there is a function $\delta: R \setminus \{0\} \to \mathbb{N}$ satisfying
(i) If $a,b \in R \setminus \{0\}$, then $\delta(a) \leq \delta(ab)$.
(ii) If $a,b \in R$ with $b \neq 0$, then there exist $q,r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$

Examples we have seen are $\delta = \deg$ for $F[x]$, when $F$ is a field, and $\delta(a) = |a|$ for $\mathbb{Z}$. Sometimes number rings are Euclidean domains, but not always. It will be easier to show the “not always” later, but we now show that the Gaussian integers are a Euclidean domain using the **norm** $\delta(x + yi) = x^2 + y^2$. (norm has a general definition in field theory—we must wait for that.) We first show that $\delta(ab) = \delta(a)\delta(b)$. Let $a = x + yi$, $b = s + ti$. Then

$$\delta(ab) = \delta((xs - yt) + (xt + ys)i) = (xs - yt)^2 + (xt + ys)^2$$
$$= \cdots = (x^2 + y^2)(s^2 + t^2) = \delta(a)\delta(b).$$

In particular, if $b \neq 0$, then $\delta(a) = \delta(a) \cdot 1 \leq \delta(a)\delta(b)$ and (i) holds. Now check (ii). We know that $\mathbb{Q}[i]$ is a field, so $a/b = c + di$ for some $c,d \in \mathbb{Q}$. Let $m,n$ be the closest integers to $c,d$, respectively; hence $|m - c| \leq \frac{1}{2}$ and $|n - d| \leq \frac{1}{2}$. Setting $q = m + ni$ and
\[ r = b[(c - m) + (d - n)i], \text{ we have} \]
\[
\begin{align*}
a &= b[c + di] \\
&= b[(m + ni) + (c - m) + (d - n)i] \\
&= b[m + ni] + b[(c - m) + (d - n)i] \\
&= bq + r
\end{align*}
\]

Here \( r = a - bq \in \mathbb{Z}[i] \) and
\[
\delta(r) = \delta(b)\delta((c - m) + (d - n)i) = \delta(b)((c - m)^2 + (d - n)^2) \leq \delta(b)(\frac{1}{4} + \frac{1}{4}) = \delta(b)/2 < \delta(b),
\]
so (ii) holds.

While we used the division algorithm extensively in our proofs in Chapters 1–5, it was actually a stronger condition than we really needed. In this chapter we shall see that most everything we want will also work for PID’s.

**Definition.** A **principal ideal domain (PID)** is an integral domain in which every ideal is principal.

**Theorem 9.8.** *Every Euclidean domain is a PID.*

**Proof.** Let \( I \) be a nonzero ideal in a Euclidean domain \( R \). The set of nonnegative integers \( \{ \delta(a) \mid a \in I \} \) has a smallest element by the well-ordering axiom, say \( \delta(b) \), \( b \in I \). We will show that \( b \) generates \( I \). Clearly \( \langle b \rangle \subseteq I \); conversely, suppose \( a \in I \). Then there exist \( q, r \in R \) such that \( a = bq + r \) and either \( r = 0 \) or \( \delta(r) < \delta(b) \). But \( r = a - bq \in I \), so we must have \( r = 0 \) by our choice of \( b \). Therefore \( a = bq \in I \) and \( I = \langle b \rangle \) is principal. \( \square \)

The converse is false, but hard to show. An example is \( \mathbb{Z}[\sqrt{-19}] \). It isn’t too hard to show that \( \mathbb{Z}[\sqrt{-d}], d > 0, \) is a Euclidean domain using the norm if \( d = 1, 2, 3, 7 \) or \( 11 \) with a proof by contradiction. But it is much harder to show that \( \mathbb{Z}[\sqrt{-19}] \) is a PID. It turns out that \( \mathbb{Z}[\sqrt{d}], d > 0, \) is a Euclidean domain using the norm if and only if \( d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 \) or \( 73 \). But it is not known if there exists another Euclidean domain using some other function \( \delta \). Generally, if number rings are not PID’s, it is proved by showing that they lack the weaker property of unique factorization—the next major thing we want to prove about PID’s.

**Lemma 9.9.** *Let \( a, b \in R \). (Recall that \( R \) is always an integral domain unless specified to be even more restrictive.) Then*

1. \( (a) \subseteq (b) \) if \( b \mid a \). (note misprint in book)
2. \( (a) = (b) \) if \( b \mid a \) and \( a \mid b \).
3. \( (a) \nsubseteq (b) \) if \( b \mid a \) and \( b \) is not an associate of \( a \).
Proof. \( a \in (b) \) implies \( a \) is a multiple of \( b \), so \( b \mid a \). Conversely, if \( b \mid a \), then \( a \) is a multiple of \( b \) and \( a \in (b) \). Since \((a)\) is the smallest ideal containing \( a \) and \((b)\) is an ideal, it follows that \( a \in (b) \) iff \((a) \subseteq (b)\), proving (1).

(2) is just a double application of (1) since \((a) = (b)\) iff each is a subset of the other.

(3) is a combination of (1) and (2). \((a) \subseteq (b) \iff (a) \subseteq (b) \wedge (a) \neq (b) \iff b \mid a \) and \( a \nmid b \iff b \mid a \) and they are not associates. □

Definition. A ring \( R \) satisfies the **ascending chain condition (ACC)** on principal ideals if whenever we have a chain of ideals \((a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots\), there exists a positive integer \( n \) such that \((a_i) = (a_n)\) for all \( i \geq n\).

From our knowledge of divisibility of integers, we see that Lemma 9.9 shows us that \( \mathbb{Z} \) has ACC on principal ideals. ACC on all ideals also turns out to be a very important property in ring theory, but we shall not pursue it in this class.

**Lemma 9.10.** Every PID \( R \) satisfies ACC on principal ideals.

**Proof.** Let \((a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots\) be an ascending chain of ideals in \( R \). Let \( I = \bigcup (a_i) \). Let \( x, y \in I, r \in R \); then \( x \in (a_j), y \in (a_k) \) for some \( j, k \). But then \( x + y \) and \( rx \) lie in \((a_{\max(j,k)}) \subseteq I\). Therefore \( I \) is an ideal. Since \( R \) is a PID, \( I = (a) \) for some \( a \in R \). But then \( a \in \bigcup (a_i) \), so \( a \) lies in some \((a_n)\). This implies that all \((a_i) = (a) = (a_n)\) for \( i \geq n \). □

**Lemma 9.11.** Let \( R \) be a PID and let \( p \in R \) be irreducible. If \( p \mid (bc) \), then \( p \mid b \) or \( p \mid c \) (that is, \( p \) is a prime ideal).

**Proof.** We prove more. We will show \((p)\) is maximal, hence prime. Assume \( I \) is an ideal with \((p) \subseteq I \subseteq R\). Since \( R \) is a PID, we know that \( I = (a) \) for some \( a \in R \), and so \( a \mid p \). Write \( p = ar \); since \( p \) is irreducible, either \( a \) is a unit (and \( I = R \)) or \( r \) is a unit (and \( I = (p) \)). Therefore \((p)\) is maximal. □

Definition. An integral domain \( R \) is a **unique factorization domain (UFD)** if every nonzero, nonunit element of \( R \) is a product of irreducible elements and the factorization is unique up to order and associates.

**Theorem 9.12.** Every PID is a UFD.

**Proof.** Let \( a \neq 0 \) be a nonunit in a PID \( R \). Assume that \( a \) is not a product of irreducibles. Then \( a \) itself must be reducible, so \( a = a_1b_1 \) for some nonunits \( a_1 \) and \( b_1 \). If both \( a_1 \) and
are products of irreducibles, then so is \( a \), hence one of them, say \( a_1 \) is not a product of irreducibles. Furthermore, since \( b_1 \) is a nonunit, \( a \) and \( a_1 \) are not associates and Lemma 9.9 tells us that \( (a) \nsubseteq (a_1) \). Now iterate the process: write \( a_1 = a_2 b_2 \), where \( a_2 \) and \( b_2 \) are nonunits and \( a_2 \) is not a product of irreducibles. Then \( (a_1) \nsubseteq (a_2) \). Continuing, we obtain a sequence of ideals \( (a) \nsubseteq (a_1) \nsubseteq (a_2) \nsubseteq \cdots \) contradicting the ACC on principal ideals for PID’s. Thus \( a \) must have a factorization into irreducibles. The uniqueness of the factorization is proved the same way as for \( \mathbb{Z} \) and \( F[x] \). (Assume two factorizations are equal and cancel elements one at a time...) \( \square \)

We have seen rings such as \( \mathbb{R}[x, y] \) and \( \mathbb{Z}[x] \) which have unique factorization but are not PID’s. (The maximal ideals \( (x, y) \subseteq \mathbb{R}[x, y] \) and \( (2, x) \subseteq \mathbb{Z}[x] \) are not principal.) But we really have not seen unique factorization fail in an integral domain (where it has a chance of holding, which it does not if there are zero divisors). We shall look at two examples and see it fail two different ways. In the first, we violate the ACC, so that elements can be repeatedly factored further, never reaching an end. In the second, we shall have factorization into irreducibles, but it will not be unique.

Example (page 299). Let

\[
R = \{ a_0 + a_1 x + \cdots + a_n x^n \mid n \geq 0, \ a_0 \in \mathbb{Z}, \ a_k \in \mathbb{Q} \text{ for } k > 0 \}.
\]

Note that (1) \( R \) is a ring (since constant terms add and multiply each other in doing ring operations) and (2) \( R \) has no zero divisors (since it is a subring of \( \mathbb{Q}[x] \)). Now we try factoring the nonunit \( x \):

\[
x = 2 \cdot \left( \frac{1}{2} x \right) = 2 \cdot 2 \cdot \left( \frac{1}{4} x \right) = 2 \cdot 2 \cdot 2 \cdot \left( \frac{1}{8} x \right) \cdots ,
\]

where neither \( 2 \) nor \( \frac{1}{2} x \) is a unit. The element 2 is irreducible, but we are seeing that for any \( n \in \mathbb{Z} \), \( \frac{1}{n} x = 2 \cdot \left( \frac{1}{2n} x \right) \) is not irreducible. Thus we never get \( x \) as a product of irreducibles. If we look at the corresponding chain of ideals, this says

\[
(x) \nsubseteq \left( \frac{1}{2} x \right) \nsubseteq \left( \frac{1}{4} x \right) \nsubseteq \left( \frac{1}{8} x \right) \cdots
\]

Example (page 309). Next we work with the number ring \( R = \mathbb{Z}[\sqrt{-5}] \) and get a little taste of algebraic number theory. As with the Gaussian integers, we work with the norm, \( N(x + y\sqrt{-5}) = x^2 + 5y^2 \). A similar computation shows that \( N(ab) = N(a)N(b) \) for any \( a, b \in R \). (This works for any \( \mathbb{Z}[\sqrt{d}] \), \( d \) square free, by Theorem 9.19.) We can use \( N \) to determine the units in \( R \); for if \( ab = 1 \), then \( N(a)N(b) = N(1) = 1 \), so either \( N(a) = N(b) = 1 \) or \( N(a)N(b) = -1 \). The converse is also true. If \( u = x + y\sqrt{-5} \) and
\[ N(u) = \pm 1, \text{ then } u\bar{u} = (x + y\sqrt{-5})(x - y\sqrt{-5}) = N(u) = \pm 1, \text{ so either } \bar{u} \text{ or } -\bar{u} \text{ is the inverse of } u. \]

Now \( N(x + y\sqrt{-5}) = x^2 + 5y^2 = \pm 1 \) iff \( x = \pm 1, \ y = 0, \) so we happen to have the same units in \( R \) as in the integers. To see that \( R \) lacks unique factorization, we will show there is an element with two distinct factorizations into irreducibles, namely

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \]

We need to check that the four elements \( 2, 3, 1 \pm \sqrt{-5} \) are all irreducible. We already see that \( 2, 3 \) are not associates of \( 1 \pm \sqrt{-5} \) since the only units are \( \pm 1. \) We can check for irreducibility using the norm. \( 2, 1 + \sqrt{-5} \) are done in the book, so we do the other two. If \( 3 = ab \) is a factorization into nonunits, then \( 9 = N(3) = N(a)N(b). \) But 9 has the unique factorization \((\pm 3)^2 \) in \( \mathbb{Z}, \) hence we must have \( N(a) = \pm 3. \) (We can’t use \( 1 \cdot 9 \) as that makes \( a \) or \( b \) a unit.) Looking at the definition of the norm, we see that \( N(a) = \pm 3 \) is impossible, and therefore \( 3 \) is irreducible. Similarly, if \( 1 - \sqrt{-5} = ab \) is a factorization into nonunits, then \( 6 = N(1 - \sqrt{-5}) = N(a)N(b), \) which implies that \( N(a), N(b) \) must be \( \pm 2, \pm 3. \) But we have already seen that \( \pm 3 \) is impossible, and therefore \( 1 - \sqrt{-5} \) is also irreducible.

**Unique factorization domains.**

Theorem 9.13 belabors the obvious: in a UFD, \( a \mid b \) iff in the factorizations, each irreducible \( p \) in the factorization of \( a \) occurs to at least as high a power in the factorization of \( b, \) but possibly as an associate \( up \) for some unit \( u. \) In working with specific examples, it is handy to be able to pick a single associate for each irreducible, such as the positive primes in \( \mathbb{Z} \) or the monic irreducible polynomials in \( F[x]. \)

**Corollary 9.14.** Every UFD satisfies ACC on principal ideals.

*Proof.* Let \( R \) be a UFD, \( a_k \in R \) with \((a_1) \subset (a_2) \subset (a_3) \subset \cdots. \) Then for each \( k = 2, 3, \ldots, \) \( a_k \mid a_{k-1} \) and they are not associates by Lemma 9.9. Now consider the factorization of \( a_1 \) into irreducibles. There are only a finite number, say \( n, \) in the factorization. Each \( a_k \mid a_1, \) so at each step \( a_k \) involves only some subset of the irreducibles of \( a_1. \) And since \( a_k \) and \( a_{k-1} \) are not associates, \( a_k \) has at least one less of the irreducibles. After at most \( n \) such steps, we can have no irreducibles left and the remainder of the \( a_k \)’s must be units, giving \((a_k) = R \) and contradicting the assumption that the chain inclusions must be proper. \( \square \)

We say that a nonzero element \( a \) of \( R \) is **prime** if the ideal \((a)\) is a prime ideal. This is equivalent to saying that if \( a \) divides \( bc, \) then \( a \) divides \( b \) or \( a \) divides \( c \) (by the definition of prime ideal). By homework problem 21, page 294, a prime element of an integral domain is always irreducible.
Theorem 9.15. Irreducible elements in a UFD are prime.

Proof. Let $p$ be irreducible and assume $p|ab$; i.e., $pt = ab$ for some $t \in R$. We must show that $p|a$ or $p|b$. This is clear if $a$ or $b$ is 0, so assume they are not. Since $p$ is not a unit, $a, b$ cannot both be units. If one, say $a$, is a unit, then $a^{-1}pt = b$ implies $p|b$. If both are nonunits, factor them into irreducibles: $a = q_1 \cdots q_r$ and $b = q_{r+1} \cdots q_n$. Then $pt = q_1 \cdots q_n$. By uniqueness of factorizations, some associate of $p$ occurs on the right hand side, say $q_i$. Then $p$ divides either $a$ or $b$, the one which has $q_i$ as a factor. \[\Box\]

What is really interesting is that these last two properties of UFD’s completely characterize them.

Theorem 9.16. An integral domain $R$ is a UFD iff

1. $R$ satisfies ACC on principal ideals; and
2. every irreducible element of $R$ is prime.

Proof. We have already seen that (1) implies the existence of a factorization. This was the way we proved that PID’s have a factorization. Furthermore, we have seen that (2) implies that factorizations, if they exist, are unique. The proof is the same as we have done for $\mathbb{Z}$ and $F[x]$. \[\Box\]

Our examples above show that each of these conditions is needed. The polynomial ring with integer constant terms and rational coefficients otherwise failed to satisfy (1), and hence had no factorization for the element $x$. The ring $\mathbb{Z}[\sqrt{-5}]$ satisfied (1) but not (2) and so had factorizations, but they were not necessarily unique.

Definition. A greatest common divisor of $a_1, \ldots, a_n$ in an integral domain $R$ is an element $d \in R$ such that $d|a_i$ for all $i = 1, \ldots, n$ and if $c \in R$ divides all $a_i$’s, then $c|d$.

This is equivalent to our earlier definitions, as proved in theorems for $\mathbb{Z}$ and $F[x]$. This is the best we can do in general for a meaning for “greatest”. There is also no way to make a choice among possible gcd’s to choose a unique one (positive for $\mathbb{Z}$ and monic for $F[x]$). Thus there may be more than one gcd, but they are all associates: clearly any associate of a gcd again satisfies the 2 conditions. On the other hand, if we have $d_1, d_2$ both gcd’s of $a_1, \ldots, a_n$, then they must each divide the other, and hence are associates.

Theorem 9.18. Nonzero elements in a UFD always have a gcd.

Proof. Factor each of the elements into a product

\[a_i = u_ip_1^{e_{i1}} \cdots p_t^{e_{it}} \quad (i = 1, \ldots, n)\]
where \( u_i \) is a unit and \( p_1, \ldots, p_t \) are irreducible. Note that we may assume they all have a common number \( t \) by allowing some \( e_{ij} = 0 \) and we may assume all use the same set of nonassociate irreducibles by putting the other factors into the units \( u_i \). Then a gcd is \( p_1^{f_1} \cdots p_t^{f_t} \) where \( f_j = \min(e_{1j}, \ldots, e_{nj}) \). □

In general, we may not be able to write \( \gcd(a, b) \) as a linear combination of \( a, b \) even in a UFD: consider \( 2, x \) in \( \mathbb{Z}[x] \) with gcd 1. You can always do so in a PID (homework). If you do not have a UFD, you may not even have a gcd. As an example, look at \( 6, 2(1 + \sqrt{-5}) \in R = \mathbb{Z}[\sqrt{-5}] \). Any common divisor will have a norm dividing both \( N(6) = 36 \) and \( N(2 + 2\sqrt{-5}) = 24 \), so the norm is 1, 2, 3, 4, 6 or 12. But it must also have the form \( x^2 + 5y^2 \), so must be 1, 4 or 6. 1 gives a unit, so isn’t useful, so common divisors have norm 4 or 6. We have already seen that 2 and \( 1 + \sqrt{-5} \) are common divisors and this shows there are no others other than associates (multiply by \(-1\)). But these two numbers are not associates and neither divides the other. Thus there are common divisors, but no greatest common divisor.

You expect from experience that rings such as \( \mathbb{Z}[x] \) and \( \mathbb{R}[x, y] \) have unique factorization, but we have not proved it. In general, the theorem says that if \( R \) is a UFD, then so is \( R[x] \). The proof is basically done by first embedding \( R \) in a field of quotients \( F \) (like \( \mathbb{Z} \) in \( \mathbb{Q} \)) where we know \( F[x] \) is a UFD. And then using Gauss’ lemma (generalized to our current situation) to say we can also factor over \( R \). To carry this out, we first need to do the construction of a field of quotients for any integral domain.

**Fields of quotients.**

Let \( R \) be an integral domain. We define a relation on ordered pairs in \( S = \{ (a, b) \in R \times R \mid b \neq 0 \} \) by

\[
(a, b) \sim (c, d) \iff ad = bc.
\]

Check that this is an equivalence relation (see Theorem 9.25). Denote the equivalence class of \( (a, b) \) by \( \frac{a}{b} \) and let \( F \) be the set of all equivalence classes.

**Theorem 9.30.** \( F \) is a field with the operations defined by

\[
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.
\]

\( F \) has the property that

\[
\frac{a}{b} = \frac{c}{d} \iff ad = bc \text{ in } R
\]

and \( R \) is isomorphic to the set of elements in \( F \) of the form \( \frac{r}{1} \) for \( r \in R \).
We call $F$ the field of quotients or field of fractions of $R$. Examples you are familiar with are the construction of $\mathbb{Q}$ from $\mathbb{Z}$ and of rational functions over a field $F$, namely $F(x) = \left\{ \frac{f(x)}{g(x)} \middle| g(x) \neq 0 \right\}$, as quotients of polynomials. The field of quotients is the smallest field containing $R$ in the following sense.

**Theorem 9.31.** Let $R$ be an integral domain and $F$ its field of quotients. If $K$ is any field containing $R$, then $K$ contains a subfield which contains $R$ and is isomorphic to $F$.

**Proof.** Define a mapping $f: F \to K$ by $f(a/b) = ab^{-1}$ which lies in $K$ since $K$ is a field. Since $a/b$ is an equivalence class, we need to check that $f$ is well-defined; indeed, assume that $a/b = c/d$, so $ad = bc$ in $R \subseteq K$. Then $f(a/b) = ab^{-1} = cd^{-1} = f(c/d)$ and $f$ is well-defined. We also need to check that $f$ is a homomorphism. For $a/b, c/d \in F$, we have $f(a/b + c/d) = f((ad + bc)/bd) = (ad + bc)(bd)^{-1} = ab^{-1} + cd^{-1} = f(a/b) + f(c/d)$ and $f(a/b \cdot c/d) = f((ac)/(bd)) = ac(bd)^{-1} = ab^{-1}cd^{-1} = f(a/b)f(c/d)$. Now $\ker f = 0$ since the only other ideal of the field $F$ is $F$ itself, so $f$ is injective, and hence an isomorphism onto its image in $K$. 

Exercise 12 of page 322 is an important thing to know. Recall that an integral domain is said to be of characteristic zero if no sum of copies of 1 is ever zero. Equivalently, this happens if the homomorphism $\mathbb{Z} \to R$ defined by $n \mapsto n \cdot 1_R$ has kernel $(0)$, so $\mathbb{Z}$ is isomorphic to a subring of $R$. In particular, a field of characteristic 0 contains a copy of $\mathbb{Z}$, and therefore a copy of $\mathbb{Q}$ by Theorem 9.31. This will be a useful fact when we study fields in the next chapter.

**Unique factorization domains revisited.**

Let $R$ be a UFD. Our goal is to prove that $R[x]$ is also a UFD. The main tool we still need is Gauss’s lemma which says that if we can factor a polynomial into polynomials with coefficients from the field of quotients, then we can actually factor it with polynomials from $R[x]$ of the same degrees. You might recall that we did this for $\mathbb{Z}$ and it was just a matter of factoring out common denominators and getting them to cancel. This is true in general, but we now need to be a bit more careful and will do it from scratch.

Recall from Chapter 4 that the units of $R[x]$ are the units in $R$. Furthermore, the irreducible elements of $R$ are precisely the irreducible constant polynomials of $R[x]$: ($\Leftarrow$) is clear; if $p \in R$ is irreducible and $p = f(x)g(x)$ in $R[x]$, then $0 = \deg p = \deg f + \deg g$, so $f, g$ also lie in $R$. Since $p$ is irreducible, either $f$ or $g$ must be a unit, so $p$ is also irreducible in $R[x]$.

Our main interest is in factoring polynomials, not the coefficients from $R$; we say a polynomial is primitive if the only constants that divide it are the units. Example:
2x^2 + 4 \in \mathbb{Z}[x] \text{ can be written as } 2(x^2 + 2) \text{ where } x^2 + 2 \text{ is primitive. Since } R \text{ is a UFD, we can always factor out the gcd of the coefficients: if } 0 \neq f(x) \in R[x], \text{ then } f(x) = cg(x) \text{ where } c \in R \text{ is the gcd of the coefficients of } f(x) \text{ and } g(x) \text{ is primitive.}

**Lemma 1.** Let \( F \) be the field of quotients of \( R \), \( 0 \neq f(x) \in F[x] \). Then \( f(x) = dg(x) \) where \( d \in F \) and \( g(x) \) is a primitive polynomial in \( R[x] \). This factorization is unique up to multiplication by units in \( R \).

**Proof.** Let \( f(x) = r_0 + r_1x + \cdots + r_nx^n \), where \( r_i \in F \), \( r_n \neq 0 \). Write each \( r_i = a_i/b_i \), with \( a_i, b_i \in R \). Set \( b = \prod b_i \), so \( bf(x) \in R[x] \). Then we can write \( bf(x) = cg(x) \) where \( c \in R \) and \( g(x) \in R[x] \) is primitive. Then \( d = c/b \) gives the desired factorization. To check uniqueness, assume that we also have \( f(x) = d_1g_1(x) \) with \( d_1 \in F \) and \( g_1(x) \) a primitive polynomial in \( R[x] \). Write \( d_1 = st^{-1} \) with \( s, t \in R \). Therefore \( ctg(x) = sbg_1(x) \). Since the gcd of the coefficients is determined uniquely up to associates, \( ct \) and \( sb \) must be associates. That is, \( ct = usb \) for some unit \( u \in R \), and so \( d = ud_1 \). It follows that \( g(x) = u^{-1}g_1(x) \), and we obtain the desired uniqueness. \( \square \)

**Corollary 9.36.** If primitive polynomials of \( R[x] \) are associates in \( F[x] \), then they are associates in \( R[x] \).

**Proof.** If \( f(x) = ag(x) \) with \( f, g \) primitive and \( a \in F \), then the uniqueness of \( a \) from Lemma 1 shows that \( a \) is a unit in \( R \). \( \square \)

**Gauss’s Lemma.** The product of primitive polynomials is primitive. (This is a more common way to state it than the one given last semester. See below.)

**Proof.** Suppose \( f(x), g(x) \) are primitive but \( h(x) = f(x)g(x) \) is not. Then it is divisible by some irreducible \( p \in R \), but \( p \nmid f(x) \) and \( p \nmid g(x) \). Since \( R \) is a UFD, \((p)\) is a prime ideal, and hence \( R/(p) \) is an integral domain. Consider the homomorphism \( \phi: R[x] \to R/(p)[x] \) obtained by just reducing all coefficients modulo \( p \). \( R/(p)[x] \) is again an integral domain by Corollary 4.3. But the image of \( h(x) \) is zero while the images of \( f \) and \( g \) are nonzero, a contradiction of \( R/(p)[x] \) being an integral domain. \( \square \)

To relate this to last semester’s statement, we show that it implies:

**Corollary 9.37.** If \( f(x) \in R[x] \) has positive degree and is irreducible, then it is also irreducible in \( F[x] \). (Or the contrapositive, if it factors over \( F \), then it factors over \( R \).)

**Proof.** Since \( f(x) \) is irreducible, it is primitive. Assume it factors as \( f(x) = g(x)h(x) \) with \( g(x), h(x) \in F[x] \) of degree at least 1. Write \( g(x) = cg_1(x), h(x) = dh_1(x) \), where
c, d ∈ F and g₁, h₁ are primitive polynomials in R[x]. Then \( f(x) = (cd)(g₁(x)h₁(x)) \) where \( g₁(x)h₁(x) \) is primitive by Gauss’s Lemma. It follows that \( cd \) is a unit in \( R \), contradicting the irreducibility of \( f(x) \) in \( R[x] \).

**Theorem 9.38.** If \( R \) is a UFD, then so is \( R[x] \).

**Proof.** Let \( f(x) \in R[x] \) be nonzero and not a unit. We use induction on the degree of \( f \). If \( \deg f(x) = 0 \), then \( f \in R \) and we have unique factorization by the hypothesis on \( R \). Assume the degree is positive. Write \( f(x) = df₁(x) \) with \( f₁(x) \) primitive. If \( f₁(x) \) is not irreducible, we can factor it as \( g₁(x)g₂(x) \), with \( 1 \leq \deg g₁(x) < \deg f(x) \). By the induction hypothesis, each \( gᵢ(x) \) can be factored into irreducibles, hence \( f₁(x) \) can also. Factor \( d \) as well, and we have a factorization of \( f(x) \).

Uniqueness is the part that needs Gauss’s lemma. So consider two factorizations of \( f(x) \),

\[
c₁ \cdots cₘp₁(x)\cdots pₙ(x) = d₁ \cdots dₙq₁(x)\cdots qₜ(x),
\]

where \( cᵢ, dᵢ \in R \) are irreducible and \( pᵢ(x), qⱼ(x) \) are irreducible polynomials of positive degree (and hence primitive). By Gauss’s lemma, \( p₁(x)\cdots pₙ(x) \) and \( q₁(x)\cdots qₜ(x) \) are primitive, so Lemma 1 says \( c₁ \cdots cₘ \) and \( d₁ \cdots dₙ \) are associates as are the products of polynomials. Since \( R \) is a UFD, we see that \( m = n \) and with relabeling, each \( cᵢ \) is an associate of \( dᵢ \). Let \( F \) be the field of quotients of \( R \). Unique factorization in \( F[x] \) shows that \( s = t \) and, after relabeling, each \( pᵢ(x) \) is an associate of \( qⱼ(x) \) in \( F[x] \). By Corollary 9.36, they are actually associates in \( R[x] \), so we are done.

**Isomorphism theorems.**

We end our study of ring theory by doing the second and third isomorphism theorems, which were left out last semester. Since they say essentially the same thing as in group theory, the main thing still needed is to check that they work with the multiplication as well as the addition. \( R \) is now an arbitrary ring, not necessarily having an identity element. In terms of our understanding of group theory, an ideal can now be thought of as a subgroup of the additive group of the ring which is also closed under multiplication by elements of \( R \).

**Second Isomorphism Theorem.** Let \( I, J \) be ideals in \( R \). Then \( I \cap J, I + J \) are ideals of \( R \) and

\[
\frac{I}{I \cap J} \cong \frac{I + J}{J}.
\]

**Proof.** From group theory we know that \( I \cap J, I + J \) are additive subgroups of \( R \) and such an isomorphism holds as groups (Second Isomorphism Theorem for groups). Let
Theorem.

Let \( K \subseteq I \) be ideals in \( R \). Then \( I/K \) is an ideal in \( R/K \) and

\[
\frac{R/K}{I/K} \cong R/I.
\]

Proof. Again we know that everything works for additive groups, with the mapping \( R/K \to R/I \) being surjective with kernel \( I/K \). The only thing left to prove is that the additive groups are actually ideals and the mapping is a ring homomorphism, so that the First Isomorphism Theorem for rings gives the desired isomorphism of rings. We know from Theorem 7.43 that \( I/K \) is a subgroup of \( R/K \). But, for \( r \in R \), \( x \in I \),

\[
(r + K)(x + K) = rx + K \in I/K
\]

(and similarly for multiplication on the right), so \( I/K \) is an ideal of \( R/K \). Also, the (group) homomorphism \( f: R/K \to R/I \) satisfies

\[
f((r + K)(s + K)) = f(rs + K) = rs + I = (r + I)(s + I) = f(r + K)f(s + K)
\]

for any \( r, s \in R \), hence is a ring homomorphism. \( \square \)