Course Notes for MAT 612: Abstract Algebra II

Dana C. Ernst, PhD
Northern Arizona University

Spring 2016

Contents

1 Ring Theory

1.1 Definitions and Examples

This section of notes roughly follows Sections 7.1–7.3 in Dummit and Foote.

Recall that a group is a set together with a single binary operation, which together satisfy a few modest properties. Loosely speaking, a ring is a set together with two binary operations (called addition and multiplication) that are related via a distributive property.

Definition 1.1. A **ring** R is a set together with two binary operations $+$ and $\times$ (called **addition** and **multiplication**, respectively) satisfying the following:

(i) $(R, +)$ is an abelian group.

(ii) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$.

(iii) The **distributive property** holds: $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$ for all $a, b, c \in R$.

Note 1.2. We make a couple comments about notation.

(1) We write ab in place $a \times b$.

(2) The additive inverse of the ring element $a \in R$ is denoted $-a$.

Theorem 1.3. Let R be a ring. Then for all $a, b \in R$:

(1) $0a = a0 = 0$

(2) $(-a)b = a(-b) = -(ab)$

(3) $(-a)(-b) = ab$

Definition 1.4. A ring R is called **commutative** if multiplication is commutative.

Definition 1.5. A ring R is said to have an **identity** (or called a **ring with 1**) if there is an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Theorem 1.6. If R is a ring with 1, then the multiplicative identity is unique and $-a = (-1)a$.

Question 1.7. Requiring $(R, +)$ to be a group is fairly natural, but why require $(R, +)$ to be abelian? Here's one reason. Suppose R has a 1. Compute $(1 + 1)(a + b)$ in two different ways.

Definition 1.8. A ring R with 1 (with $1 \neq 0$) is called a **division ring** if every nonzero element in R has a multiplicative inverse: if $a \in R \setminus \{0\}$, then there exists $b \in R$ such that $ab = ba = 1$.

Definition 1.9. A commutative division ring is called a **field**.

Definition 1.10. A nonzero element a in a ring R is called a **zero divisor** if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

Theorem 1.11 (Cancellation Law)**.** Assume $a, b, c \in R$ such that a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$.

Definition 1.12. Assume R is a ring with 1 with $1 \neq 0$. An element $u \in R$ is called a **unit** in R if u has a multiplicative inverse (i.e., there exists $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Theorem 1.13. If $R^\times \neq \emptyset$, then $R^\times$ forms a group under multiplication.

Note 1.14. We make a few observations.

(1) A field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F \setminus \{0\}$.

(2) Zero divisors can never be units.

(3) Fields never have zero divisors.

Definition 1.15. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

Note 1.16. The Cancellation Law (Theorem 1.11) holds in integral domains for any three elements.

Corollary 1.17. Any finite integral domain is a field.

Proof. For any nonzero $a \in R$, define $f_a : R \to R$ via $f_a(x) = ax$. If R is an integral domain, the Cancellation Law forces f_a to be injective. If R is finite, then f_a is also surjective. In this case, there exists $b \in R$ such that $ab = 1$. □

Example 1.18. Here are some examples of rings. Details left as an exercise.

(1) **Zero Ring**: If $R = \{0\}$, we can turn R into a ring in the obvious way. The zero ring is a finite commutative ring with 1. It is the only ring where the additive and multiplicative identities are equal. The zero ring is not a division ring, not a field, and not an integral domain.

(2) **Trivial Ring:** Given any abelian group R, we can turn R into a ring by defining multiplication via $ab = 0$ for all $a, b \in R$. Trivial rings are commutative rings in which every nonzero element is a zero divisor. Hence a trivial ring is not a division ring, not a field, and not a integral domain.

(3) The integers $\mathbb{Z}$ form a ring under the usual operations of addition and multiplication. The integers form an integral domain, but $\mathbb{Z}$ is not a division ring, and hence not a field.

(4) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields under the usual operations of addition and multiplication.

(5) For $n \geq 1$, the set $\mathbb{Z}_n$ is a commutative ring with 1 under the operations of addition and multiplication mod n. The group of units $\mathbb{Z}_n^\times$ is the set of elements in $\mathbb{Z}_n$ that are relatively prime to n. All other nonzero elements are zero divisors. It turns out that $\mathbb{Z}_n$ forms a finite field iff n is prime.

(6) The set of even integers $2\mathbb{Z}$ forms a commutative ring under the usual operations of addition and multiplication. However, $2\mathbb{Z}$ does not have a 1, and hence cannot be a division ring nor a field nor an integral domain.

(7) **Polynomial Ring:** Fix a commutative ring R. Let $R[x]$ denote the set of polynomials in the variable x with coefficients in R. Then $R[x]$ is a commutative ring with 1. The units of $R[x]$ are exactly the units of R (if there are any). So, $R[x]$ is never a division ring nor a field. However, if R is an integral domain, then so is $R[x]$.

(8) **Matrix Ring:** Fix a ring R and let n be a positive integer. Let $M_n(R)$ be the set of $n \times n$ matrices with entries from R. Then $M_n(R)$ forms a ring under ordinary matrix addition and multiplication. If R is nontrivial and $n \geq 2$, then $M_n(R)$ always has zero divisors and $M_n(R)$ is not commutative even if R is. If R has a 1, then the matrix with 1's down the diagonal and 0's elsewhere is the multiplicative identity in $M_n(R)$. In this case, the group of units is the set of invertible $n \times n$ matrices, denoted $GL_n(R)$ and called the **general linear group of degree** n **over** R.

(9) **Quadratic Field:** Define $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. It turns out that $\mathbb{Q}(\sqrt{2})$ is a field. In fact, we can replace 2 with any rational number that is not a perfect square in $\mathbb{Q}$.

(10) **Hamilton Quaternions:** Define $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i, j, k \in Q_8\}$ Then $\mathbb{H}$ forms a ring, where addition is definite componentwise in i, j, and k and multiplication is defined by expanding products and the simplifying using the relations of Q_8. It turns out that $\mathbb{H}$ is a non-commutative ring with 1.

Definition 1.19. A **subring** of a ring R is a subgroup of R that is closed under multiplication.

Note 1.20. The property "is a subring" is clearly transitive. To show that a subset S of a ring R is a subring, it suffices to show that $S \neq \emptyset$, S is closed under subtraction, and S is closed under multiplication.

Example 1.21. Here are a few quick examples.

(1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which in turn is a subring of $\mathbb{C}$.

(2) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(3) The set $\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{2})$.

(4) The ring R is a subring of $R[x]$ if we identify R with set of constant functions.

(5) The set of polynomials with zero constant term in $R[x]$ is a subring of $R[x]$.

(6) $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.

(7) $\mathbb{Z}_n$ is *not* a subring of $\mathbb{Z}$.

Definition 1.22. Let R and S be rings. A **ring homomorphism** is a map $\phi : R \to S$ satisfying

(i) $\phi(a+b) = \phi(a) + \phi(b)$

(ii) $\phi(ab) = \phi(a)\phi(b)$

for all $a, b \in R$. The **kernel** of ϕ is defined via $\ker(\phi) = \{a \in R \mid \phi(a) = 0\}$. If ϕ is a bijection, then ϕ is called an **isomorphism**, in which case, we say that R and S are **isomorphic rings** and write $R \cong S$.

Example 1.23.

(1) For $n \in \mathbb{Z}$, define $\phi_n : \mathbb{Z} \to \mathbb{Z}$ via $\phi_n(x) = nx$. We see that $\phi_n(x+y) = n(x+y) = nx + ny = \phi_n(x) + \phi_n(y)$. However, $\phi_n(xy) = n(xy)$ while $\phi_n(x)\phi_n(y) = (nx)(ny) = n^2xy$. It follows that ϕ_n is a ring homomorphism exactly when $n \in \{0, 1\}$.

(2) Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ via $\phi(p(x)) = p(0)$ (called **evaluation at 0**). It turns out that ϕ is a ring homomorphism, where $\ker(\phi)$ is the set of polynomials with 0 constant term.

Theorem 1.24. Let $\phi : R \to S$ be a ring homomorphism.

(1) $\phi(R)$ is a subring of S.

(2) $\ker(\phi)$ is a subring of R.

In fact, we can say something even stronger about the kernel of a ring homomorphism, which will lead us to the notion of an **ideal**.

Theorem 1.25. Let $\phi : R \to S$ be a ring homomorphism. If $\alpha \in \ker(\phi)$ and $r \in R$, then $\alpha r, r\alpha \in \ker(\phi)$. That is, $\ker(\phi)$ is closed under multiplication by elements of R.

1.2 Ideals and Quotient Rings

This section of notes roughly follows Sections 7.3–7.4 in Dummit and Foote.

Recall that in the case of a homomorphism ϕ of groups, the fibers of ϕ have the structure of a group (that happens to be isomorphic to the image of ϕ by the First Isomorphism Theorem). In this case, the kernel of ϕ is the identity of the associated quotient group. This naturally led to the notion of a normal subgroup (i.e., those groups that correspond to kernels of homomorphisms). Can we do the same sort of thing for rings?

Let $\phi : R \to S$ be a ring homomorphism with $\ker(\phi) = I$. Note that ϕ is also a group homomorphism of abelian groups and the fibers of ϕ are the cosets $r + I$. That is, if $\phi(r) = a$, then the fiber of ϕ over a is the coset $\phi^{-1}(a) = r + I$.

These cosets naturally have the structure of a ring isomorphic to the image of ϕ:

$$(r + I) + (s + I) = (r + s) + I \tag{1.1}$$

$$(r + I)(s + I) = (rs) + I \tag{1.2}$$

The reason for this is that if the fiber of $a \in S$ is $\phi^{-1}(a) = X$ and the fiber of $b \in S$ is $\phi^{-1}(b) = Y$, then the fibers of $a + b$ and ab are $X + Y$ and XY, respectively.

The corresponding ring of cosets is called the **quotient ring** of R by $I = \ker(\phi)$ and is denoted by R/I. The additive structure of the quotient ring R/I is exactly the additive quotient group of the additive abelian group R by the normal subgroup R (all subgroups are normal

in abelian groups). When I is the kernel of some ring homomorphism ϕ, the additive abelian quotient group R/I also has a multiplicative structure defined in (2) above, making R/I into a ring.

Question 1.26. Can we make R/I into a ring for any subring I?

The answer is "no" in general, just like in the situation with groups. But perhaps this isn't obvious because if I is an arbitrary subring of R, then I is necessarily an additive subgroup of the abelian group R, which implies that I is an additive normal subgroup of the group R. It turns out that the multiplicative structure of R/I may not be well-defined if I is an arbitrary subring.

Let I be an arbitrary *subgroup* of the additive subgroup R. Let $r+I$ and $s+I$ be two arbitrary cosets. In order for multiplication of the cosets to be well-defined, the product of the two cosets must be independent of choice of representatives. Let $r+\alpha$ and $s+\beta$ be arbitrary representatives of $r+I$ and $s+I$, respectively ($\alpha, \beta \in I$), so that $r+I = (r+\alpha)+I$ and $s+I = (s+\beta)+I$. We must have

$$(r+\alpha)(s+\beta)+I = rs+I. \tag{1.3}$$

This needs to be true for all possible choices of $r, s \in R$ and $\alpha, \beta \in I$. In particular, it must be true when $r = s = 0$. In this case, we must have

$$\alpha\beta + I = I. \tag{1.4}$$

But this only happens when $\alpha\beta \in I$. That is, one requirement for multiplication of cosets to be well-defined is that I must be closed under multiplication, making I a *subring*.

Next, if we let $s = 0$ and let r be arbitrary, we see that we must have $r\beta \in I$ for every $r \in R$ and every $\beta \in I$. That is, it must be the case that I is closed under multiplication on the left by elements from R. Similarly, letting $r = 0$, we can conclude that we must have I closed under multiplication on the right by elements from R.

On the other hand, if I is closed under multiplication on the left and on the right by elements from R, then it is clear that relation (4) above is satisfied.

It is easy to verify that if the multiplication of cosets defined in (2) above is well-defined, then this multiplication makes the additive quotient group R/I into a ring (just check the axioms for being a ring).

We have shown that the quotient R/I of the ring R by a subgroup I has a natural ring structure iff I is closed under multiplication on the left and right by elements of R (which also forces I be a subring). Such subrings are called **ideals**.

Definition 1.27. Let R be a ring and let I be a subset of R.

(1) I is a **left ideal** (respectively, **right ideal**) of R iff I is a subring and $rI \subseteq I$ (respectively, $Ir \subseteq I$) for all $r \in R$.

(2) I is an **ideal** (or **two-sided ideal**) iff I is both a left and a right ideal.

Here's a summary of everything that just happened.

Theorem 1.28. Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I)=(r+s)+I \tag{1.5}$$
$$(r+I)(s+I)=(rs)+I \tag{1.6}$$

for all $r,s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

As you might expect, we have some isomorphism theorems.

Theorem 1.29 (First Isomorphism Theorem for Rings)**.** If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R and $R/\ker(\phi) \cong \phi(R)$.

If I and J are ideals of R, then it is easy to verify that $I \cap J$, $I+J = \{a+b \mid a \in I, b \in J\}$, and $IJ = \{\text{finite sums of elements of the form } ab \text{ for } a \in I, b \in J\}$ are also ideals of R. We also have the expected Second, Third, and Fourth Isomorphism Theorems for rings.

The next theorem tells us that a subring is an ideal iff it is a kernel of a ring homomorphism.

Theorem 1.30. If I is any ideal of R, then the **natural projection** $\pi : R \to R/I$ defined via $\pi(r) = r+I$ is a surjective ring homomorphism with $\ker(\pi) = I$.

For the remainder of this section, assume that R is a ring with identity $1 \neq 0$.

Definition 1.31. Let A be any subset of R.

(1) Let (A) denote the smallest idea of R containing A, called the **ideal generated by** A. If A consists of a single element, say $A = \{a\}$, then $(a) := (\{a\})$ is called a **principal ideal**.

(2) $RA := \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$, $AR := \{a_1r_1 + \cdots + a_nr_n \mid a_i \in A, r_i \in R, n \in \mathbb{Z}^+\}$, and $RAR := \{r_1a_1r_1' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$.

Note 1.32. The following facts are easily verified.

(1) (A) is the intersection of all ideals containing A.

(2) RA, AR, and RAR are the left, right, and two-sided ideals generated by A.

(3) If R is commutative, then $RA = AR = RAR = (A)$.

(4) If R is commutative, then $(a) = Ra = aR$.

Example 1.33. Here are a couple of examples. The details are left as exercises.

(1) In $\mathbb{Z}$, $n\mathbb{Z} = (n) = (-n)$. In fact, these are the only ideals in $\mathbb{Z}$ (since these are the only subgroups). So, all the ideals in $\mathbb{Z}$ are principal. If m and n are positive integers, then $n\mathbb{Z} \subseteq m\mathbb{Z}$ iff m divides n. Moreover, we have $(m, n) = (d)$, where d is the greatest common divisor of m and n.

(2) Consider the ideal $(2, x)$ in $\mathbb{Z}[x]$. Note that $(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Then $(2, x)$ is the collection of polynomials from $\mathbb{Z}[x]$ that have even constant term. In particular, $2, x \in (2, x)$. However, there is no single polynomial in $\mathbb{Z}[x]$ that we can use to generate both 2 and x that only produces polynomials with even constant terms.

Theorem 1.34. Let I be an ideal of R.

(1) $I = R$ iff I contains a unit.

(2) Assume R is commutative. Then R is a field iff its only ideals are 0 and R.

Loosely speaking, the previous result says that fields are "like simple groups."

Corollary 1.35. If R is a field, then every nonzero ring homomorphism from R into another ring is an injection.

1.3 Maximal and Prime Ideals

This section of notes roughly follows Section 7.4 in Dummit and Foote. Throughout this entire section, we assume that all rings have a multiplicative identity $1 \neq 0$.

In this section of notes, we will study two important classes of ideals, namely **maximal** and **prime** ideals, and study the relationship between them.

Definition 1.36. An ideal M in a ring R is called a **maximal ideal** if $M \neq R$ and the only ideals containing M are M and R.

Example 1.37. Here are a few examples. Checking the details is left as an exercise.

(1) In $\mathbb{Z}$, all the ideals are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}^+$. The maximal ideals correspond to the ideals $p\mathbb{Z}$, where p is prime.

(2) Consider the integral domain $\mathbb{Z}[x]$. The ideals (x) (i.e., the subring containing polynomials with 0 constant term) and (2) (i.e, the set of polynomials with even coefficients) are not maximal since both are contained in the proper ideal $(2, x)$. However, as we shall see soon, $(2, x)$ is maximal in $\mathbb{Z}[x]$.

(3) The zero ring has no maximal ideals.

(4) Consider the abelian group $\mathbb{Q}$ under addition. We can turn $\mathbb{Q}$ into a trivial ring by defining $ab = 0$ for all $a, b \in \mathbb{Q}$. In this case, the ideals are exactly the additive subgroups of $\mathbb{Q}$. However, $\mathbb{Q}$ has no maximal subgroups, and so $\mathbb{Q}$ has no maximal ideals.

The next result states that rings with an identity $1 \neq 0$ always have maximal ideals. It turns out that we won't need this result going forward, so we'll skip its proof. However, it is worth noting that all known proofs make use of Zorn's Lemma (equivalent to the Axiom of Choice), which is also true for the proofs that a finitely generated group has maximal subgroups or that every vector spaces has a basis.

Theorem 1.38. In a ring with 1, every proper ideal is contained in a maximal ideal.

For commutative rings, there is a very nice characterization about maximal ideals in terms of the structure of their quotient rings.

Theorem 1.39. Assume R is commutative. The ideal M is maximal iff R/M is a field.

Example 1.40. We can use the previous theorem to verify whether an ideal is maximal.

(1) Recall that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ and that $\mathbb{Z}_n$ is a field iff n is prime. We can conclude that $n\mathbb{Z}$ is a maximal ideal precisely when n is prime.

(2) Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ via $\phi(p(x)) = p(0)$. Then ϕ is surjective and $\ker(\phi) = (x)$. By the First Isomorphism Theorem for Rings, we see that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. However, $\mathbb{Z}$ is not a field. Hence (x) is not maximal in $\mathbb{Z}[x]$. Now, define $\psi : \mathbb{Z} \to \mathbb{Z}_2$ via $\psi(x) = x \mod 2$ and consider the composite homomorphism $\psi \circ \phi : \mathbb{Z} \to \mathbb{Z}_2$. It is clear that $\psi \circ \phi$ is onto and the kernel of $\psi \circ \phi$ is given by $\{p(x) \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\} = (2, x)$. Again by the First Isomorphism Theorem for Rings, $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, $(2, x)$ is a maximal ideal.

Definition 1.41. Assume R is commutative. An ideal P is called a **prime ideal** if $P \neq R$ and whenever the product $ab \in P$ for $a, b \in R$, then at least one of a or b is in P.

Example 1.42. In any integral domain, the 0 ideal (0) is a prime ideal. What if the ring is not an integral domain?

Note 1.43. The notion of a prime ideal is a generalization of "prime" in $\mathbb{Z}$. Suppose $n \in \mathbb{Z}^+ \setminus \{1\}$ such that n divides ab. In this case, n is guaranteed to divide either a or b exactly when n is prime. Now, let $n\mathbb{Z}$ be a proper ideal in $\mathbb{Z}$ with $n > 1$ and suppose $ab \in \mathbb{Z}$ for $a, b \in \mathbb{Z}$. In order for $n\mathbb{Z}$ to be a prime ideal, it must be true that n divides either a or b. However, this is only guaranteed to be true for all $a, b \in \mathbb{Z}$ when p is prime. That is, the nonzero prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where p is prime. Note that in the case of the integers, the maximal and nonzero prime ideals are the same.

Theorem 1.44. Assume R is a commutative ring. Then the ideal P is a prime ideal in R iff the quotient ring R/P is an integral domain.

Corollary 1.45. Assume R is a commutative ring. Every maximal ideal of R is a prime ideal.

Example 1.46. Recall that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, it must be the case that (x) is a prime ideal in $\mathbb{Z}[x]$. However, as we saw in an earlier example, (x) is not maximal in $\mathbb{Z}[x]$ since $\mathbb{Z}$ is not a field. This shows that the converse of the previous corollary is not true.

1.4 Rings of Fractions

This section of notes roughly follows Section 7.5 in Dummit and Foote.

Throughout this whole section, we assume that R is a commutative ring.

Note 1.47. We recall a few relevant facts.

(1) Theorem 1.11 (Cancellation Law) tells us that if $ab = ac$ and a is neither 0 nor a zero divisor, then $b = c$.

(2) Zero divisors are never units.

One upshot of the above is that ring elements that are not zero divisors possess some of the behavior of units. The goal of this section is to prove that every commutative ring R is aways a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q. In particular, we can apply this to integral domains, in which case Q will be a field. This generalizes the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Note 1.48. Recall that in $\mathbb{Q}$, the fraction $\frac{a}{b}$ is the equivalence class of order pairs (a, b) of integers with $b \neq 0$ under the equivalence relation:

$$(a, b) \sim (c, d) \text{ iff } \frac{a}{b} = \frac{c}{d} \text{ iff } ad = bc.$$

Also, every nonzero rational number $\frac{a}{b}$ has multiplicative inverse $\frac{b}{a}$. That is, every nonzero rational number is a unit, making $\mathbb{Q}$ a field. The integers $\mathbb{Z}$ are a subring of $\mathbb{Q}$. But $\mathbb{Z}$ is an integral domain, not a field.

Theorem 1.49. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication. Then there exists a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q.

Theorem 1.50. Let R, D, and Q be as in Theorem 1.49. Then every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R \setminus \{0\}$, then Q is a field.

Theorem 1.51. Let R, D, and Q be as in Theorem 1.49. Then Q is the smallest ring containing R in which all elements of D become units, in the following sense. Let S be any commutative ring with 1 and let $\phi : R \to S$ be any injective ring homomorphism such that $\phi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \phi$.

Definition 1.52. Let R, D, and Q be as in Theorem 1.49.

(1) The ring Q is called the **ring of fractions** of D with respect to R and is denoted $D^{-1}R$.

(2) If R is an integral domain and $D = R \setminus \{0\}$, then Q is called the **field of fractions** (or **quotient field**) of R.

Corollary 1.53. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R, then the subfield of F generated by R' (i.e., the intersection of all the subfields of F containing R') is isomorphic to Q.

Example 1.54. Here are a few quick examples.

(1) If R is a field, then its field of fractions is R itself.

(2) The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. The field of fractions of $2\mathbb{Z}$ is also $\mathbb{Q}$.

(3) Consider the polynomial ring $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is an integral domain, so is $\mathbb{Z}[x]$. Then the field of fractions of $\mathbb{Z}[x]$ is the set of rational functions (i.e., functions of the form $p(x)/q(x)$, where $p(x)$ and $q(x)$ are polynomials with integer coefficients and $q(x)$ is not the zero polynomial). Notice that this field contains the field of fractions of $\mathbb{Z}$, namely $\mathbb{Q}$. However, it is interesting to point out that the field of fractions of $\mathbb{Q}[x]$ is the same as the field of fractions of $\mathbb{Z}[x]$.

1.5 Principal Ideal Domains

This section of notes roughly follows Sections 8.1-8.2 in Dummit and Foote. Throughout this whole section, we assume that R is a commutative ring.

Definition 1.55. Let R b a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be **multiple** of b if there exists an element $x \in R$ with $a = bx$. In this case, b is said to **divide** a or be a **divisor** of a, written $b \mid a$.

(2) A **greatest common divisor** of a and b is a nonzero element d such that

   (a) $d \mid a$ and $d \mid b$, and

   (b) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

   A greatest common divisor of a and b will be denoted $\gcd(a, b)$ (or possibly (a, b)).

Note 1.56. Note that $b \mid a$ in a ring R iff $a \in (b)$ iff $(a) \subseteq (b)$. In particular, if d is any divisor of both a and b, then (d) must contain both a and b, and hence must contain (a, b). Moreover, if d is a greatest common divisor iff $(a, b) \subseteq (d)$ and if (d') is any principal ideal containing (a, b), then $(d) \subseteq (d')$.

The note above immediately proves the following result.

Theorem 1.57. If a and b are nonzero elements in the commutative ring R such that $(a, b) = (d)$, then d is a gcd of a and b.

Note 1.58. It is important to point out that the theorem above is giving us a sufficient condition, but it is not necessary. For example, $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$ that is not principal. Then $\mathbb{Z}[x] = (1)$ is the unique principal ideal containing both 2 and x, and so 1 is a gcd of 2 and x.

Theorem 1.59. Let R be an integral domain. If $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, if d and d' are both gcds of a and b, then $d' = ud$ for some unit $u \in R$.

Proof. Easy exercise. □

Definition 1.60. A **principal ideal domain** (PID) is an integral domain in which every ideal is principal.

Example 1.61. Here are some short examples.

(1) $\mathbb{Z}$ is a PID.

(2) $\mathbb{Z}[x]$ is not a PID since $(2, x)$ is not principal.

Theorem 1.62. Let R be a PID, $a, b \in R \setminus \{0\}$, and $(d) = (a, b)$. Then

(1) $d = \gcd(a, b)$

(2) $d = ax + by$ for some $x, y \in R$

(3) d is unique up to multiplication by a unit of R.

Proof. The result follows from Theorems 1.57 and 1.59. □

Theorem 1.63. Every nonzero prime ideal in a PID is a maximal ideal.

Corollary 1.64. If R is a commutative ring such that the polynomial ring $R[x]$ is a PID, then R is necessarily a field.

Example 1.65. Here are a few quick examples.

(1) We already know that $\mathbb{Z}[x]$ is not a PID, but the above corollary tells us again that it isn't since $\mathbb{Z}$ is not a field.

(2) The polynomial ring $\mathbb{Q}[x]$ is an eligible PID and it turns out that it is. In fact, $F[x]$ ends up being a PID for every field F.

(3) The polynomial ring $\mathbb{Q}[x, y]$ turns out not to be a PID. The reason for this is that $\mathbb{Q}[x, y] = (\mathbb{Q}[x])[y]$ and $\mathbb{Q}[x]$ is not a field.

1.6 Euclidean Domains

This section roughly follows Sections 8.1 and 8.2 in Dummit and Foote. Throughout this whole section, we assume that all rings are commutative.

The goal of this section is to study rings with a division algorithm. First, let's recall the division algorithm that you are familiar with in the integers.

Theorem 1.66 (Division Algorithm)**.** If $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exists unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r,$$

where $0 \leq r < |b|$. In this case, we call q the **quotient** and r the **remainder**.

In order to generalize the Division Algorithm, we need the notion of a norm, which is essentially a measure of "size" in a ring R.

Definition 1.67. Let R be an integral domain. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a **norm** on R. If $N(a) > 0$ for all $a \neq 0$, then N is called a **positive norm**.

Observe that it is possible for an integral domain to possess many different norms.

Definition 1.68. An integral domain R is called a **Euclidean Domain** (or is said to possess a **Division Algorithm**) if there is a norm N on R such that for any two $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r,$$

where either $r = 0$ or $N(r) < N(b)$. In this case, we call q the **quotient** and r the **remainder**.

Example 1.69. If we use absolute value as our norm, the integers form a Euclidean Domain. In this case, the corresponding division algorithm is the standard division algorithm.

As with the standard Division Algorithm, a Division Algorithm on a **Euclidean Domain** yields a **Euclidean Algorithm**. For two elements a and b of a Euclidean Domain R, we can obtain the following by successive "divisions" (where we really are doing division in the field of fractions of R):

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since $N(b) > N(r_0) > N(r_1) > \cdots > N(r_n)$ is a decreasing sequence of nonnegative integers if the remainders are nonzero (and such a sequence cannot be infinite).

Example 1.70. Here are two quick examples. Details left as an exercise.

(1) Every field is a Euclidean Domain, where we can take the norm to be whatever we like. The reason for this is that for every a and b in the field with $b \neq 0$, we have $a = qb + 0$, where $q = ab^{-1}$.

(2) If F is a field, then the polynomial ring $F[x]$ is a Euclidean Domain with norm given by $N(p(x)) =$ degree of $p(x)$. The Division Algorithm for polynomials is just long division of polynomials that you learn in precalculus. We will prove later that if R is not a field, then $R[x]$ cannot be a Euclidean Domain.

Theorem 1.71. Every ideal in a Euclidean Domain is principal. In particular, if I is any nonzero ideal in the Euclidean Domain R, then $I = (d)$, where d is any nonzero element of I of minimum norm.

The above theorem immediately implies the following.

Corollary 1.72. Every Euclidean Domain is a PID.

The previous corollary yields the following, which we already knew was true.

Corollary 1.73. Every ideal in $\mathbb{Z}$ is principal.

Of course, we should immediately wonder if every PID is a Euclidean Domain. It turns out that the answer is "no."

Example 1.74. It turns out that the quadratic integer ring $\mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID but not a Euclidean Domain. For details, see the last example in Section 8.3 of Dummit and Foote.

We can use Theorem 1.71 to verify that some integral domains are not Euclidean Domains (with respect to any norm).

Example 1.75. Details left as an exercise.

(1) Since the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal (see Example 1.33(2)), the polynomial ring $\mathbb{Z}[x]$ cannot be a Euclidean Domain under any norm by Theorem 1.71.

(2) Consider the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. It turns out that the ideal $I = (3, 2+\sqrt{-5})$ is not principal, which implies that $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Domain under any norm by Theorem 1.71.

Recall that the standard Euclidean Algorithm on $\mathbb{Z}$ produces the gcd of two nonzero integers. The next theorem tells us that gcds always exist in Euclidean Domains and that we can compute them algorithmically. Before digesting the next theorem, it might be a good idea to review Theorems 1.57, 1.59, and 1.62.

Theorem 1.76. Let R be a Euclidean Domain and let $a, b \in R$ with $a, b \neq 0$. Let $d = r_n$ be the last nonzero remainder obtained from the Euclidean Algorithm on R. Then

(1) d is a gcd of a and b;

(2) $(d) = (a, b)$;

(3) There exists $x, y \in R$ such that $d = ax + by$.

Notice that we didn't make any claims about the uniqueness of x and y in the previous theorem. For the Euclidean Domain $\mathbb{Z}$, it turns out that if x_0 and y_0 are solutions to the Diophantine equation $ax + by = N$, then every solution is of the form

$$x = x_0 + m\frac{b}{\gcd(a,b)}$$
$$y = y_0 - m\frac{a}{\gcd(a,b)}$$

where $m \in \mathbb{Z}$. For more details, see a standard number theory book.

Notice that the equation $ax + by = N$ is another way of saying that N is an element of the ideal generated by a and b. However, this ideal is simply the principal ideal (d) (where $d = \gcd(a,b)$). That is, $N \in (d)$, which implies that N is divisible by d. It follows that the equation $ax + by = N$ is solvable in integers x and y iff N is divisible by the gcd of a and b.

It is important to point out that gcds exist in both PIDs and Euclidean Domains. However, an advantage of Euclidean Domains is that we are guaranteed an algorithm for finding gcds.

It might be a good idea to run through an example of using the Euclidean Algorithm in case you've never see it or forgotten how to do it.

Example 1.77. Compute the gcd of the integers $a = 11391$ and $b = 5673$ and then translate the answer into the language of ideals.

1.7 Unique Factorization Domains

This section roughly follows Section 8.3 in Dummit and Foote. Throughout this whole section, we assume that all rings are integral domains (unless we specify differently).

Recall that the Euclidean Algorithm is a method for determining the gcd of two nonzero elements in the integers (or any Euclidean Domain). Another way to obtain the gcd of two nonzero integers is to obtain the prime factorization of both and look for common factors. Note that the Euclidean Algorithm is a fairly efficient method for obtaining a gcd, whereas obtaining the prime factorization of a single integer is a hard problem in general. Nonetheless, we want to generalize the notion of "prime factorization" to other rings.

In this section, we will introduce a class of rings, called **Unique Factorization Domains** (UFD), that allow factorization into primes as we would in the integers. The main result of this section is that all PIDs are UFDs.

Definition 1.78. Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and not a unit. Then r is called **irreducible** in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit. Otherwise, r is called **reducible**.

(2) The nonzero element $p \in R$ is called **prime** in R if the ideal (p) is a prime ideal. That is, p is prime iff whenever $p \mid ab$ for any $a, b \in R$, $p \mid a$ or $p \mid b$.

(3) Two elements a and b of R differing by a unit are said to be **associate** in R (i.e., $a = ub$ for some unit R.

An intermediate goal is to understand the relationship between irreducible and prime.

Example 1.79. In the integers, 6 and -6 are associates since $-6 = -1 \cdot 6$ and -1 is a unit. In general, two integers a and b are associates of one another iff $a = \pm b$. In the integers, the primes are the positive and negative primes from the natural numbers that you are familiar with. Notice that in the integers, the primes and irreducibles are identical. However, this is not always the case as we shall see.

Theorem 1.80. In an integral domain, a prime element is always irreducible.

It turns out that the converse is false.

Example 1.81. Consider the element 3 in the ring $\mathbb{Z}[\sqrt{-5}]$. Suppose $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Then we must have $ac - 5bd = 3$ and $ad + bc = 0$. One can check that the only integer solutions to this system are $a = 3, -3, 1, -1$ and $c = 1, -1, 3, -3$, respectively and $b = d = 0$. This shows that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. However, notice that $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$, which is divisible by 3. But neither $2 + \sqrt{-5}$ nor $2 - \sqrt{-5}$ is divisible by 3 in $\mathbb{Z}[\sqrt{-5}]$. Therefore, 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Recall that in a commutative ring, every maximal ideal is also prime while the converse is false (e.g., (x) is prime in $\mathbb{Z}[x]$ but not maximal). However, in a PID, nonzero ideals are prime iff they are maximal (see Theorem 1.63). We have a similar relationship with prime and irreducible elements.

Theorem 1.82. In a PID, a nonzero element is prime iff it is irreducible.

Example 1.83. Back in Part (2) of Example 1.75, we argued that $\mathbb{Z}[\sqrt{-5}]$ was not a Euclidean Domain by claiming that $\mathbb{Z}[\sqrt{-5}]$ was not a PID, but we omitted the details. Since 3 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$, the ring $\mathbb{Z}[\sqrt{-5}]$ cannot be a PID, which implies that $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Domain (by Theorem 1.71).

In $\mathbb{Z}$, every integer n can be written as a product of primes. This decomposition is unique in the sense that any two prime factorizations for n differ only in the order in which the positive prime factors are written. The restriction to positive integers is so that we don't have to think of the factorizations $(2)(3)$ and $(-2)(-3)$ of 6 as different. Rings with an analogous property are given a name.

Definition 1.84. A **Unique Factorization Domain** (UFD) is an integral domain R in which every nonzero element $r \in R$ that is not a unit has the following properties:

(1) The ring element r can be written as a product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$;

(2) The decomposition in (1) is unique up to associates: if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that q_i and p_i are associates for all i.

Example 1.85. Details left as an exercise.

(1) In a field, every nonzero element is a unit. Hence there are no elements for which Conditions (1) and (2) for a UFD must be verified.

(2) The ring $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$, where $i^2 = -1$, is an integral domain. Note that the elements 2 and $2i$ are irreducibles that are not associates in $\mathbb{Z}[2i]$ since $i \notin \mathbb{Z}[2i]$. We see that $4 = 2 \cdot 2 = (2i) \cdot (-2i)$ has two distinct factorizations in $\mathbb{Z}[2i]$. This shows that $\mathbb{Z}[2i]$ is not a UFD.

Since $\mathbb{Z}[2i]/(2i) \cong \mathbb{Z}/4\mathbb{Z}$ is not an integral domain, the ideal $(2i)$ is not prime, which implies that $2i$ is irreducible but not prime.

Notice that in the larger ring of Gaussian integers $\mathbb{Z}[i]$, 2 and $2i$ are associates since i is a unit in this larger ring (with inverse $-i$).

(3) Consider the ring $\mathbb{Z}[\sqrt{-5}]$. Notice that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is two distinct factorizations of 6 into irreducibles in $\mathbb{Z}[\sqrt{-5}]$. Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

The next theorem is analogous to Theorem 1.82.

Theorem 1.86. In a UFD, a nonzero element is prime iff it is irreducible.

In a generic UFD, we can now use the terms "prime" and "irreducible" interchangeably. Typically, we will refer to "primes" in $\mathbb{Z}$ and " irreducibles" in $F[x]$.

Theorem 1.87. Let a and b be two nonzero elements of the UFD R and suppose

$$a = up_1^{e_1} \cdots p_n^{e_n} \quad \text{and} \quad b = vp_1^{f_1} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, \ldots, p_n$ are distinct and the exponents e_i and f_i are nonnegative. Then

$$d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)},$$

where $d = 1$ if all exponents are 0, is a gcd of a and b.

The next theorem is the punchline of this section. It's proof takes a little bit work.

Theorem 1.88. Every PID is a UFD. In particular, every Euclidean Domain is a UFD.

Corollary 1.89 (Fundamental Theorem of Arithmetic)**.** The integers are a UFD.

Example 1.90. Details left as an exercise.

(1) In the next section, we will prove that if F is a field, then $F[x]$ is a Euclidean Domain. Theorem 1.88 implies that $F[x]$ is a UFD. As an example, $\mathbb{Q}[x]$ is a UFD.

(2) It turns out that $R[x]$ is a UFD exactly when R is a UFD (we will prove this later). In particular, $\mathbb{Z}[x]$ is a UFD. Notice that the properties of being a PID or Euclidean Domain do not necessarily carry over from R to $R[x]$.

Note 1.91. The upshot of what we have done to this point is the following chain of containments:

$$\text{fields} \subset \text{Euclidean Domains} \subset \text{PIDs} \subset \text{UFDs} \subset \text{integral domains},$$

where are all containments are strict.

1.8 More on Polynomial Rings

This section roughly follows Sections 9.1–9.5 in Dummit and Foote. Throughout this whole section, we assume that all rings are commutative with identity $1 \neq 0$.

First, let's recall several facts about polynomial rings. Assume that R is at least an integral domain.

(1) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$

(2) The units of $R[x]$ are exactly the units of R.

(3) $R[x]$ is an integral domain.

(4) The quotient field of $R[x]$ consists of all rational functions of the form $p(x)/q(x)$, where $p(x), q(x) \in R[x]$ and $q(x) \neq 0$.

(5) If $R[x]$ is a PID or Euclidean Domain, then R must be a field. (Corollary 1.64)

The next theorem describes a relationship between the ideals in $R[x]$ and the ideals in R.

Theorem 1.92. Let I be an ideal in R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (i.e., the set of polynomials with coefficients from I). Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Note 1.93. We cannot replace "prime" with "maximal" in the theorem above. That is, if I is a maximal ideal of R, then (I) may not be maximal in $R[x]$. However, if I is maximal in R, then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

Example 1.94. Consider the ideal $n\mathbb{Z}$ of $\mathbb{Z}$. The Theorem 1.92 tells us that

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$$

and the natural projection map from $\mathbb{Z}[x]$ to $\mathbb{Z}/n\mathbb{Z}[x]$ by reducing coefficients mod n is a ring homomorphism. If n is composite, then the quotient ring is not an integral domain (since the ring of coefficients is not an integral domain). However, if n is a prime p, then $\mathbb{Z}/p\mathbb{Z}$ is a field, and so $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (in fact, a Euclidean Domain). Notice that the set of polynomials whose coefficients are divisible by p is a prime ideal in $\mathbb{Z}[x]$.

Next, we look more closely at the case when the coefficient ring is a field. Let F be a field. We can define a norm on $F[x]$ by defining $N(p(x)) = \deg(p(x))$ and $N(0) = 0$. The next theorem makes the Division Algorithm in $F[x]$ explicit.

Theorem 1.95. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. More specifically, if $a(x), b(x) \in F[x]$ with $b(x) \neq 0$, then there exists unique $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

At the beginning of this section, we mentioned that if $R[x]$ is a PID or Euclidean Domain, then R is necessarily a field. The next corollary tells us that the converse is true.

Corollary 1.96. If F is a field, then $F[x]$ is a PID and a UFD.

Example 1.97. Details left as an exercise.

(1) Recall that the ideal $(2, x)$ is not principal in the ring $\mathbb{Z}[x]$. However, Corollary 1.96 guarantees that the ring $\mathbb{Q}[x]$ is a PID since $\mathbb{Q}$ is a field. This implies that the ideal $(2, x)$ is principal in $\mathbb{Q}[x]$. In fact, since 2 is a unit in $\mathbb{Q}[x]$, $(2, x) = (1) = \mathbb{Q}[x]$.

(2) If p is prime, the ring $\mathbb{Z}/p\mathbb{Z}[x]$ obtained by reducing $\mathbb{Z}[x]$ mod the prime ideal (p) is a PID since $\mathbb{Z}/p\mathbb{Z}$ is a field. This example shows that the quotient of a ring that is not a PID may be a PID. Notice that if $p = 2$, then the ideal $(2, x)$ reduces to the ideal (x) in $\mathbb{Z}/2\mathbb{Z}[x]$, which is a proper maximal ideal. If $p \neq 2$, then 2 is a unit in the quotient, and hence the ideal $(2, x)$ reduces to the entire ring $\mathbb{Z}/p\mathbb{Z}$.

(3) The ring $\mathbb{Q}[x, y]$ is not a PID since $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ and $\mathbb{Q}[x]$ is not a field.

Let R be an integral domain and let F be its field of fractions. Then $R[x]$ is an integral domain that is a subring $F[x]$, where $F[x]$ is a Euclidean Domain (and hence PID and UFD). Sometimes it is handy to perform computations in $F[x]$ (e.g., factorizations of polynomials) and then cross your fingers and hope that you can pass back to $R[x]$.

For example, suppose $p(x) \in R[x]$. Since $F[x]$ is a UFD, we can factor $p(x)$ into a product of irreducibles in $F[x]$. Can we factor $p(x)$ into irreducibles in $R[x]$? In general, the answer is "no". Shit. However, as we shall see, if R happens to be a UFD, then we're in luck.

Theorem 1.98 (Gauss' Lemma)**.** Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x) = A(x)B(x)$ for nonconstant polynomials $A(x), B(x) \in F[x]$, then there exist nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$. That is, if we can factor $p(x)$ in $F[x]$, then we can factor $p(x)$ in $R[x]$.

Note 1.99. A couple comments are in order.

(1) Note that we cannot prove that $a(x)$ and $b(x)$ are necessarily R-multiples of $A(x)$ and $B(x)$, respectively. For example, consider $x^2 \in \mathbb{Q}[x]$ with $A(x) = 2x$ and $B(x) = \frac{1}{2}x$. Then $x^2 = A(x)B(x)$, but no integer multiples of $A(x)$ and $B(x)$ give a factorization of x^2 in $\mathbb{Z}[x]$.

(2) The nonzero elements of R become units in the UFD $F[x]$ and the units in $F[x]$ are the nonzero elements of F. For example, $7x$ factors in $\mathbb{Z}[x]$ into two irreducibles: 7 and x. So, $7x$ is not irreducible in $\mathbb{Z}[x]$. However, in $\mathbb{Q}[x]$, $7x$ is the unit 7 times the irreducible x. Thus, $7x$ is irreducible in $\mathbb{Q}[x]$.

Corollary 1.100. Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. Suppose the gcd of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

And now for the moment you've all been waiting for.

Theorem 1.101. The ring R is a UFD iff $R[x]$ is a UFD.

Corollary 1.102. If R is a UFD, then a polynomial ring in an arbitrary number of variables is also a UFD.

Example 1.103. The polynomial rings $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{Z}[x,y]$, and $\mathbb{Q}[x,y]$ are all UFDs. Note that $\mathbb{Z}[x]$ is an example of UFD that is not a PID. Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD (and hence not a PID and not a Euclidean Domain), the polynomial ring $(\mathbb{Z}[\sqrt{-5}])[x]$ is not a UFD.

In light of Theorem 1.101, it is natural to wonder what the irreducible elements in $R[x]$ look like when R is a UFD. Note that a nonconstant monic polynomial is irreducible if it cannot be factored as the product of two other polynomials of smaller degrees. In general, determining whether a polynomial factors is a difficult problem. If R is a UFD, Gauss' Lemma guarantees that it is enough to consider factorizations in $F[x]$, where F is the field of fractions of R.

The next theorem tackles the case when there is a linear factor. It tells us that polynomials over a field behave in a way that we are familiar with.

Theorem 1.104. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree 1 iff $p(x)$ has a root in F.

Corollary 1.105. A polynomial of degree 2 or 3 over a field F is reducible iff it has a root in F.

The next result should look familiar from precalculus. Note that the theorem is stated in terms of $\mathbb{Z}$, but generalizes to $R[x]$, where R is any UFD.

Theorem 1.106 (Rational Root Test)**.** Let $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_n \neq 0$. If $r/s \in \mathbb{Q}$ is in lowest terms and r/s is a root of $p(x)$, then r divides a_0 and s divides a_n.

Corollary 1.107. Let $p(x) = x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_n \neq 0$. If $p(d) \neq 0$ for all integers d dividing a_0, then $p(x)$ has no roots in $\mathbb{Q}$.

Example 1.108. Let's tinker with a few examples.

(1) Consider the polynomial $p(x) = x^3 - 3x - 1$ in $\mathbb{Z}[x]$. We will argue that $p(x)$ is irreducible in $\mathbb{Z}[x]$. By the Rational Root Test, the only eligible rational roots are integers that divide the constant term 1, namely ± 1. But $p(\pm 1) \neq 0$. So, $p(x)$ does not have any roots in $\mathbb{Q}$, which implies that $p(x)$ is irreducible over $\mathbb{Q}$ by Corollary 1.105. Thus, $p(x)$ is irreducible over $\mathbb{Z}$.

(2) Consider the polynomials $x^2 - p$ and $x^3 - p$ in $\mathbb{Z}[x]$, where p is prime. We claim that both polynomials are irreducible. By the Rational Root Test, the only candidates for (rational) roots are ± 1 and $\pm p$. But none of these are roots for either polynomial. By Corollary 1.105, both polynomials are irreducible over $\mathbb{Q}$.

(3) The polynomial $x^2 + 1$ is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since 1 is a root. We see that $x^2 + 1 = (x + 1)(x + 1)$ in $\mathbb{Z}/2\mathbb{Z}[x]$.

(4) Consider the polynomial x^2+x+1 in $\mathbb{Z}/2\mathbb{Z}[x]$. In $\mathbb{Z}/2\mathbb{Z}$, $0^2+0+1=1\neq 0$ and $1^2+1+1=1\neq 0$. So, the polynomial does not have a root in $\mathbb{Z}/2\mathbb{Z}$. Once again, Corollary 1.105 tells us that the polynomial is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$. The same approach works for x^3+x+1 in $\mathbb{Z}/2\mathbb{Z}[x]$.

Notice that the approach in the examples above does not generalize to polynomials of larger degree since it relies on having a linear factor. It is possible for a polynomial of degree 4 to factor into two irreducible polynomials of degree 2, and hence have no linear factors. Occasionally, the next result can be used to circumnavigate this difficulty.

Theorem 1.109. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Unfortunately, there are examples of polynomials in $\mathbb{Z}[x]$ that are irreducible but whose reductions modulo every ideal are reducible, and so their irreducibility is not evident by the previous theorem.

Example 1.110. Some details omitted.

(1) Consider the polynomial x^2+x+1 in $\mathbb{Z}[x]$. Reducing modulo 2, we see that x^2+x+1 is irreducible in in $\mathbb{Z}/2\mathbb{Z}[x]$ by Example 1.108(4). Then the previous theorem tells us that the original polynomial is irreducible in $\mathbb{Z}[x]$. The same approach works for the polynomial x^3+x+1 in $\mathbb{Z}[x]$.

(2) The polynomial x^2+1 is irreducible in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$ (since it has no root in $\mathbb{Z}/3\mathbb{Z}$). However, it is reducible mod 2 by Example 1.108(3). This shows that the converse of the previous theorem is false.

Theorem 1.111 (Eisenstein's Criterion)**.** Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $n \geq 1$. Suppose $a_{n-1}, \ldots, a_1, a_0 \in P$ while $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.

Eisenstein's Criterion is most frequently applied to $\mathbb{Z}[x]$.

Corollary 1.112. Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. Suppose p divides $a_{n-1}, \ldots, a_1, a_0 \in P$ while p^2 does not divide a_0. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Example 1.113. Some details omitted.

(1) The polynomial $x^4 + 10x + 5$ in $\mathbb{Z}[x]$ is irreducible by Eisenstein's Criterion (applied for the prime 5).

(2) If a is any integer divisible by a prime p but not divisible by p^2, then $x^n - a$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion. In particular, $x^n - p$ is irreducible for all positive integers n. This implies that for $n \geq 2$, the nth roots of p are not rational numbers.

The next result follows immediately from Theorems 1.63 and 1.82 (where $F[x]$ is the corresponding PID).

Theorem 1.114. Let F be a field. Then the maximal ideas in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field iff $f(x)$ irreducible.

Here's one last for this section.

Theorem 1.115. Let F be a field. If the polynomial $f(x) \in F[x]$ has roots $\alpha_1, \ldots, \alpha_k$ in F (not necessarily distinct), then $f(x)$ has $(x-\alpha_1)\cdots(x-\alpha_k)$ as a factor. In particular, if $\deg(f(x)) = n$, then $f(x)$ has at most n roots (even when counting multiplicity).

2 Field Theory

This chapter loosely follows Chapter 13 of Dummit and Foote.

2.1 Field Extensions

We begin with a definition that you encountered on a previous homework problem.

Definition 2.1. Let R be a ring with $1 \neq 0$. We define the **characteristic** of R, denoted $\mathrm{Char}(R)$, to be the smallest positive integer n such that $n \cdot 1_R = 0$ if such an n exists and to be 0 otherwise.

Note that $n \cdot 1_R$ is an shorthand for

$$\underbrace{1_R + \cdots + 1_R}_{n \text{ terms}}.$$

The integer n may not even be in R.

Example 2.2. Here are a few quick examples.

(1) The characteristic of the ring $\mathbb{Z}/n\mathbb{Z}$ is n. In particular, if p is prime, then the field $\mathbb{Z}/p\mathbb{Z}$ has characteristic p. The polynomial ring $\mathbb{Z}/n\mathbb{Z}[x]$ also has characteristic n.

(2) The ring $\mathbb{Z}$ has characteristic 0.

(3) The fields $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ all have characteristic 0.

(4) If F is a field with characteristic 0, then $F[x]$ has characteristic 0.

The next theorem tells us what the possible characteristics are for integral domains.

Theorem 2.3. Let R be an integral domain. Then $\mathrm{Char}(R)$ is either 0 or a prime p.

Theorem 2.4. If R is an integral domain such that $\mathrm{Char}(R) = p$ (p prime), then

$$p \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{p \text{ terms}} = 0.$$

Theorem 2.5. The characteristic of an integral domain is the same as its field of fractions.

It turns out that if F is a field, F either contains a subfield isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ depending on whether $\mathrm{Char}(F)$ is 0 or p (for p prime). To see why this is true, define $\phi : \mathbb{Z} \to F$ via $\phi(n) = n \cdot 1_F$, where we interpret $(-n) \cdot 1_F = -(n \cdot 1_F)$ for positive n and $0 \cdot 1_F = 0$. Then $\ker(\phi) = \mathrm{Char}(F)\mathbb{Z}$. The First Isomorphism Theorem for Rings tells us that there is an injection of either $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ into F. This implies that F either contains a subfield isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, depending on the characteristic of F. In either case, this subfield is the smallest subfield containing 1_F, which we call the **subfield generated by** 1_F.

The next definition makes sense in light of the discussion above.

Definition 2.6. The **prime subfield** of a field F is the subfield generated by 1_F (i.e., the smallest subfield of F containing 1_F).

Note that the prime subfield of F is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$.

Example 2.7. Here are a couple quick examples.

(1) The prime subfield of both $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$.

(2) The prime subfield of the field of rational functions with coefficients from the field $\mathbb{Z}/p\mathbb{Z}$ (denoted $\mathbb{Z}/p\mathbb{Z}(x)$) is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Definition 2.8. If K is a field containing the subfield F, then K is said to be an **extension field** (or simply an **extension**) of F, denoted K/F and read "K over F" (not be be confused with quotients!). The field F is called the **base field** of the extension.

Note that every field is an extension of its prime subfield.

Note 2.9. If K/F is a field extension, then we can interpret K as a vector space over F. In this case, K is the set of vectors and the scalars are coming from F.

Definition 2.10. The **degree** (or **index**) of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e., $[K : F] = \dim_F(K)$).

Example 2.11. For example, $[\mathbb{C} : \mathbb{R}] = 2$.

If we are given a polynomial $p(x)$ in $F[x]$, it is possible that $p(x)$ does not have any roots in F. It is natural to wonder if there is an extension K of F such that $p(x)$ has roots in K.

For example, consider the polynomial $x^2 + 1$ in $\mathbb{R}[x]$. We know that this polynomial does not have a root in $\mathbb{R}$. However, this polynomial has roots in $\mathbb{C}$.

Note that given any polynomial $p(x)$ in $F[x]$, any root of a factor of $p(x)$ is also a root of $p(x)$. It is enough to consider the case where $p(x)$ is irreducible.

Theorem 2.12. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.