MATH 436 Notes: Factorization in Commutative Rings.

Jonathan Pakianathan

December 2, 2003

1 Prime and Maximal Ideals

Throughout this section, ideal always means two-sided ideal.

The following proposition is basic and its proof is left to the reader:

Proposition 1.1. *Let $f : R_1 \to R_2$ be a homomorphism of rings.*
If J is an ideal of R_2, then $f^{-1}(J)$ is an ideal of R_1 containing $ker(f)$ and furthermore $f(f^{-1}(J)) \subseteq J$.

Now let $f : R_1 \to R_2$ be an **epimorphism** *of rings.*
If J is an ideal of R_2 then $f(f^{-1}(J)) = J$. If I is an ideal of R_1 then $f(I)$ is an ideal of R_2. Furthermore we have $I \subseteq f^{-1}(f(I)) = I + ker(f)$ and thus $I = f^{-1}(f(I))$ if I contains $ker(f)$.

Thus if $f : R_1 \to R_2$ is an epimorphism of rings, then there is a bijective correspondence:

$$\{ \text{ Ideals of } R_1 \text{ which contain } ker(f)\} \leftrightarrow \{ \text{ Ideals of } R_2\}$$

given by $I \leftrightarrow J$ when $I = f^{-1}(J)$ or equivalently when $f(I) = J$.

We now introduce two types of ideals which will play an important role in the future.

Definition 1.2 (Prime Ideals). *P is called a prime ideal of R if P is a proper ideal of R with the property that*

$$ab \in P \implies (a \in P) \vee (b \in P).$$

Definition 1.3 (Maximal Ideals). *M is called a maximal ideal of R if M is a proper ideal of R with the property that if $M \subseteq I \subseteq R$ for some ideal I of R then $(M = I) \vee (I = R)$.*

Proposition 1.4 (Characterization of Prime and Maximal Ideals). *Let R be a ring and I an ideal of R then:*
(1) I is a prime ideal if and only if R/I is a nonzero integral ring.
(2) I is a maximal ideal if and only if R/I is a simple ring.

Proof. First of all the fact that I is proper is equivalent to R/I being not equal to the zero ring.

For any $a, b \in R$ we let $\bar{a}, \bar{b}$ denote their images in R/I. Then we have the following:

$$\bar{a}\bar{b} = \bar{0} \leftrightarrow ab \in I.$$
$$(\bar{a} = \bar{0}) \vee (\bar{b} = \bar{0}) \leftrightarrow (a \in I) \vee (b \in I).$$

Thus the implication $\bar{a}\bar{b} = \bar{0} \implies (\bar{a} = \bar{0}) \vee (\bar{b} = \bar{0})$ is logically equivalent to the implication $ab \in I \implies (a \in I) \vee (b \in I)$ which gives us (1).

For (2), recall that Proposition 1.1 gives us a bijective correspondence

$$\{ \text{ Ideals of } R/I \} \leftrightarrow \{ \text{ Ideals of } R \text{ containing } I \}$$

given by $J \leftrightarrow \phi^{-1}(J)$ where $R \xrightarrow{\phi} R/I$ is the canonical quotient homomorphism.

Thus it is easy to see that I is maximal if and only if the only ideals of R/I are 0 and R/I, i.e., R/I is a simple ring.

□

For commutative rings this specializes to:

Corollary 1.5 (Characterization of prime and maximal ideals in commutative rings). *Let R be a commutative ring and I an ideal. Then:*
(1) I is prime if and only if R/I is a nonzero integral domain.
(2) I is maximal if and only if R/I is a field.

Thus in particular in a commutative ring, every maximal ideal is a prime ideal.

Proof. Part (1) follows immediately from Proposition 1.4. Part (2) also follows when one notes that every commutative simple ring R is a field. (Since for any nonzero element $x \in R$ we have $(x)_L = (x) = (x)_R = R$ by simplicity which shows that x is a unit.)

Finally since every field has no zero divisors, every field is an integral domain and hence maximal ideals must be prime ideals.

□

Example 1.6 (Maximal ideals need not be prime in noncommutative rings). *Consider $R = Mat_2(\mathbb{R})$ the ring of 2×2 matrices with real entries.*

Then R is a simple ring so $\{\mathbb{O}\}$ is a maximal (two-sided) ideal. However $\{\mathbb{O}\}$ is not a prime ideal as there exist nonzero matrices $\mathbb{A}, \mathbb{B}$ with $\mathbb{AB} = \mathbb{O}$.

We next show that the preimage mapping preserves the property of being a prime ideal:

Proposition 1.7. *Let $f : R_1 \to R_2$ be a homomorphism of rings and let J be an ideal of R_2.*
(1) If J is a proper ideal of R_2 then $f^{-1}(J)$ is a proper ideal of R_1.
(2) If J is a prime ideal of R_2 then $f^{-1}(J)$ is a prime ideal of R_1.

If $f : R_1 \to R_2$ is an **epimorphism** *of rings then:*
(3) If J is a maximal ideal of R_2 then $f^{-1}(J)$ is a maximal ideal of R_1.

Proof. For (1), note that J proper in R_2 means $1 \notin J$ and so $1 \notin f^{-1}(J)$ and hence $f^{-1}(J)$ is a proper ideal of R_1.

For (2), suppose J is a prime ideal in R_2 and let $ab \in f^{-1}(J)$. Then $f(ab) = f(a)f(b) \in J$. Since J is prime, this gives $(f(a) \in J) \vee (f(b) \in J)$. Thus $(a \in f^{-1}(J)) \vee (b \in f^{-1}(J))$ and thus $f^{-1}(J)$ is a prime ideal in R_1.

For (3), suppose J is a maximal ideal in R_2 and f is an epimorphism. Let I be an ideal of R_1 such that $f^{-1}(J) \subseteq I \subseteq R_1$. Then applying f to this chain of inclusions we find $J \subseteq f(I) \subseteq R_2$. Since J is maximal this gives $f(I) = J$ or $f(I) = R_2$. Since I contains $f^{-1}(J)$, it contains $ker(f)$ from which it follows that $f^{-1}(f(I)) = I + ker(f) = I$ and so $I = f^{-1}(J)$ or $I = f^{-1}(R_2) = R_1$. Hence $f^{-1}(J)$ is a maximal ideal of R_1.

□

Example 1.8 (Preimages of maximal ideals need not be maximal). *Let R be an ID contained inside a field F, e.g. $\mathbb{Z} \subseteq \mathbb{Q}$ and consider the inclusion homomorphism of rings $i : R \to F$ given by $i(r) = r$ for all $r \in R$.*

Then $i^{-1}(0) = (0)$ and (0) is maximal in F but not necessarily in R. For example (0) is not a maximal ideal in $\mathbb{Z}$ since $(0) \subset (2) \subset \mathbb{Z}$.

Definition 1.9 (Spec). *Let R be a ring. We define $Spec(R)$ to be the set of all prime ideals of R. This is called the prime ideal spectrum of R. If $f : R_1 \to R_2$ is a ring homomorphism we define the function $Spec(f) : Spec(R_2) \to Spec(R_1)$ by $Spec(f)(P) = f^{-1}(P)$. This is a well-defined function by Proposition 1.7.*

Since $(g \circ f)^{-1}(P) = f^{-1}(g^{-1}(P))$ in general, it follows that Spec is a contravariant functor from the category of rings and ring homomorphisms to the category of sets and functions.

We may also define $MaxSpec(R)$ to be the set of all maximal ideals of R. This is called the maximal ideal spectrum of R. When R is a commutative ring, $MaxSpec(R) \subseteq Spec(R)$. However in general $MaxSpec$ does not give us a functor from the category of rings to the category of sets as the preimage of a maximal ideal need not be maximal.

1.1 Zorn's Lemma

Before we go on to a discussion of factorization in commutative rings. There is one final fact about maximal ideals we would like to mention and that is any proper (left) (right) (two-sided) ideal I of a ring R is contained in a maximal (left) (right) (two-sided) ideal of R.

For (left) (right) (two-sided) Noetherian rings this follows by applying the Noetherian property to the nonempty set of proper (left) (right) (two-sided) ideals containing I.

However the general case requires the use of Zorn's lemma which we recall next:

Definition 1.10 (Poset). *A partially ordered set $(P, \preceq)$ is a set P together with a relation $\preceq$ which satisfies:*
(1) $x \preceq x$ for all $x \in P$ [Reflexivity]
(2) $x \preceq y$ and $y \preceq x \implies x = y$ for all $x, y \in P$. [Anti-symmetry]
(3) $x \preceq y$ and $y \preceq z \implies x \preceq z$ for all $x, y, z \in P$. [Transitivity].

We often call a partially ordered set a poset.

Definition 1.11. *Given a poset $(P, \preceq)$, a subset C is called a chain if any two elements $x, y \in C$ are comparable i.e., either $x \preceq y$ or $y \preceq x$.*

An upper bound for a chain C is an element $\alpha \in P$ such that $x \preceq \alpha$ for all $x \in C$.

A maximal element of P is an element $m \in P$ such that for any $x \in P$, $m \preceq x \implies m = x$.

Example 1.12. *Let $S = \{1, 2, 3\}$ be a set and let $P = \{A \subseteq S | A \neq S\}$ be a poset under the relation given by inclusion of sets.*

Note the elements $\{1, 2\}, \{2, 3\}$ and $\{1, 3\}$ are the maximal elements of P.

Also note that $\{\{1, 2\}, \{2, 3\}\}$ forms a subset of 2 elements in P which is not a chain in P.

On the other hand $\{\emptyset, \{1\}, \{1, 2\}\}$ is a chain in P with upper bound $\{1, 2\}$.

We now state Zorn's Lemma:

Lemma 1.13 (Zorn's Lemma). *Let $(P, \preceq)$ be a nonempty poset such that every (nonempty) chain has an upper bound. Then $(P, \preceq)$ has a maximal element.*

As an application, we prove:

Proposition 1.14 (Proper ideals are contained in maximal ideals). *Let R be a ring and let I be a proper (left) (right) (two-sided) ideal of R. Then I is contained in a maximal (left) (right) (two-sided) ideal of R.*

Proof. We will do the case for left ideals, the other cases are similar and left to the reader.

Let P be the poset of proper left ideals of R which contain I, ordered by inclusion. Thus $(P, \subseteq)$ is a nonempty poset as it contains I.

Let C be a nonempty chain in $(P, \subseteq)$. Consider $K = \cup_{J \in C} J$. Then since each $J \in C$ is a proper left ideal, it does not contain 1, and thus K does not contain 1. Also given $x, y \in K$ then $x \in J_x$ and $y \in J_y$ for some $J_x, J_y \in C$. Since C is a chain, one of J_x or J_y is contained in the other. WLOG $J_x \subseteq J_y$. Then $x + y \in J_y \subseteq K$ as J_y is a left ideal of R. Similarly $ry \in J_y \subseteq K$ for any $r \in R$. Thus we see that K is a proper left ideal of R which contains I as the $J \in C$ contain I. Thus $K \in P$ is an upper bound for the chain C.

So we have shown that every chain in the nonempty poset $(P, \subseteq)$ has an upper bound. Thus by Zorn's Lemma, there is a maximal element M in $(P, \subseteq)$. It is then clear that M is a maximal left ideal containing I. $\square$

2 Factorization in Commutative Rings

For the remainder of this section, all rings will be commutative (with 1).

Recall that one of the most important facts when dealing with integers is that every nonzero integer can be written **uniquely** as $n = \pm p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where $p_1 < p_2 < \cdots < p_k$ are primes and $\alpha_j \geq 1$ are integers. Notice $Units(\mathbb{Z}) = \{\pm 1\}$, thus every nonzero integer can be written uniquely as a unit times a product of primes to uniquely determined powers.

This fact is so important that it is sometimes refered to as the fundamental theorem of arithmetic. We will seek to find a similar factorization theorem in a more general class of rings. We will see that in fact there are two important properties of the prime numbers in $\mathbb{Z}$ that we will need to generalize. One of these properties will give us the existance of factorizations as above and the other will give us the uniqueness of the factorizations. Unfortunately, in a general ring, the two properties are not the same as we will see in examples later.

Before we define these two properites, let us define the concept of division for general rings:

Definition 2.1 (Division). *Let R be a commutative ring. If $a, b \in R$ then we say "a divides b" and write $a|b$ if $ax = b$ for some $x \in R$.*

Note that $a|b \leftrightarrow b \in (a) \leftrightarrow (b) \subseteq (a)$ for all $a, b \in R$.

The reader is encouraged to note once and for all that $a|b$ if and only if $(b) \subseteq (a)$, i.e., the "reverse" inclusion of ideals holds.

Definition 2.2 (Associates). *Let R be a commutative ring. If $a|b$ and $b|a$ then we call a and b associates. Note that a and b are associates if and only if $(a) = (b)$.*

Thus the relation of being associates defines an equivalence relation on R. Note that if u is a unit of R then $(a) = (au)$ and so a and au are associates.

On the other hand, suppose a and b are associate. Then we have $a = xb$ and $b = ya$ for some $x, y \in R$. Thus if one of a or b is zero, so is the other and so $a = 1b$. On the other hand if a and b are nonzero then we have $b = xyb$. Thus as long as R is an integral domain, we may cancel b and conclude $xy = 1$ and so x, y are units of R, and $b = ya$.

Thus we see that in an integral domain R, we have a is associate to b if and only if $a = bu$ where u is a unit of R.

We are now ready to define the two concepts mentioned in the beginning of this section:

Definition 2.3 (Primes). *Let R be a commutative ring. A nonzero, nonunit element $p \in R$ is called a prime if for any $a, b \in R$, whenever $p|ab$ then $(p|a) \vee (p|b)$.*

Definition 2.4 (Irreducibles). *Let R be a commutative ring. A nonzero, nonunit element $\alpha \in R$ is called irreducible when*

$$(\alpha = xy \text{ with } x, y \in R) \implies (x \text{ a unit of } R) \vee (y \text{ a unit of } R).$$

A nonzero, nonunit element β is called reducible in R if $\beta = xy$ where $x, y \in R$ but neither x or y are units of R.

The next proposition characterizes whether an element $\alpha \in R$ has these properties in terms of the principal ideal (α):

Proposition 2.5 (Ideal characterization). *Let R be a commutative ring and take $\alpha \in R$. Then:*
(1) $\alpha = 0 \leftrightarrow (\alpha) = (0)$.
(2) α is a unit of $R \leftrightarrow (\alpha) = R$.
(3) α is a prime of $R \leftrightarrow (\alpha)$ is a nonzero prime ideal of R.
(4) If R is an integral domain then:
α is an irreducible of $R \leftrightarrow (\alpha)$ is a nonzero ideal which is maximal in the poset of all proper principal ideals of R (under inclusion), i.e., $(\alpha) \subseteq (\beta)$ then $(\beta) = (\alpha)$ or $(\beta) = R$.

Thus in an integral domain, any element that is associate to a prime is prime and any element that is associate to an irreducible is irreducible.

Proof. The proofs of (1) and (2) are easy and left to the reader.

Let $\alpha, a, b \in R$.

In general we have the following equivalences:

$$\alpha|ab \leftrightarrow ab \in (\alpha)$$
$$(\alpha|a) \vee (\alpha|b) \leftrightarrow (a \in (\alpha)) \vee (b \in (\alpha)).$$

Thus the implication $\alpha|ab \implies (\alpha|a) \vee (\alpha|b)$ is logically equivalent to the implication $ab \in (\alpha) \implies (a \in (\alpha)) \vee (b \in (\alpha))$.

From this observation, together with part (1) and (2), (3) follows.

Take $\alpha \in R$ nonzero and assume now that R is an integral domain. For (4) first note that $\alpha = ab$, with a, b nonunits is equivalent to $a|\alpha$, a a nonunit with a and α not associate. (For if $\alpha = au$, u a unit then $au = ab$ which gives $u = b$ by cancellation contradicting that b is not a unit.)

Thus $\alpha = ab$ with a, b nonunits is equivalent to $(\alpha) \subset (a) \subset R$ where the inclusions are proper. Thus (4) follows. □

From now on we will confine ourself to dealing with factorization in integral domains. Here we will have the following useful conventions:

Definition 2.6 (Set of prime representatives). *Let R be an integral domain. A set P of prime representatives for R is a subset of R consisting of prime elements such that every prime element in R is associate to a unique element in P. Thus P consists of one element from every associate equivalence class of primes.*

Similarly, a set Irr of irreducible representatives for R is a subset of R consisting of irreducible elements such that every irreducible element in R is associate to a unique element in Irr. Thus Irr consists of one element from every associate equivalence class of irreducibles.

Example 2.7. *In the integral domain $\mathbb{Z}$, being prime is the same as being irreducible and n is associate to $-n$ for all $n \in \mathbb{Z}$. Thus one possible set of prime representatives of $\mathbb{Z}$ is just the set of positive prime numbers which is usually what is meant when someone refers to a prime number in the integers.*

The following proposition describes a relationship between prime and irreducible elements in an integral domain which is fundamental.

Theorem 2.8. *Let R be an integral domain, then every prime element is irreducible.*

Suppose in addition R is a PID, then every irreducible is also prime. Thus in a PID, the set of prime elements is the same as the set of irreducible elements.

Proof. For the first part, let R be an integral domain and let p be a prime element. Suppose $p = ab$ for some $a, b \in R$. Then $p|ab$ and so by the prime property $p|a$ or $p|b$, WLOG let us assume $p|a$. Then $pk = a$ for some $k \in R$ and so $p = pkb$. Since p is nonzero and R is an integral domain this gives that $1 = kb$ and so b is a unit. Thus whenever $p = ab$ one of a or b must be a unit. Thus p is irreducible.

Now assume R is a PID and let α be irreducible. Then (α) is maximal in the set of all proper principal ideals of R. However since all ideals of R are principal, we conclude that (α) is a maximal ideal of R. Thus (α) is a nonzero prime ideal of R and so α is a prime element of R. This concludes the proof.

□

In the homework, you will look at examples of integral domains with irreducible elements which are not prime. It follows that these integral domains are not PIDs.

An important corollary of the previous theorem and its proof is the following:

Corollary 2.9. *If R is a PID then every nonzero prime ideal is maximal. Thus $Spec(R) - \{(0)\} = MaxSpec(R) - \{(0)\}$.*

(0) is always a prime ideal in an integral domain R, but is not a maximal ideal unless R is a field.

Proof. If P is a nonzero prime ideal, then since R is a PID, $P = (p)$. Since such a principal ideal is prime if and only if its generator is, it follows that p is prime. Thus p is irreducible which makes $P = (p)$ maximal in the set of all proper principal ideals and hence maximal in R as every ideal of R is principal. Thus we have shown that any nonzero prime ideal P of R is maximal in R.

The final comments are easy to verify and left to the reader. □

We are now done with enough preliminaries so that we are ready to discuss the issues of factorization.

Theorem 2.10 (Irreducible decompositions in Noetherian IDs). *Let R be a Noetherian integral domain. Then every nonzero element $\alpha \in R$ can be decomposed as $\alpha = u\alpha_1 \dots \alpha_k$ where α_j is irreducible in R for all $1 \leq j \leq k$ and u is a unit of R. We will call such a decomposition a factorization of α into irreducibles.*

Proof. Suppose the theorem is not true. Then the set of nonzero principal ideals

$$S = \{(a) | a \text{ does not have a factorization into irreducibles.}\}$$

is nonempty. Since R is Noetherian, there exists a maximal element of S say (m). If m were a unit or irreducible, it would trivially have a factorization into irreducibles and hence wouldn't be in S which would be a contradiction. Thus $m = ab$ where a, b are nonunits. Thus $(m) \subset (a)$ and $(m) \subset (b)$ where the inclusions are proper. Thus both $(a), (b)$ do not belong to S and so a and b have factorizations into irreducibles which implies $m = ab$ also has a factorization into irreducibles which gives the final contradiction. Thus the set S of elements which do not have such a factorization is empty and so the theorem is proven. □

On the other hand we have the following uniqueness theorem:

Theorem 2.11 (Uniqueness of prime decompositions in IDs). *Let R be an ID and let P be a set of prime representatives for R. Suppose*

$$up_1p_2 \dots p_k = vq_1q_2 \dots q_s$$

where u, v are units in R and $p_j, q_t \in P$ for all $1 \leq j \leq k, 1 \leq t \leq s$. Then $u = v$, $s = k$ and there exists a permutation $\sigma \in \Sigma_k$ such that $q_j = p_{\sigma(j)}$.

Proof. We prove the theorem by induction on k. First we consider the case $k = 0$. Then $u = vq_1 \dots q_s$. If $s \geq 1$ then $q_1|u$ which gives $R = (u) \subseteq (q_1)$ which shows that q_1 is a unit. This contradicts that prime elements are not units. Thus $s = 0$ and $u = v$ and so we are done in this case.

Thus assume $k > 0$ and that all smaller cases have been proven.

Consider p_1 since p_1 divides the left hand factorization, it also divides the right hand factorization as the two factorizations equal the same element. Since p_1 is prime, it follows that p_1 divides one of $v, q_1, \dots, q_s$. $p_1|v$ yields $R = (v) \subseteq (p_1)$ giving a contradiction as before so p_1 divides one of the q_j. After reordering and reindexing we may assume p_1 divides q_1. Thus $p_1x = q_1$. Since q_1 is prime, it is irreducible and so x must be a unit. Thus p_1 and q_1 are associates. Since we are using a set of prime representatives we can conclude that $q_1 = p_1$.

Thus we have $up_1p_2 \dots p_k = vp_1q_2 \dots q_s$. After cancelling p_1 this yields $up_2 \dots p_k = vq_2 \dots q_s$. Thus by induction, $u = v, k = s$ and the q_j's are a reordering of the p_j's.

Thus by induction we are done. □

We are now ready to state our main factorization theorem. First a definition:

Definition 2.12 (UFDs). *Let R be an integral domain and let Irr be a set of irreducible representatives. R is called a unique factorization domain (abbreviated UFD) if every nonzero element α has a* **unique** *factorization $\alpha = u\prod_{p\in Irr} p^{\nu_p(\alpha)}$ where $\nu_p(\alpha) \in \mathbb{N}$ are nonzero for only finitely many $p \in Irr$ and u is a unit in R. Uniqueness means that the unit u and the numbers $\nu_p(\alpha), p \in Irr$ are determined uniquely by α.*

It is not hard to show that in any UFD, the prime elements are the same as the irreducible elements. For if β is irreducible and $\beta|ab$ then $\beta x = ab$. (If $a = 0$ then $\beta|a$ and similarly $\beta|b$ when $b = 0$ so assume a, b are nonzero) Let Irr be a set of irreducible representatives which includes β and factor x, a, b into irreducibles. By the uniqueness of such factorizations and the equality $\beta x = ab$ it follows that β must occur in the factorizations of either a or b and hence β must divide either a or b. Thus irreducible elements in a UFD are indeed prime.

However the prime and maximal ideals of a UFD can be wildly different as we will see later as not every ideal need be principal.

The following fundamental theorem follows now easily from our previous work in Theorem 2.10 and Theorem 2.11.

Theorem 2.13 (Fundamental Factorization Theorem). *Let R be a Noetherian ID such that every irreducible element is prime, then R is a UFD.*

Thus in particular, every PID is a UFD.

In following sections we will strive to give many examples of PIDs. It follows from the theorem above, that we will be able to factor nonzero elements uniquely into products of irreducible elements which will be important in many applications!