

Math 551 – Algebra – Fall 2000

Richard Lyons
Rutgers University
New Brunswick, New Jersey, USA

D. Factorization in Commutative Rings.

We have touched on this subject above, in particular defining UFD 's, and the terms “prime element” and “irreducible element”. We first review some of the rudiments of ring theory.

1. Rings.

1a. Rudiments

A ring is an abelian group $(R, +)$ together with a bilinear multiplication operation $(r, s) \mapsto rs$ (i.e., both left and right distributive laws hold). The ring is **associative** if and only if multiplication operation is associative. The ring is a ring with identity if and only if there is an identity element 1 for multiplication. Generally when one speaks of a “ring” one means an associative ring with identity, so it is best to use terminology like (not necessarily associative) ring when speaking of non-associative rings. Sometimes a ring in which no assumption is made about the existence of an identity can also be called a rng.

A homomorphism of rings $\phi : R \rightarrow S$ is a mapping which preserves addition and multiplication. A homomorphism of rings with identity $\phi : R \rightarrow S$ is a homomorphism of rings such that $\phi(1_R) = 1_S$.

Unless otherwise specified we shall take “ring” to mean ring with identity, and homomorphisms will be assumed to take 1 to 1.

An isomorphism of rings is a bijective homomorphism of rings.

A ring R commutative if and only if the multiplication in R is commutative.

If A and B are subsets of the ring R , then

$$AB = \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbf{Z}^+, a_i \in A \text{ and } b_i \in B \forall i = 1, \dots, n \right\}.$$

Thus by definition AB is closed under multiplication, and if A and B are additive subgroups of R , then so is AB .

A subring $S \subseteq R$ of a ring is a subset which is a ring with respect to the same operations, and (in the case of rings with identity) such that $1_S = 1_R$. A (left, right, two-sided) ideal of R is an additive subgroup I of R such that, respectively, $RI \subseteq I$, $IR \subseteq I$, or $RIR \subseteq I$. (Since $1 \in R$, these are equivalent to $RI = I$, $IR = I$, $RIR = I$.)

If I is a 2-sided ideal of R , then R/I has the binary operation $(r + I) \cdot (s + I) = rs + I$ (this is not the notion of multiplication of subsets displayed above!!). Since $Is \subseteq I$ and $rI \subseteq I$, this operation is well-defined, i.e., independent of the coset representatives r and s , but dependent only on the cosets $r + I$ and $s + I$.

It is trivial to check that then R/I is a ring, and that the projection $\pi_I : R \rightarrow R/I$ is a ring homomorphism.

The kernel of a ring homomorphism $\phi : R \rightarrow S$ is $\ker \phi = \{r \in R \mid \phi(r) = 0\}$.

First Isomorphism Theorem. *Let $\phi : R \rightarrow S$ be a ring homomorphism. Then $\ker \phi$ is an ideal of R , $\phi(R)$ is a subring of S , and $R/\ker \phi \cong \phi(R)$ via the mapping $(r + \ker \phi) \mapsto \phi(r)$.*

Third Isomorphism Theorem. *Let $\phi : R \rightarrow S$ be a surjective homomorphism of rings. Then the mappings $I \mapsto \phi(I)$ and $J \mapsto \phi^{-1}(J)$ induce inverse bijections between the set of all (left, right, two-sided) ideals of R containing $\ker \phi$ and the set of all (left, right, two-sided) ideals of S . Moreover for any two-sided ideal I of R such that $\ker \phi \subseteq I$, we have $R/I \cong S/\phi(I)$.*

The proofs are virtually the same as for groups and are left to the reader.

1b. Examples

- (a) \mathbf{Z} , \mathbf{Q} ; any field (a commutative ring R in which every element of $R - \{0\}$ has a multiplicative inverse).
- (b) If R is a ring and $X \subseteq R$ is any subset, then the intersection of all subrings of R containing X is a subring, called $[X]$, the subring generated by X . It consists of all sums and differences of products of elements of X (including the empty product 1_R).
- (c) The ring of real quaternions, which is the four-dimensional real vector space

$$\mathcal{H} = \{\alpha 1 + \beta i + \gamma j + \delta k \mid \alpha, \beta, \gamma, \delta \in \mathbf{R}\}$$

in which multiplication is defined by specifying $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, and then defining products of arbitrary elements using these definitions and distributivity. \mathcal{H} is an example of an \mathbf{R} -algebra (an F -algebra, F any field, is a ring which is also an F -vector space and such that $\alpha(rs) = (\alpha r)s = r(\alpha s)$ for all $\alpha \in F$ and all $r, s \in R$). Moreover, every nonzero element of \mathcal{H} has an inverse; namely if for any $x = \alpha 1 + \beta i + \gamma j + \delta k \in \mathcal{H}$ we set

$$\|x\|^2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \text{ and } \bar{x} = \alpha 1 - \beta i - \gamma j - \delta k,$$

then $x\bar{x} = \|x\|^2$, and $\|x\| = 0$ if and only if $x = 0$, so $x^{-1} = (\|x\|)^{-1}\bar{x}$ for any $x \neq 0$. A (noncommutative) ring in which every nonzero element has a multiplicative inverse is a **division ring**, and \mathcal{H} is then a **division algebra**. It

has \mathbf{C} as a subring, namely the subring generated by 1 and i . (Also the subring generated by 1 and j is a copy of \mathbf{C} .)

- (d) If R is a ring and X is an indeterminate, then $R[X]$, the set of all polynomials in X with coefficients in R , is a ring under the obvious operations.
- (e) There are many variations on (d).
- (1) We may similarly form $R[X_1, \dots, X_n]$ for any finite number of (multiplicatively commuting) indeterminates X_1, \dots, X_n ; as an R -module this is free, and the monomials $X_1^{e_1} \cdots X_n^{e_n}$, all $e_i \geq 0$, form a basis. One can generalize this further by allowing an infinite number of indeterminates (although all monomials are of course of finite degree); thus for any set \mathcal{S} of indeterminates there is a polynomial ring $R[\mathcal{S}]$. If \mathcal{S} and \mathcal{T} are disjoint then there is an isomorphism $R[\mathcal{S} \cup \mathcal{T}] \cong (R[\mathcal{S}])[\mathcal{T}]$.
 - (2) $R[[X]]$ is the set of formal power series in X with coefficients in R , multiplied by the usual formal rule. The ring $R[X]$ is a subring, but a small one.
 - (3) One can form polynomials in several indeterminates X_1, \dots , but impose no multiplicative commutativity condition on the X_i . (However, elements of R commute with the X_i , so that the ring is a free R -module, with an R -basis consisting of all monomials which are words in X_1, \dots , (without inverses).
- (f) If α is an algebraic integer ($\alpha \in \mathbf{C}$ and α is a root of a monic integer polynomial, say of degree n) then $\mathbf{Z}[\alpha]$ is a ring and as abelian group is finitely generated (by $1, \alpha, \dots, \alpha^{n-1}$.) Thus we have $\mathbf{Z}[\sqrt{5}]$, $\mathbf{Z}[e^{2\pi i/n}]$, etc.
- (g) If R is a ring then $R^{n \times n}$, the set of $n \times n$ matrices with entries in R , is a ring, containing R as a subring.
- (h) The set of meromorphic functions on the Riemann sphere (except the constant function ∞) is a ring under pointwise addition and multiplication. So is the set of entire functions. So is the set $\mathbf{C}^n(U)$ of continuously n -times differentiable real valued functions on U , U an open subset of \mathbf{R}^m .
- (i) An algebraist's version of this, fundamental to algebraic geometry, is the ring of all complex-valued functions $\mathbf{C}^n \rightarrow \mathbf{C}$ defined by a polynomial in n variables. Again the ring operations are pointwise. One may also restrict to a "Zariski-open" set $U \subseteq \mathbf{C}^n$, defined by the common non-vanishing of some set of polynomials, and consider the ring of all "locally rational" functions $f : U \rightarrow \mathbf{C}$. Such a function by definition is a function such that for each $u \in U$ there is a polynomial g in n variables not vanishing at u and a polynomial h in n variables such that f and h/g agree at each point of U where g does not vanish (in particular at u).

Exercise. If R is a division ring then $R^{n \times n}$ is a simple ring, that is, its only 2-sided ideals are 0 and R . However, as a left R -module, we have ${}_R R = Re_{11} \oplus Re_{22} \cdots \oplus Re_{nn}$, where e_{ii} are the diagonal matrix units; and the Re_{ii} are simple left R -modules, i.e., their only submodules are 0 and themselves.

2. Commutative rings.

We shall concentrate on commutative rings.

2a. Integral domains and fields

Let R be a commutative ring (with 1). The multiplicative powers a^n , $n \geq 0$, are well-defined and satisfy the usual laws $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$. A zero-divisor in R is an element $0 \neq a \in R$ such that $ab = 0$ for some $0 \neq b \in R$. A unit in R is an element $a \in R$ such that $ab = 1$ for some $b \in R$ (equivalently: $1 \in Ra$; equivalently: $Ra = R$). By associativity $(ab)c = a(bc)$, b cannot simultaneously be a unit and a zero-divisor, as we could then arrange $ab = 1$, $c \neq 0$ and $bc = 0$. A nilpotent element in R is $a \in R$ such that $a^n = 0$ for some positive integer n .

Exercise. *The set of nilpotent elements of R is an ideal $N(R)$. The ring $R/N(R)$ has no nilpotent elements other than 0.*

In a field R , every nonzero element is a unit, so there are no zero divisors: a field is an integral domain. The converse is of course false, but just as $\mathbf{Z} \subseteq \mathbf{Q}$ there is a way to embed any integral domain in a field.

If R is an integral domain, then so is the polynomial ring $R[X]$ (and hence by induction on n , the polynomial rings $R[X_1, \dots, X_n]$ are integral domains too). However if R is a field, then $R[X]$ is definitely not a field; X , for instance, has no inverse.

Let R be an integral domain. We construct a “minimal” field containing R as a subring. Namely we consider the set \mathcal{S} of all symbols

$$\frac{a}{b}, \quad a \in R, \quad 0 \neq b \in R,$$

and define the equivalence relation \sim on \mathcal{S} by

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc.$$

(If also $\frac{c}{d} \sim \frac{e}{f}$, then $ad = bc$ and $cf = de$, so $adf = bcf = bde$ and so $af = be$, i.e., $\frac{a}{b} \sim \frac{e}{f}$, proving transitivity.) Let $Q = \mathcal{S}/\sim$ be the set of equivalence classes, and define addition and multiplication on Q by

$$\begin{aligned} \left[\frac{a}{b} \right] + \left[\frac{c}{d} \right] &= \left[\frac{ad + bc}{bd} \right], \\ \left[\frac{a}{b} \right] \left[\frac{c}{d} \right] &= \left[\frac{ac}{bd} \right]. \end{aligned}$$

(Since R is an integral domain and b and d are nonzero, also $bd \neq 0$ so the symbols on the right make sense.) One must check that these operations are well-defined, i.e., do not depend on the choice of representative of the equivalence classes of the two elements on the left. This is straightforward to do, and it is similarly straightforward to check that Q is a commutative ring, in which the 0 element is $\left[\frac{0}{1} \right]$ and the unit element is $\left[\frac{1}{1} \right]$. Now

$[\frac{a}{b}] = [\frac{0}{1}]$ if and only if $a = 0$, by definition. And then if $[\frac{a}{b}]$ is nonzero, i.e., $a \neq 0$, then $[\frac{a}{b}][\frac{b}{a}] = [\frac{ab}{ab}] = [\frac{1}{1}]$. Therefore Q is a field. Q is called the (or a) quotient field of R .

The mapping $i : R \rightarrow Q$ defined by $i(a) = [\frac{a}{1}]$ is easily checked to be a ring homomorphism and is injective. Moreover, it is a universal embedding of R into a field:

Theorem. *Let R be an integral domain, Q its quotient field, and $i : R \rightarrow Q$ the natural mapping. Then for any field F and any injective homomorphism $\phi : R \rightarrow F$, there is a unique homomorphism of rings $\psi : Q \rightarrow F$ making the diagram commute:*

$$\begin{array}{ccc} R & \rightarrow & Q \\ & \searrow & \downarrow \\ & & F \end{array}$$

A “functional” definition of quotient field is as a solution of this universal mapping problem.

Proof. For any $0 \neq a \in R$, $\phi(a) \neq 0$ since ϕ is injective. For the diagram to commute we must have $\psi([\frac{a}{1}]) = \phi(a)$, and so $\psi([\frac{1}{b}]) = \phi(b)^{-1}$ and so

$$\psi([\frac{a}{b}]) = \psi([\frac{a}{1}][\frac{1}{b}]) = \phi(a)\phi(b)^{-1}.$$

This proves uniqueness. On the other hand, it is routine to check that with this definition, ψ is a homomorphism making the diagram commute. QED

Examples of integral domains embedded in their quotient fields are $\mathbf{Z} \subseteq \mathbf{Q}$; for a field F , $F[X] \subseteq F(X)$, where $F(X)$ is the field of rational functions in one variable over F ; (the definition of $F(X)$ is indeed that it is the quotient field of $F[X]$); the several variable analogue $F[X_1, \dots, X_n] \subseteq F(X_1, \dots, X_n)$.

Exercise. *The quotient field of $\mathbf{Z}[X]$ is $\mathbf{Q}(X)$.*

In between \mathbf{Z} and \mathbf{Q} , or between any integral domain and its quotient field, lie many rings, called “localizations” of the integral domain.

2b. Prime and maximal ideals

An ideal P in the commutative ring R is said to be a prime ideal in R if and only if $P \neq R$ and whenever $a, b \in R$ with $ab \in P$, then either $a \in P$ or $b \in P$. Equivalently: R/P is an integral domain. (Sometimes R itself is also called a prime ideal.)

An ideal M in R is maximal if and only if it is maximal with respect to inclusion (among all ideals of R other than R itself). By the third isomorphism theorem, this is equivalent to the condition that R/M have no ideals other than 0 and itself. But this is equivalent to saying that every nonzero element of R/M generates the ideal which is all of R/M , and so is a unit, i.e., R/M is a field.

Proposition. *Let R be a commutative ring and I an ideal in R . Then I is prime if and only if R/I is an integral domain. Also I is maximal if and only if R/I is a field.*

Corollary. *Every maximal ideal in a commutative ring is a prime ideal.*

The existence of maximal ideals in a commutative ring R (with 1) follows from Zorn's Lemma: let \mathcal{S} be the set of all ideals of R other than R itself. The union of a chain of such ideals is again such an ideal (it isn't R since it doesn't contain 1), so Zorn's Lemma implies the existence of a maximal element in \mathcal{S} .

In an integral domain R , (0) is a prime ideal, which is not maximal unless R is a field.

Proposition. *In a PID, every nonzero prime ideal is maximal.*

The same property holds in "Dedekind domains", which include certain subrings of algebraic number fields, e.g., $\mathbf{Z}[\sqrt{3}]$, $\mathbf{Z}[e^{2\pi i/n}]$.

Proof. Let I be a nonzero prime ideal in the PID R . Then $I = Ra$ for some $a \neq 0$, and a is not a unit since $I \neq R$ (by definition of prime ideal). Since R is a PID, it is a UFD. Let p be a prime divisor of a . Then $a = pb$ for some b . Since $a \in Ra$, which is prime, either p or b lies in Ra . Therefore a divides p or b , respectively. But then b or p is a unit. Therefore b is a unit and $I = Rp$. Finally any ideal containing I must be of the form Rc with c dividing p , so c is associated with 1 or p , and hence $Rc = I$ or R . □

However, in the polynomial ring $R = F[X, Y]$ in two variables over a field F , the ideal $I = RX$ is prime; indeed $R/I \cong F[Y]$, an integral domain (check this!). However, I is not maximal, since $J = RX + RY$ is also prime, indeed maximal, as $R/J \cong F$ (check this). The structure of commutative rings is linked with the possible lengths of chains of prime ideals.

2d. Unique Factorization

We have defined UFD's above in the section on the fundamental theorem for finitely generated modules over a PID, and have proved

Theorem. *Let R be a PID. Then R is a UFD.*

In this section we prove:

Theorem. *Let R be a UFD. Then $R[X]$ is a UFD.*

Corollary. *Let R be a UFD, and $n > 0$. Then $R[X_1, \dots, X_n]$ is a UFD.*

The corollary follows by induction and the isomorphism $R[X_1, \dots, X_n] \cong (R[X_1, \dots, X_{n-1}])[X_n]$. ■

To prove the theorem we let F be the quotient field of R and consider the embedding

$$R[X] \subseteq F[X].$$

We know that $F[X]$ is a PID (indeed a Euclidean domain!), hence a UFD. The game is to relate the notions of irreducibility in $R[X]$ and in $F[X]$. But note that even if R is a PID, then $R[X]$ need not be a PID. For example in $\mathbf{Z}[X]$, the ideal I generated by 2 and X is not principal. This is because 2 and X have no common divisors other than units. If I had a single generator x , then x would have to be a unit, so $I = \mathbf{Z}[X]$, a contradiction.

Let us begin with some simple facts about these rings. First of all, the units in $F[X]$ are precisely the nonzero constants. On the other hand, the units in $R[X]$ are the constants which are units in R . Thus some nonunits in $R[X]$ become units in $F[X]$ (namely, constants which are not units in R). This complicates the relationship between the notions of irreducibility in the two rings.

For example, the polynomial $2X$ is irreducible in $\mathbf{Q}[X]$, but reducible in $\mathbf{Z}[X]$ since neither 2 nor X is a unit in $\mathbf{Z}[X]$. To deal with this “trivial” kind of factorization we introduce the notion of “content” and “primitive” polynomial in $R[X]$, and even in $F[X]$.

We have defined two elements $a, b \in R$ to be associated if and only if

$$a = bu \text{ for some unit } u \in R.$$

We extend this definition to arbitrary $a, b \in F$, and say that a and b are R -associated. Thus for example, two rational numbers a, b are \mathbf{Z} -associated if and only if $b = \pm a$.

Recall also that gcd's exist in any UFD.

Definition. Let $f(X) = \sum_i a_i X^i$ be a nonzero polynomial in $R[X]$, with R being a UFD. The content $c(f)$ of f is defined to be

$$c(f) = \gcd_i a_i,$$

the gcd of all the coefficients. (This is defined only up to associates in R .) The nonzero polynomial f is **primitive** if and only if $[c(f)] = [1]$.

Thus $2X$ is not primitive in $\mathbf{Z}[X]$. Factoring out the gcd of the coefficients yields the following canonical factorization:

Lemma. Let $0 \neq f \in R[X]$, R being a UFD. Then there is a primitive polynomial $f_0 \in R[X]$ such that $f = c(f)f_0$. Up to multiplication by units of R , this is the unique factorization of f as an element of R times a primitive polynomial in $R[X]$.

Proof. The existence of the factorization is trivial. If also $f = cf_1$, then c divides all the coefficients of f , so $c|c(f)$, and similarly $c(f)|c$, so $[c(f)] = [c]$, proving the result.

This extends immediately to polynomials in $F[X]$:

contradiction. .

Lemma. Let $0 \neq f \in F[X]$, F being the quotient field of the UFD R . Then there exists a primitive $f_0 \in R[X]$ and an element $c \in F$ such that $f = cf_0$. The element c is unique up to R -association, and f_0 is unique up to multiplication by a unit in R .

Proof. There exists $0 \neq r \in R$ such that $rf \in R[X]$; for example, take r to be the product of all the denominators of the coefficients of f . Then writing $rf = c(rf)f_0$, we get the existence of a factorization, with $c = c(rf)/r$. For uniqueness, if $cf_0 = dg_0$, writing $c = a/b$ and $d = e/f$ we get $af f_0 = beg_0$, so by the uniqueness in the previous lemma, $af = ube$ for some unit $u \in R$. Then $c = ud$ as required. \square

The following basic lemma is very useful for untangling factorizations in $R[X]$.

Gauss' Lemma. Let R be a UFD, and let $f, g \in R[X]$ be primitive polynomials. Then fg is primitive.

Proof. Suppose that fg is not primitive. Then the coefficients of fg are all divisible by some prime $p \in R$. Set $\overline{R} = R/Rp$. The projection $R \rightarrow \overline{R}$ induces a ring homomorphism $R[X] \rightarrow \overline{R}[X]$, which we write as $f \mapsto \overline{f}$. Our condition is that $\overline{fg} = 0$, so $\overline{f}\overline{g} = 0$.

However, p is prime, i.e., $p|ab$ implies $p|a$ or $p|b$ in R . This is precisely the statement that \overline{R} is an integral domain. Hence $\overline{R}[X]$ is as well. Therefore $\overline{f} = 0$ or $\overline{g} = 0$. Therefore p divides all the coefficients of either f or g , a contradiction to the assumed primitivity. \square

Now we can relate divisibility and irreducibility in $R[X]$ and $F[X]$.

Lemma. Suppose that $f, g \in R[X]$ and $f|g$ in $F[X]$. If f is primitive, then $f|g$ in $R[X]$.

Proof. We have $g = fh$ in $F[X]$. Writing $h = ch_0$ with h_0 primitive in $R[X]$ we get $g = c.fh_0$, with fh_0 primitive by Gauss' Lemma. Thus $c(g).g_0 = c.fh_0$, so g_0 and fh_0 are equal up to units in R . Therefore $f|fh_0|g_0|g$. \square

Lemma. Let R be a UFD with quotient field F , and let $f \in R[X]$. If f is constant, then f is irreducible if and only if it is irreducible in R . If f is nonconstant, then f is irreducible if and only if f is irreducible in $F[X]$ and primitive.

Proof. The constant case is obvious, since the units in $R[X]$ are the constants which are units in R . In the nonconstant case, suppose that

$$f = gh \text{ in } R[X], \text{ with neither } g \text{ nor } h \text{ a unit in } R[X].$$

If g or h is constant, then it is not a unit, and as $g|c(f)$, f is not primitive. If neither g nor h is constant, then f is not irreducible in $F[X]$. This proves one direction of the second statement. Conversely, if f is irreducible in $R[X]$, then it is trivially primitive. Moreover if in addition $f = gh$ in $F[X]$, with neither factor constant, then writing $g = cg_0$ and $h = dh_0$ as above, we get $f = (cd)(g_0h_0)$, with $g_0h_0 \in R[X]$ primitive by Gauss' Lemma. But f is

primitive. By the uniqueness of such a factorization, cd is a unit in R . Consequently f is reducible in $R[X]$, contradiction. \square

Proof of theorem. Let f be a nonzero nonunit in $R[X]$. Then f is primitive in $R[X]$, a constant, or a product of these two. In the second case f is the product of irreducibles in R , which are irreducible in $R[X]$ by the previous lemma. In the first case write $f = f_1 \cdots f_n$, an irreducible factorization in $F[X]$. Write each $f_i = c_i g_i$ with the g_i primitive in $R[X]$ and $c_i \in F$. Then $f = (c_1 \cdots c_n) g_1 \cdots g_n$, with each g_i irreducible in $R[X]$ by the previous lemma. Also $g_1 \cdots g_n$ is primitive by Gauss' Lemma, so $c_1 \cdots c_n$ is a unit in R , hence in $R[X]$. This proves the existence of irreducible factorizations.

To prove uniqueness, it suffices to show that every irreducible $f \in R[X]$ is prime. If f is constant and $f|gh$, then $f = c(f)|c(gh) = c(g)c(h)$, then last by Gauss' Lemma, so f divides $c(g)$ or $c(h)$ and hence g or h . If f is not constant, then $f|gh$ in $F[X]$, and f is irreducible in $F[X]$, so $f|g$ or $f|h$ in $F[X]$. Moreover f is primitive. Now if $f|g$, then $g = kf$ in $F[X]$, so $c(g)g_0 = ck_0f$, and by uniqueness, $g_0 = k_0f$, so $f|g_0|g$. \square

Exercise. If R is a UFD, then the power-series ring $R[[X]]$ is also a UFD. Prove this. First show that the units in $R[[X]]$ are those power series f for which $f(0)$ is a unit in R ; then show that the irreducibles in $R[[X]]$ are the irreducibles in R , together with the single monomial X (and its associates).

Exercise. Show that if F is a field, then the ring of Laurent series $\sum_{n=N}^{\infty} a_n X^n$, $a_n \in F$, $N \in \mathbf{Z}$ (not necessarily positive!) is a field, and is the quotient field of $F[[X]]$.

Exercise. Show that when $X^n - 1$ (or any monic integer polynomial) is written as the product of monic irreducibles in $\mathbf{Q}[X]$, then the factors actually lie in $\mathbf{Z}[X]$.

2e. Generalizations: Noetherian Rings

Various important commutative rings arising in algebraic geometry and algebraic number theory are not unique factorization domains, but have closely related but weaker properties. Namely, one can try to “factorize” every ideal, and this is possible in various ways for certain rings which are not PID's. It is important however that the rings be noetherian.

Definition. A commutative ring R is noetherian if and only if it satisfies the following equivalent conditions:

- a) Every ideal of R is finitely generated.
- b) The set of ideals of R satisfies the maximum condition.

Of course fields are noetherian, as is \mathbf{Z} and any PID.

Hilbert Basis Theorem. Let R be a commutative noetherian ring. Then $R[X]$ is noetherian.

There are several immediate corollaries:

Corollary. *If R is commutative and noetherian, then so is $R[X_1, \dots, X_n]$.*

This is immediate by induction on n and the observation $R[X_1, \dots, X_n] \cong R[X_1, \dots, X_{n-1}][X_n]$.
As a special case:

Corollary. *If F is a field, then $F[X_1, \dots, X_n]$ is noetherian.*

Corollary. *Let S be a commutative ring and R a subring such that $S = R[x_1, \dots, x_n]$ for some $x_1, \dots, x_n \in S$, i.e., S is finitely generated as a ring over R . Then S is noetherian.*

In the last corollary, $R[x_1, \dots, x_n]$ means the smallest subring of S containing R and x_1, \dots, x_n . Equivalently it is the set of elements of S which can be written as “polynomials” in x_1, \dots, x_n with coefficients in R . More precisely, given $x_1, \dots, x_n \in S$ there is a ring homomorphism

$$R[X_1, \dots, X_n] \rightarrow R[x_1, \dots, x_n], \quad f \mapsto f(x_1, \dots, x_n)$$

and under the corollary’s hypothesis, this mapping is surjective. Since $R[X_1, \dots, X_n]$ satisfies the maximal condition on the set of ideals, so does $R[x_1, \dots, x_n]$ by the third isomorphism theorem, and this proves the corollary.

Proof of Hilbert Basis Theorem It is enough to show that any ideal I of $R[X]$ is finitely generated.

For any integer n let $\ell_n(I) = \{a \in R \mid \exists f \in I \text{ such that } f = ax^n + \text{lower terms}\}$. Thus $0 \in \ell_n(I)$ as $0 \in I$. Moreover since I is closed under addition and multiplication by elements of R , so is $\ell_n(I)$ for each n . And since I is closed under multiplication by X , $\ell_n(I) \subseteq \ell_{n+1}(I)$.

Thus from I we get the chain of ideals

$$\ell_0(I) \subseteq \ell_1(I) \subseteq \dots$$

of R . Since R is noetherian, this chain terminates, say at $\ell_N(I)$. For each $i = 0, \dots, N$, choose a finite set of generators of $\ell_i(I)$, and for each generator so chosen, choose $f \in I$ of degree i whose leading coefficient is that generator. All the f ’s so obtained comprise a subset S of I with the property that for any $g \in I$ there exist $h_k \in R[X]$ and $f_k \in S$ such that g and $\sum_k h_k f_k$ have the same leading term. (If f has degree at most N , we can take $f_k \in \ell_k(I)$ and $h_k \in R$. If f has degree $m > N$, we can take $f_k \in \ell_N(I)$ and h_k of the form $c_k X^{m-N}$, with $c_k \in R$.) Thus $g - \sum_k h_k f_k$ has degree smaller than that of g . An inductive argument on the degree of g shows that g lies in the ideal generated by S . Hence I is generated by S . QED

A typical such ring arising in algebraic geometry is a quotient of $F[X_1, \dots, X_n]$ by a prime ideal P ; for example $F[X, Y, Z]/(XY - Z^2)$ or $F[X, Y]/(X^2 - Y^3)$. The polynomials being factored out are irreducible, hence prime (as the polynomial ring is a UFD); therefore each generates a prime ideal. These rings need not be UFD’s, however.

Exercise. Show that $F[X, Y]/(X^2 - Y^3)$ is isomorphic to the subring of $F[X]$ generated by F , X^2 and X^3 , and that it is not a UFD.

A substitute for unique factorization in noetherian rings is “Lasker-Noether” decomposition. We prove the existence here but omit discussion of uniqueness, which is not much harder. The basic ideas are those of prime ideal, primary ideal, irreducible ideal and radical ideal.

Definition. Let I be an ideal in the commutative ring R . Then

- a) I is irreducible if and only if whenever $I = J \cap K$, with J and K ideals of R , then either $J = I$ or $K = I$.
- b) I is prime if and only if whenever $I \supseteq JK$, with J and K ideals of R , then either $I \supseteq J$ or $I \supseteq K$. (**Exercise.** Prove that this is equivalent to our previous definition of prime ideal: whenever $ab \in I$, then either $a \in I$ or $b \in I$.)
- c) I is radical if and only if whenever $a \in R$ and $a^n \in I$ for some $n \geq 0$, then $a \in I$.
- d) I is primary if and only if whenever $a, b \in R$ and $ab \in I$, then either $a \in I$ or some power of b lies in I .

It is easy to check that an ideal is prime if and only if it is primary and radical. Furthermore, the properties above are properties of the ring R/I (I is prime iff R/I is an integral domain; I is radical iff R/I has no nonzero nilpotent elements; I is primary iff every zero-divisor in R/I is nilpotent; I is irreducible iff in R/I , any two nonzero ideals have a nonzero intersection.)

Theorem. In a commutative noetherian ring, every ideal is the intersection of a finite number of primary ideals. Every radical ideal is the intersection of a finite number of prime ideals.

Proof. Let R be the ring in question. First we show that every ideal of R is the intersection of finitely many irreducible ideals. If this were false, there would be an ideal I , not so expressible, and maximal with this condition. In particular I could not be irreducible itself, so $I = J \cap K$ with J and K containing I properly. But then J and K are intersections of finitely many irreducible ideals, so I is too, contradiction.

Next we show that every irreducible ideal I must be primary. By the remark after the definition of these terms, we may pass to R/I . Assuming that the intersection of any two nonzero ideals is nonzero (and R is noetherian) we must show that every zero-divisor is nilpotent. Suppose then $a, b \in R$, $ab = 0$, $a \neq 0$, and b is not nilpotent. We must derive a contradiction (to the irreducibility of 0). For each n let $I_n = \{x \in R \mid xb^n = 0\}$, an ideal of R . Clearly $a \in I_1 \subseteq I_2 \subseteq \dots$. Therefore there exists N such that $I_N = I_{N+i}$ for all $i \geq 0$. Now $I_N \cap Rb^N = 0$, since if $rb^N \in I_N$, then $rb^N b^N = 0$, so $r \in I_{2N} = I_N$, so $rb^N = 0$. But I_N contains $a \neq 0$, and Rb^N contains $b^N \neq 0$, so we have contradicted the irreducibility of the 0 ideal. This proves the first statement of the theorem.

Definition. For any ideal I of R the radical \sqrt{I} of I is the ideal defined by

$$\sqrt{I}/I = \{x \in R/I \mid x \text{ is nilpotent.}\}$$

Equivalently, $\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n \geq 0\}$.

The following lemma is left to the reader:

Lemma. In a commutative ring R , if I is an ideal, then I is radical if and only if $I = \sqrt{I}$. Moreover, if J is another ideal, then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. Finally, if I is primary then \sqrt{I} is prime.

(The last statement holds since if $ab \in \sqrt{I}$, then $a^n b^n \in I$ for some n , so $a^n \in I$ or $b^{nN} \in I$, whence a or b lies in \sqrt{I} .)

Returning to our theorem, if I is a radical ideal of R , then we write $I = Q_1 \cap Q_2 \cap \cdots$ as the intersection of primary ideals, and take radicals to conclude that $I = \sqrt{I} = \sqrt{Q_1} \cap \cdots$ is the intersection of prime ideals. QED

Exercise. The intersection of two prime (or even radical) ideals is radical, in any commutative ring.

In $F[X, Y]$, the ideal $I = (XY, Y^2)$ is the intersection $I = J \cap K$, where $J = (X^2, XY, Y^2)$ is primary and $K = (Y)$ is prime. But also $I = J_1 \cap K$, where $J_1 = (X, Y^2)$ is primary. So this decomposition is not unique. It turns out that those ideals Q_i such that the “associated primes” $\sqrt{Q_i}$ are minimal in the set $\{\sqrt{Q_1}, \sqrt{Q_2}, \dots\}$ are unique.

2f. Generalizations: Dedekind Domains

We now consider integral domains in which unique factorization holds for ideals: i.e., every nonzero is uniquely the product of prime ideals. This is an important idea in algebraic number theory because it holds in “rings of algebraic numbers”, such as $\mathbf{Z}[e^{2\pi i/n}]$ for any n , or $\mathbf{Z}[\sqrt{3}]$, or $\mathbf{Z}[(1 + \sqrt{5})/2]$. The connection is provided by the notion of “integrality”.

Definition. Let R be a subring of the commutative ring S . Let $x \in S$. Then x is **integral over R** if and only if there is a **monic** polynomial $f \in R[X]$ such that $f(x) = 0$.

Of course every element $x \in R$ is integral over R , being a root of $X - x$.

Definition. The integral domain R is **integrally closed** if and only if it contains every element of its quotient field which is integral over R .

As an example, notice that $\mathbf{Z}[\sqrt{5}]$ is not integrally closed, since $(1 + \sqrt{5})/2$ is a root of the monic integer polynomial $X^2 - X - 1$. However, every UFD is integrally closed.

Proposition. Every UFD is integrally closed.

Proof. Let R be a UFD and S its quotient field. Let $x = a/b \in S$, with $a, b \in R$, and assume that $f(x) = 0$ where $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, with $a_i \in R$,

$0 \leq i < n$. By cancelling common prime factors of a and b (R is a UFD!) we may assume that they have no common prime factors, i.e. a/b is in “lowest terms”. We must then show that b is a unit in R , which will imply $x \in R$ as desired. But the equation $b^n f(x) = 0$ reads

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n = 0.$$

Solving for a^n we find that $b|a^n$. As a and b have no common prime factor, b must be a unit. QED

Corollary. \mathbf{Z} is integrally closed.

The connection between this notion and factorization of ideals is the following:

Theorem. Let R be an integral domain. Then every ideal of R is uniquely the product of prime ideals, if and only if the following three conditions hold:

- a) R is noetherian.
- b) R is integrally closed.
- c) Every nonzero prime ideal of R is a maximal ideal.

A domain satisfying the three conditions of the theorem is called a **Dedekind domain**.

Before we consider the proof of this theorem, consider consider the ring $R = \mathbf{Z}[\alpha]$, $\alpha = (1 + \sqrt{5})/2$, which is an example of a Dedekind domain. Let us check this.

Integral closure: The quotient field F of R consists of all rational linear combinations of 1 and $\sqrt{5}$; indeed such rational combinations form a field and the quotient field of R must contain all of them. Equivalently, F consists of all rational linear combinations of 1 and α . It is 2-dimensional over \mathbf{Q} . Now suppose that $\beta = a + b\alpha \in F$ is integral over R . Then the powers $1, \beta, \beta^2, \dots, \beta^n, \dots$, after a certain point, are expressible as R -linear combinations of the earlier ones, so the abelian group which they generate (under addition) is finitely generated, say by g_1, \dots, g_m . Thus $\beta g_i = \sum_j c_{ij} g_j$, with the c_{ij} being integers. Therefore β is an eigenvalue of the integer matrix c_{ij} , so is integral over \mathbf{Z} . The elements of $\mathbf{Q}[X]$ satisfied by β thus include a nonzero monic integral polynomial; but also they form an ideal, which is then principal ($\mathbf{Q}[X]$ being a PID) and hence generated by a monic rational polynomial of least degree. By an exercise above, this monic minimal polynomial is itself a polynomial over \mathbf{Z} . Note also that $1, \beta, \beta^2$ is linearly dependent over \mathbf{Q} (since $\dim F = 2$). So β satisfies a monic integral quadratic or linear polynomial, say $\beta^2 + m\beta + n = 0$, $m, n \in \mathbf{Z}$. If we write $\beta = c + d\sqrt{5}$ with $c, d \in \mathbf{Q}$ and use the equation $\beta^2 = -m\beta - n$ we find that c and d are either both integers or both half-integers. Hence $\beta \in R$, so R is integrally closed.

Noetherian-ness: We know that \mathbf{Z} is noetherian, and $R = \mathbf{Z}[1, \alpha]$ is finitely generated over \mathbf{Z} (as a ring), so R is noetherian by one of the corollaries to the Hilbert Basis Theorem.

Nonzero primes are maximal: Let P be a nonzero prime ideal of R . Choose $a + b\sqrt{5} \in P$; then $a^2 - 5b^2 = (a + b\sqrt{5})(a - b\sqrt{5}) \in P$, and $a^2 - 5b^2 \in \mathbf{Z}$. So $P \cap \mathbf{Z} \neq 0$. It is easy to check that $P \cap \mathbf{Z}$ is an ideal of \mathbf{Z} , and indeed a prime ideal. We now have the embedding $\mathbf{Z}/P \cap \mathbf{Z} \subseteq R/P$ of integral domains. The smaller one is a field, and is finite. But R is

generated by 1 and α as a \mathbf{Z} -module. Hence R/P is 1- or 2-dimensional over $\mathbf{Z}/P \cap \mathbf{Z}$, and in any case is finite. But any finite integral domain is a field (for any nonzero element x , there must be a coincidence among the powers x, x^2, \dots , and the cancellation law yields $x^i = 1$ for some $i > 0$). Therefore R/P is a field so P is maximal.

With similar ideas it can be proved that the following construction always yields an integral domain R : Let f be an irreducible rational polynomial. Let α be a root of f in \mathbf{C} and let $F = \mathbf{Q}[\alpha]$, the ring consisting of all rational linear combinations of powers of α . Since $f(\alpha) = 0$, it turns out that $F = \mathbf{Q}(\alpha)$ is a field. Let $R = \{x \in F \mid x \text{ is integral over } \mathbf{Z}\}$. This ring R is the “ring of algebraic integers” in the “algebraic number field” F .

Now consider the theorem.

The key step is to prove that every nonzero ideal is **invertible** in the following sense.

Definition. Let R be an integral domain and F its quotient field. Let I be an ideal in R . Then

$$I^{-1} = \{x \in F \mid xI \subseteq R\}.$$

It is immediate that I^{-1} is an R -submodule of the R -module F , and that $R \subseteq I^{-1}$ and $I^{-1}I \subseteq R$.

(Recall that for any two subsets $A, B \subseteq F$, we define $AB = \{\sum_i a_i b_i \mid a \in A, b \in B\}$. It is trivial to check that $(AB)C = A(BC)$ for any subsets A, B, C . This associativity will be critical for the theorem.)

Definition. In the situation of the previous definition, I is said to be invertible if and only if $II^{-1} = R$.

We shall show that in a Dedekind domain, every maximal ideal is invertible, and then from this we shall deduce the unique factorization property.

Lemma. Suppose that I is a nonzero ideal of the Dedekind domain R , F is the quotient field of R , and $x \in F$ is such that $xI \subseteq I$. Then $x \in R$.

Proof. Since R is Dedekind, it is noetherian. Hence I is generated by finitely many a_1, \dots, a_n of its elements. Since $xI \subseteq I$, there are $c_{ij} \in R$ such that $xa_i = \sum_j c_{ij}a_j$. This means however that x is an eigenvalue of the R -matrix (c_{ij}) . Hence x is integral over R . Since R is Dedekind, it is integrally closed in F , so $x \in R$. QED

Lemma. Suppose that R is a Dedekind domain. If every nonzero maximal ideal of R is invertible, then unique factorization holds for the ideals of R .

Proof. If 0 is a maximal ideal, then R is a field and there is nothing to prove. So assume not. For the existence of factorizations, suppose that some ideal is not the product of prime ideals, and use the fact that R is noetherian to select a maximal such ideal I . Then $I \subseteq M$ for some maximal ideal M . We use the invertibility of M . Now $M^{-1} \supseteq R$ so $I \subseteq IM^{-1} \subseteq MM^{-1} = R$. Thus IM^{-1} is an ideal of R . If $I \neq IM^{-1}$, then by our maximal choice of

I , $IM^{-1} = P_1 \cdots P_m$ for some prime ideals P_i , so $I = IR = IM^{-1}M = MP_1 \cdots P_m$, as needed. If $I = IM^{-1}$, then by the preceding lemma $M^{-1} \subseteq R$. But this is impossible by the invertibility of M , since $MM^{-1} = R \not\subseteq M = MR$.

For the uniqueness, if $P_1 \cdots P_m = Q_1 \cdots Q_n$, all P_i 's and Q_j 's being nonzero prime (and hence maximal), if $P_i = Q_j$ for some i and j , we may multiply both sides by $P_i^{-1} = Q_j^{-1}$ to cancel these terms, and complete the proof of uniqueness by induction. Thus we are reduced to the case that no P_i is a Q_j . But then $P_1 \supseteq P_1 \cdots P_m = Q_1 \cdots Q_n$. As P_1 is prime, we deduce that either $Q_1 \subseteq P_1$ or $Q_2 \cdots Q_n \subseteq P_1$. In the latter case we may repeat this reasoning, and we eventually deduce that some Q_j lies in P_1 . But the Q_i are maximal ideals. Hence $Q_j = P_1$, contradiction. □

Lemma. *Let R be a Dedekind domain. Let M be a maximal ideal of R . If $M^{-1} \neq R$, then $MM^{-1} = R$.*

Proof. Since M is maximal and MM^{-1} lies between M and R , the only alternative is $MM^{-1} = M$. But then $M^{-1} \subseteq R$ by the first lemma, implying $M^{-1} = R$, contradiction. □

Lemma. *Let R be a Dedekind domain. Let M be a nonzero maximal ideal of R . Then $M^{-1} \neq R$.*

Proof. Choose any $0 \neq r \in M$. Then $Rr \subseteq M$, and we claim that $MN \subseteq Rr$ for some ideal N which is a product of primes, possibly $N = R$. Namely Rr , like any nonzero ideal of R , contains a product of maximal ideals. (If this were false, then an ideal I maximal with respect to not containing such a product would not itself be prime, as every nonzero prime is maximal; hence $I \supseteq JK$ for some ideals J, K not contained in I ; then $I \subseteq J^*K^*$ where $J^* = I + J$ and $K^* = I + K$; then the maximality of I means that J^* and K^* contain products of maximal ideals, so I does as well.) Write $Rr \supseteq M_1 \cdots M_n$. Then $M \subseteq M_1 \cdots M_n$. This implies that in the field R/M , the images of the ideals M_i have 0 product, so $M \supseteq M_i$ for some i and hence $M = M_i$ for some i , say $i = 1$. Thus our claim holds with $N = M_2 \cdots M_n$ (or R , if $n = 1$).

Choose $N = P_1 \cdots P_m$, P_i prime, such that $MN \subseteq Rr \subseteq M$ and m is as small as possible. Now $r^{-1}NM \subseteq r^{-1}Rr = R$, so $r^{-1}N \subseteq M^{-1}$. If $r^{-1}N \not\subseteq R$, then $M^{-1} \not\subseteq R$ and we are done. So we may assume that $r^{-1}N \subseteq R$. Therefore $N \subseteq Rr \subseteq M$. In particular $m \geq 1$. The same argument as before shows now that some P_i equals M , say $M = P_1$. Then $MN' \subseteq Rr$ where $N' = P_2 \cdots P_m$, contradicting the minimality of m and completing the proof. □

Collecting the last three lemmas, we find that in a Dedekind domain every nonzero maximal ideal is invertible and so unique factorization holds.

We omit the proof of the converse. From the structure of our proof, however, notice that once the converse is proved, we can deduce that R is a Dedekind domain if and only if every ideal of R is invertible.

Exercise. *A commutative ring is a PID if and only if it is a UFD and a Dedekind domain.*