

RING THEORY

For us, *ring* will mean a ring with 1, an identity element for multiplication. There is one exceptional ring to be careful of, namely $R = \{0\}$ in which $1 = 0$ is both the additive and multiplicative identity. For any ring, we denote the additive identity by 0 and the multiplicative identity by 1. To define the category *Rings* we must specify the morphisms.

Definition. A *ring homomorphism* $f: R \rightarrow S$, where R, S are rings, is a function satisfying

- (1) $f(x + y) = f(x) + f(y)$,
- (2) $f(xy) = f(x)f(y)$, and
- (3) $f(1_R) = 1_S$.

The third condition is one that is not used in the larger category *Rngs* of rings without (necessarily) identity.

Easy results and basic definitions.

The *additive inverse* of x is denoted by $-x$.

Easily proved facts for a ring R :

- (1) $x \cdot 0 = 0 \cdot x = 0$ for all $x \in R$.
- (2) $(-1) \cdot x = -x$ for all $x \in R$.
- (3) $(-x)y = -(xy) = x(-y)$ for all $x, y \in R$.
- (4) $(-x)(-y) = xy$ for all $x, y \in R$.

A *commutative ring* is a ring in which $xy = yx$ for all x, y .

A *domain* is a ring $R \neq \{0\}$ in which $xy = 0 \implies x = 0$ or $y = 0$.

An *integral domain* is a commutative domain. [Note: Steinberger uses *domain* to mean commutative as well.]

If $xy = 0$, where $x \neq 0 \neq y$, we say x, y are *zero divisors* (or more specifically, x is a left zero divisor and y is a right zero divisor).

If $x^2 = x$, we say x is *idempotent*. It is a *nontrivial idempotent* if it is not 0 or 1.

If $x^n = 0$ for some $n \geq 0$, we say x is *nilpotent*.

We say x is a *unit* if x has both a right and a left inverse. [One easily checks that they must then be equal.] The set of all units in R is a multiplicative group denoted by R^\times .

If $R \neq \{0\}$ and every nonzero element of R is a unit, then R is called a *division ring*. A commutative division ring is a *field*.

A *subring* of a ring R is a subset $S \subseteq R$ such that S is itself a ring using the operations from R and including the identity 1_R .

Examples. \mathbb{Z} , the ring of integers is an integral domain.

$\mathbb{Z}/m\mathbb{Z}$, the ring of integers modulo m may have zero divisors.

\mathbb{Q} , \mathbb{R} , \mathbb{C} are the fields of rational numbers, real numbers and complex numbers, respectively. $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ is the ring of real quaternions, a noncommutative division ring.

$M_n(R)$ denotes the ring of $n \times n$ matrices over a ring R . For $n > 1$, these rings are noncommutative and contain zero divisors, nonzero nilpotent elements and nontrivial idempotent elements.

$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is the ring of *Gaussian integers*. It is an integral domain because it is a subset of the field \mathbb{C} .

$\mathbb{R}[x]$ and $\mathbb{R}[x, y]$ are polynomial rings.

Definition. A *left (right) ideal* of a ring R is a subset $I \subseteq R$ which is closed under addition and under left (right) multiplication by elements of R . A *two-sided ideal* or just *ideal* is both a left and a right ideal. We write $I \triangleleft R$ to mean I is an ideal of R .

Examples. (0) and R are ideals in any ring R .

$n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$ is an ideal in \mathbb{Z} for any fixed $n \in \mathbb{Z}$.

$\{p(x, y) \in \mathbb{R}[x, y] \mid f(0, 0) = 0\}$ is an ideal in $\mathbb{R}[x, y]$.

$\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ is a left ideal in $M_2(\mathbb{R})$, but not a right ideal.

We say an ideal $I \triangleleft R$ is *proper* if $I \neq (0)$ and $I \neq R$. If $a \in R$, then $Ra = \{ra \mid r \in R\}$ is a *principal left ideal* and $aR = \{ar \mid r \in R\}$ is a *principal right ideal*. We write $(a) = RaR$ for the *principal ideal* generated by a .

If R is commutative and every ideal in R is principal, we say R is a *principal ideal ring*. If also R has no zero divisors, then R is a *principal ideal domain (PID)*.

Basic theorems.

For a ring homomorphism $f: R \rightarrow S$, we call the set $\ker f = \{r \in R \mid f(r) = 0\}$ the *kernel* of f .

Proposition. For any ring homomorphism $f: R \rightarrow S$, we have $\ker f \triangleleft R$.

Theorem. Let $I \triangleleft R$. Then we can define a multiplication on the additive group R/I so that $R \rightarrow R/I$ is a ring homomorphism.

Theorem. Let $f: R \rightarrow S$ be a ring homomorphism with an ideal $I \subseteq \ker f$. Then there exists a unique ring homomorphism $\hat{f}: R/I \rightarrow S$ such that $\hat{f}\pi = f$, where $\pi: R \rightarrow R/I$ is the canonical homomorphism.

An ideal $I \triangleleft R$ is called *maximal* if $I \neq R$ and for any ideal J , if $I \subsetneq J$, then $J = R$.

Theorem. *Every proper ideal is contained in a maximal ideal.*

From now on R is a commutative ring, unless otherwise specified

Definition. Let $a, b \in R$. We say a *divides* b , written $a \mid b$, if there exists $r \in R$ such that $b = ar$ (equivalently, $b \in aR$ or $bR \subseteq aR$). We say that a is *irreducible* if $a = bc$ implies that either $b \in R^\times$ or $c \in R^\times$.

Note that if R is an integral domain, then $a \mid b$ and $b \mid a$ implies that $b = ua$ for some $u \in R^\times$.

Definition. An ideal $I \triangleleft R$ is called a *prime ideal* if R/I is an integral domain.

Proposition. *An ideal $I \triangleleft R$ is prime iff $ab \in I$ implies $I \neq R$ and either $a \in I$ or $b \in I$.*

Proposition. *An ideal $I \triangleleft R$ is maximal iff R/I is a field.*

Corollary. *Maximal ideals are prime.*

Definition. An integral domain R is a *unique factorization domain (UFD)* if any nonzero nonunit can be written as a finite product of irreducible elements and if the factorization is unique up to order and multiplication by units.

Examples. In \mathbb{Z} , the units are $\{\pm 1\}$. Factorization is unique but there are choices as seen in $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = (-1) \cdot (-2) \cdot 3 = (-2) \cdot (-3) = (-3) \cdot (-2)$.

In $\mathbb{Z}[\sqrt{-5}]$ (a subring of \mathbb{C}), we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. The only units are $\{\pm 1\}$ and all four of these factors are irreducible, so factorization is not unique. [Use the norm, $N: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}$ defined by $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Like the absolute value in \mathbb{C} , it is multiplicative.]

Definition. An element $p \in R$ is *prime* if $p \neq 0$ and (p) is a prime ideal. That is, $p \mid ab \implies p \mid a$ or $p \mid b$.

In $\mathbb{Z}[\sqrt{-5}]$, the elements $2, 3, 1 \pm \sqrt{-5}$ are irreducible but not prime. In any integral domain, prime implies irreducible. In a UFD, irreducible is equivalent to prime.

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

Localization.

For any integral domain R , one can construct the *field of fractions* or *quotient field* of R just as is done for defining \mathbb{Q} from \mathbb{Z} : you formally define elements of the form $\frac{a}{b}$ with $a \in R, b \neq 0$ in R with an equivalence relation $\frac{a}{b} = \frac{c}{d} \iff ad = bc$. Another example is forming the field of rational functions $\mathbb{R}(x)$ from the ring of polynomials $\mathbb{R}[x]$. [S, §7.11] shows how this can be generalized to invert certain subsets of commutative rings. We say that S is a *multiplicative subset* of R if $0 \notin S$, and $x, y \in S \implies xy \in S$. We wish to construct the *localization of R at S* , denoted $S^{-1}R$ together with a ring homomorphism $R \rightarrow S^{-1}R$ with the same universal property as fields of fractions. The construction is now complicated by the fact that R may have zero divisors. If R is an integral domain, then $R \rightarrow S^{-1}R$ is always injective and $S^{-1}R$ is a subring of the field of fractions of R . In fact, we obtain the field of fractions by taking $S = R \setminus \{0\}$.

The construction

Let $S^{-1}R$ be the set of equivalence classes of pairs (a, s) , written a/s or $\frac{a}{s}$, under

$$(a, s) \sim (b, t) \iff \exists s' \in S, s'(ta - sb) = 0.$$

Note that s' is not needed in an integral domain. Check that \sim is reflexive, symmetric and transitive. Check that $S^{-1}R$ becomes a commutative ring under the operations $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ and $\frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$.

Define $\eta: R \rightarrow S^{-1}R$ by $\eta(r) = \frac{r}{1}$. This is a ring homomorphism. The kernel is $\ker \eta = \{r \in R \mid sr = 0 \text{ for some } s \in S\}$.

More examples: begin with \mathbb{Z} . Take $S = \{2^n \mid n = 0, 1, 2, 3, \dots\}$. Then $S^{-1}\mathbb{Z} = 2^{-\infty}\mathbb{Z}$ is the subring of \mathbb{Q} with all fractions whose denominators are powers of 2. Sort of an opposite effect is obtained by taking $\mathbb{Z}_{(2)} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, 2 \nmid n\} = S^{-1}\mathbb{Z}$, where S consists of all integers not in the ideal (2) . We can generalize this.

Localization at a prime ideal

Let P be a prime ideal in a ring R and set $S = R \setminus P$. P being prime implies that S is multiplicatively closed. We denote the ring $S^{-1}R$ by R_P . A ring R is called a *local ring* if it has a unique maximal ideal. It is not hard to show that R_P is a local ring with maximal ideal PR_P .

Universal property

Let $f: R \rightarrow A$ be any ring homomorphism such that $f(s) \in A^\times$ for all $s \in S$. Then there exists a unique ring homomorphism $\bar{f}: S^{-1}R \rightarrow A$ such that $\bar{f}\eta = f$.

Corollary. *Let R be an integral domain, $f: R \rightarrow K$ with K a field. Then there exists a unique extension \bar{f} of f to an embedding of the field of fractions $R_{(0)}$ into K . The image of \bar{f} is the smallest subfield of K containing $f(R)$.*

For example, to define a homomorphism from \mathbb{Q} into any field F , it suffices to define an embedding of \mathbb{Z} into F (i.e. injective), and this is determined by sending $1 \mapsto 1$, so is unique. Therefore, **if $\text{char } F = 0$, then F contains a unique subfield isomorphic to \mathbb{Q} .** Another consequence is that the injection $\iota: \mathbb{Z} \rightarrow \mathbb{Q}$ is an *epimorphism in the category of rings* in the sense of being right cancellable. For if $\phi, \psi: \mathbb{Q} \rightarrow R$ are ring homomorphisms to a ring R such that $\phi\iota = \psi\iota$, then $\phi(m/n) = \phi(m)\phi(n)^{-1} = \psi(m)\psi(n)^{-1} = \psi(m/n)$.

Polynomial Rings over a commutative ring.

Definition. Let $R[x] = \{ (a_0, a_1, a_2, \dots) \mid a_i = 0 \ \forall i > \text{some } i_0 \}$. Thus this is isomorphic to $R^{(I)}$ where $I = \{0, 1, 2, \dots\}$, and we regard elements of $R[x]$ as equal iff all components are equal. Define addition by $(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$ and write $0 = (0, 0, 0, \dots)$ for the additive identity. This makes $R[x]$ into an abelian group. Now define a multiplication by $(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (p_0, p_1, p_2, \dots)$, where $p_i = \sum_{j=0}^i a_j b_{i-j} = \sum_{j+k=i} a_j b_k$. Note that if $a_j = 0$ for $j > n$ and $b_k = 0$ for $k > m$, then $p_i = 0$ for $i > m+n$. Also note that $1 = (1, 0, 0, 0, \dots)$ is the multiplicative identity. The associative and distributive laws are straightforward, though messy, to check. Since R is commutative, so is $R[x]$ by our definition of the elements p_i . Therefore, $R[x]$ is a commutative ring. There is an injective ring homomorphism $R \rightarrow R[x]$ defined by $r \mapsto (r, 0, 0, 0, \dots)$. We identify elements of R with their images in $R[x]$ and set $x = (0, 1, 0, 0, 0, \dots)$. By the formula for product and induction, we get $x^k = (0, 0, \dots, 1, 0, 0, \dots)$ with the 1 in the $(k+1)$ st position. With this notation, we can write $(a_0, a_1, \dots, a_n, 0, 0, 0, \dots) = \sum_{i=0}^n a_i x^i$. We call $R[x]$ the *ring of polynomials* over R in the *indeterminate* x .

We actually made no use of the commutativity of R . This same definition works if R is noncommutative, giving a polynomial ring with the indeterminate in the center. Not surprisingly, polynomial rings satisfy a certain universal property:

Theorem. *Let R, S be commutative rings, $s \in S$. For any ring homomorphism $\beta: R \rightarrow S$, there exists a unique ring homomorphism $\gamma: R[x] \rightarrow S$ such that $\gamma(x) = s$ and $\gamma\iota = \beta$, where $\iota: R \rightarrow R[x]$ is the canonical embedding.*

Corollary. $\mathbb{Z}[x_1, \dots, x_n]$ is the free commutative ring on the set $\{x_1, \dots, x_n\}$.

Definition. Let $f(x) = \sum_{i=0}^n a_i x^i$, with $a_n \neq 0$. We call a_n the *leading coefficient* of f ; we call n the *degree* of f , denoted by $\deg f$; and we say that f is a *monic polynomial* if $a_n = 1$.

By convention, we set $\deg 0 = -\infty$. Then $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$, with equality unless $\deg f = \deg g$. If we write $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{i=0}^m b_i x^i$, then $f(x)g(x) = a_0 b_0 + \cdots + a_n b_m x^{m+n}$ has degree $m + n$ if $a_n b_m \neq 0$. Thus $\deg f(x)g(x) = \deg f(x) + \deg g(x)$ when the leading coefficients are not zero divisors.

Theorem. *If R is an integral domain, so is $R[x]$.*

In particular, if R is an integral domain, then R has a field of fractions F . And $R[x]$ has a field of fractions which contains F . We denote it by $F(x)$ and note that it consists of quotients of polynomials, which we call rational functions.

Division Algorithm. *Let $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{i=0}^m b_i x^i$, with $a_n b_m \neq 0$. Then there exist elements $q(x), r(x) \in R[x]$ with $\deg r < \deg g$ such that for some integer $k \geq 0$,*

$$b_m^k f(x) = q(x)g(x) + r(x).$$

In fact, $k = \max(\deg f - \deg g + 1, 0)$ works.

Corollary. *Let F be a field. Then $F[x]$ is a Euclidean ring, hence a PID and a UFD.*

An element $r \in R$ is called a *root* of a polynomial $f(x) = \sum_{i=0}^n a_i x^i$ if $f(r)$, defined as $\sum_{i=0}^n a_i r^i$ is 0 in R .

Proposition. *In $R[x]$, if r is a root of f , then $x - r$ divides f .*

Corollary. *Let F be a field. A polynomial of degree n in F has at most n roots in F .*

For $f(x) = \sum a_i x^i \in R[x]$, we shall write $f'(x) = \sum i a_i x^{i-1}$ and call it the *derivative* of f . While we have no notion of limit or tangent line, some of calculus does carry over—namely, anything that is purely formal like the product and chain rules.

Proposition. *Let F be a field; $a \in F$ is a multiple root of $f \in F[x]$ iff a is a root of both f and f' (i.e., $(x - a)$ divides $\gcd(f, f')$).*

Definition. Let R be a ring and let $\phi: \mathbb{Z} \rightarrow R$ denote the unique ring homomorphism. Since \mathbb{Z} is a PID, $\ker(\phi) = (m)$ for some integer m . $|m|$ is called the *characteristic* of R . If R is a field, then $\text{im}(\phi)$ is an integral domain, so $\ker(\phi)$ is a prime ideal. Therefore the characteristic of a field is zero or a prime number p .

Example: $\frac{10}{3}x^2 + 6x - 20 = \frac{2}{3}(5x^2 + 9x - 30)$, where $5x^2 + 9x - 30 \in \mathbb{Z}[x]$. We would like to generalize this process.

Let R be a UFD with field of fractions F . Let $0 \neq a \in F$. For any irreducible $p \in R$, we can write $a = p^r b$, where $b = b_1/b_2 \in F$, $b_i \in R$ and p does not divide either b_i . Since R is a UFD, the integer r is uniquely determined. We write $\text{ord}_p a = r$, the order of a at p . Set $\text{ord}_p 0 = -\infty$. Then $\text{ord}_p(xy) = \text{ord}_p x + \text{ord}_p y$. For $f(x) = \sum a_i x^i \in F[x]$, set $\text{ord}_p 0 = -\infty$ and $\text{ord}_p f = \min_{a_i \neq 0} \text{ord}_p a_i$.

We define the *content* of a polynomial f to be $\text{cont}(f) = \prod p^{\text{ord}_p f}$, where the product is over irreducibles of R , one for each class modulo units. The product is actually finite since only finitely many irreducibles are needed to express the coefficients of a given polynomial. The content is well-defined up to a unit of R .

Therefore, if $0 \neq a \in F$, $\text{cont}(a) = a$, up to multiplication by a unit of R and $\text{cont}(af) = a \text{cont}(f)$ for polynomials f . Thus for any polynomial in $f[x]$, we can write $f(x) = cf_1(x)$, where $c = \text{cont}(f)$ and $\text{cont}(f_1) = 1$. Therefore all the coefficients of f_1 lie in R and have gcd equal to 1.

Example: For $f(x) = \frac{10}{3}x^2 + 6x - 20$, we have

$$\begin{aligned} \text{cont}(f) &= \frac{2}{3} \\ \text{ord}_2(f) &= \min(1, 1, 2) = 1 \\ \text{ord}_3(f) &= \min(-1, 1, 0) = -1 \\ \text{ord}_5(f) &= \min(1, 0, 1) = 0 \\ \text{ord}_p(f) &= 0 \text{ for } p \neq 2, 3, 5 \\ \frac{10}{3}x^2 + 6x - 20 &= \frac{2}{3}(5x^2 + 9x - 30), \end{aligned}$$

where $f_1(x) = \frac{2}{3}(5x^2 + 9x - 30)$ has content 1.

Gauss Lemma. *Let R be a UFD with field of fractions F . If $f, g \in F[x]$, then $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$.*

Corollary. *Let R be a UFD with field of fractions F . Let $f \in R[x]$ with $f(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$. If $c_g = \text{cont}(g(x))$, $c_h = \text{cont}(h(x))$ and $g(x) = c_g g_1(x)$, $h(x) = c_h h_1(x)$, then $f(x) = c_g c_h g_1(x)h_1(x)$ and $c_g c_h \in R$.*

Theorem. *Let R be a UFD with field of fractions F . Then $R[x]$ is a UFD. Its irreducible elements are those of R together with polynomials in $R[x]$ of content 1 which are irreducible in $F[x]$.*

Corollary. *Let R be a UFD with field of fractions F . Then $R[x_1, \dots, x_n]$ is a UFD.*

Note however, that $F[x, y]$ is *not* a PID.

Eisenstein's Criterion. *Let R be a UFD with field of fractions F . Let $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ with $a_n \neq 0$, $n \geq 1$. Let p be an irreducible element of R and assume*

$$\begin{aligned} \text{ord}_p a_n &= 0 \\ \text{ord}_p a_i &\neq 0 \quad (i < n) \\ \text{ord}_p a_0 &= 1. \end{aligned}$$

Then $f(x)$ is irreducible in $F[x]$.

REFERENCES

- [J2] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Co., 1980.
- [S] M. Steinberger, *Algebra*, PWS Publishing Co., Boston, 1994.