12 Introduction to Rings

Definition. A *ring* $(R, +, \cdot)$ is a set with two binary operations, $+$ and $\cdot$, such that

1–4) $(R, +)$ is an abelian group.

4) $a(bc) = (ab)c$ for every $a, b, c \in R$.

3) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for every $a, b, c \in R$.

Note. The expression na could be a product of n and a or it could be $\overbrace{a + \cdots + a}^{n}$. We use $n \cdot a$ to denote $a + \cdots + a$, while notation without $\cdot$ indicates the binary operation.

Definition. Beyond associativity, there are no requirements for multiplication in a ring R.

1) If multiplication is commutative, we call R a *commutative ring.*
2) If multiplication has an identity element, it is called a *unity* or *identity.*
3) If a nonzero element in a ring with a unity has a multiplicative inverse, it is called *a unit of the ring.*
4) In a commutative ring, a nonzero element a *divides* b ($a \mid b$) if there is a $c \in R$ such that $b = ac$.

Verify that each of the following sets with indicated binary operations are rings and state if it has additional properties.

Example. $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$

Example. $(\mathbf{Z}_n, +, \cdot)$

Example. $(M_n(\mathbf{Z}), +, \cdot)$, $(M_n(\mathbf{Q}), +, \cdot)$, $(M_n(\mathbf{R}), +, \cdot)$: $n \times n$ matrices with entries in specified set.

Example. If $R_1, \dots, R_n$ are rings, we can construct the *direct sum* of rings $R_1 \oplus \cdots \oplus R_n$ which is the set $R_1 \times \cdots \times R_n$ with componentwise multiplication and addition.

Example. $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$: polynomials in a single variable x with coefficients in a given set. (Polynomials are not functions here, rather, they are abstract expressions that involve an x with established rules for addition and multiplication.)

Theorem 12.1. Let $a, b, c \in R$. Then

1) a0=0a=0
2) $a(-b) = (-a)b = -(ab)$
3) $(-a)(-b) = ab$
4) $a(b - c) = ab - ac$
   $(b - c)a = ba - ca$

If, additionally, R has unity 1, then

5) $(-1)a = -a$
6) $(-1)(-1)a = 1$

Proof.

Theorem 12.2. If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Proof. Same as for groups.

Definition. A subset S of a ring R is *subring of* R if S is itself a ring with operations of R.

Theorem 12.3. A nonempty subset S of a ring R is a subring if and only if for every $a, b \in S$, $a + b$, $-a$ and ab are in S.

Example. Many examples above using same idea (polynomials, matrices) but with different underlying sets of coefficients are subrings.

Example. $k\mathbf{Z}$ is a subring of $\mathbf{Z}$.

13 Integral Domains and Fields

Definition. A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ for which $ab = 0$.

Definition. An *integral domain* is a commutative ring with unity and no zero divisors. Equivalently, a ring R is an integral domain if it is commutative, has a unity, and whenever $ab = 0$ for some $a, b \in R$, then $a = 0$ or $b = 0$.

Example. Lots of examples from section 12 are integral domains: $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$, $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$.

Example. $(M_n(\mathbf{Z}), +, \cdot)$, $(M_n(\mathbf{Q}), +, \cdot)$, $(M_n(\mathbf{R}), +, \cdot)$ are not integral domains because they are not commutative. They also have elements A, B such that $AB = 0$, but $A, B \neq 0$.

Example. $\mathbf{Z} \oplus \mathbf{Z}$ is not an integral domain.

Example. $\mathbf{Z}_n$ is an integral domain if and only if n is prime.

Cancellation Theorem 13.1. Let $a, b, c \in R$, where R is an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof.

Definition. A *field* is a commutative ring with multiplicative identity in which every nonzero element has a multiplicative inverse.

Example. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are all fields. They contain subfields such as $\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ or $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbf{Q}\}$.

Example. $\mathbf{Q}[x], \mathbf{R}[x]$ are not fields.

Theorem 13.2. A finite integral domain is a field.

Proof.

Corollary. $(\mathbf{Z}_p, +, \cdot)$ is a field whose multiplicative group is $U(p)$.

Example. Which of $Z_2[i] = \{a + bi \mid a, b \in \mathbf{Z}_2\}$ and $Z_3[i] = \{a + bi \mid a, b \in \mathbf{Z}_3\}$ is a field?

Definition. The characteristic $\operatorname{char} R$ of a ring R is the least positive integer n such that $n \cdot x = 0$ for all $x \in R$. If no such integer exists, we say $\operatorname{char} R = 0$.

Note. If R is finite, $\operatorname{char} R \leq |R|$ because the characteristic will be the maximal additive order of all elements in R.

Example. $\operatorname{char} \mathbf{Z}_n = n$

Example. $\operatorname{char} \mathbf{Z}_3[x] = 3$, even though it is an infinite ring.

Theorem 13.3. Let R be a ring with unity 1. If 1 has infinite order under addition, then $\operatorname{char} R = 0$. If 1 has order n under addition, then $\operatorname{char} R = n$.

Proof.

Theorem 13.4. The characteristic of an integral domain is prime.

Proof.

14 Ideals and Quotient Rings

Definition. A subring A of a ring R is called a *(two-sided) ideal* if for every $a \in A$ and $r \in R$, $ar \in A$ and $ra \in A$.

Theorem 14.1. A nonempty subset A of a ring R is an ideal if for every $a, b \in A$ and $r \in R$

1) $a + b \in A$, $-a \in A$
2) $ar, ra \in A$ (note this also implies A is closed under multiplication)

Example. $\{0\}$ and R are ideals of a ring R.

Example. $k\mathbf{Z}$ is an ideal of $\mathbf{Z}$.

Example. Not every subring is an ideal: $\{kI \mid k \in \mathbf{Z}\}$ is a subring of $M_n(\mathbf{Z})$, but not an ideal.

Example. In a commutative ring with unity, set $\langle a \rangle = \{ra \mid r \in R\}$. Then $\langle a \rangle$ is an ideal of R called the *principal ideal generated by a*.

Note. $\langle a \rangle$ can mean principal ideal or additive subgroup generated by a, and often they are not the same. It will be clear which one we mean from context.

Example. Show that in $\mathbf{Z}[x]$ the additive subroup generated by polynomial x and principal ideal generated by x are not same.

Example. Similarly, we can define the ideal generated by $a_1, \ldots, a_n$: $\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \ldots r_n \in R\}$. This is the smallest ideal that contains $a_1, \ldots, a_n$.

Since a ring R is a commutative group under addition, for every subring A we can form the quotient group R/A with induced addition. Does multiplicaton of cosets work if we define it as $(x + A)(y + A) = xy + A$?

Theorem 14.2. Let R be a ring and A a subring of R Then the additive quotient group R/A is a ring with multiplication $(x + A)(y + A) = xy + A$ if and only if A is an ideal of R.

Proof.

Definition. For a ring R and its ideal A, the set R/A with operations $(x + A) + (y + A) = x + y + A$ and $(x + A)(y + A) = xy + A$ is a ring, called the *quotient ring of R by ideal A*.

Example. Describe the quotient ring $\mathbf{Z}/n\mathbf{Z}$.

Example. Describe the quotient ring $\mathbf{Z}[i]/\langle 3 + 2i \rangle$.

Example. Describe the quotient ring $\mathbf{R}[x]/\langle 1+x^2\rangle$.

Definition. A *prime ideal* A of a commutative ring R is a proper ideal of R such that for every $a, b \in R$, if $ab \in A$ then $a \in A$ or $b \in A$. A *maximal ideal* A of a commutative ring R is a proper ideal not contained in any other proper ideal, that is, if B is an ideal and $A \subseteq B$, then $B = A$ or $B = R$.

Example. The ideal kZ of Z is prime if and only if k is prime. The ideal kZ is maximal if and only if k is prime.

Example. The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbf{R}[x]$.

Theorem 14.3. Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is a prime ideal.

Proof.

Theorem 14.4. Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is a maximal ideal.

Proof.

15 Ring Homomorphisms

Definition. Let R and S be rings and $\phi : R \to S$ a mapping. We say ϕ is a *ring homomorphism* if it preserves the two ring operations, that is, if for every $a, b \in R$

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b)$$

A bijective ring homomorphism is called a *ring isomorphism*.

Example. $\phi : \mathbf{C} \to \mathbf{C}$, $\phi(z) = \overline{z}$ is a ring isomorphism.

Example. Let $a \in \mathbf{R}$, and define $\phi : \mathbf{R}[x] \to \mathbf{R}$ by $\phi(f) = f(a)$. Then ϕ is a homomorphism (evaluation homomorphism).

Example. Let R be a ring of characteristic 2. Then $x \mapsto x^2$ is a ring homomorphism.

Example. The ring $2\mathbf{Z}$ is isomorphic to $\mathbf{Z}$ as an additive group, but they are not ring-isomorphic. Why?

Example. For any ring R and element $a \in R$, show there exists a ring homomorphism $\phi : \mathbf{Z}_n \to R$ such that $\phi(1) = a$ if and only if:

1) the additive order $|a|$ divides n (needed for ϕ to be an additive homomorphism)
2) $a^2 = a$ (additionally needed for ϕ to be a multiplicative homomorphism)

Theorem 15.1. Let $\phi : R \to S$ be a ring homomorphism and let A be a subring of R and B and ideal of S.

1) For any $r \in R$ and $n \in \mathbf{N}$, $\phi(n \cdot x) = n \cdot \phi(x)$ and $\phi(x^n) = \phi(x)^n$.
2) $\phi(A)$ is a subring of S.
3) If A is an ideal and ϕ is onto, then $\phi(A)$ is an ideal of S.
4) $\phi^{-1}(B)$ is an ideal of R.
5) If R is commutative, then $\phi(R)$ is commutative.
6) If R has a unity 1, ϕ is onto and $S \neq \{0\}$, then $\phi(1)$ is the unity of S.
7) ϕ is an isomorphism if and only if ϕ is onto and $\ker \phi = \{0\}$.
8) If ϕ is an isomorphism, then $\phi^{-1} : S \to R$ is an isomorphism.

Proofs. are analogous to proofs of statements about homomorphisms of groups.
Just like the following statements.

Theorem 15.2. Let $\phi : R \to S$ be a ring homomorphism. Then $\ker \phi$ is an ideal of R.

First Isomorphism Theorem for Rings 15.3. Let $\phi : R \to S$ be a ring homomorphism, $A = \ker \phi$ (an ideal). Then the mapping $R/A \to S$ given by $x + A \mapsto \phi(x)$ is a ring isomorphism, so $R/\ker \phi \approx \phi(R)$.

Theorem 15.4. Every ideal A of a ring R is the kernel of some homomorphism, in particular the quotient homomorphism $q : R \to R/A$.

Proof.

Theorem 15.5. Let R be a ring with unity 1. Then the mapping $\phi : \mathbf{Z} \to R$ given by $\phi(k) = k \cdot 1$ is a ring homomorphism. More generally, like in the example above, the mapping $\phi(k) = k \cdot a$ is a ring homomorphism if and only if $a^2 = a$.

Proof.

Corollary.

1) If R is a ring with unity and $\operatorname{char} R = n$, $n \geq 0$, then R contains a subring S that is isomorphic to $\mathbf{Z}_n$ (note that $\mathbf{Z}_0 = \mathbf{Z}/0\mathbf{Z} = \mathbf{Z}$).
2) $\mathbf{Z}_m$ is a ring-homomorphic image of $\mathbf{Z}$.
3) If F is a field with $\operatorname{char} p > 0$, then F contains a subfield isomorphic to $\mathbf{Z}_p$. If $\operatorname{char} F = 0$, then F contains a subfield isomorphic to $\mathbf{Q}$.

Proof.

Theorem 15.6. Let D be an integral domain. Then there exists a field F called *the field of quotients of* D that contains a subring isomorphic to D. (In other words, an integral domain can always be extended to a field.)

The field is constructed as follows: let $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. Using the equivalence relation $(a, b) \equiv (c, d)$ if $ad = bc$, we set F to be the set of equivalence classes $S/\equiv$. If $\frac{x}{y}$ denotes the equivalence class of (x, y), we define addition and multiplication on F as:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \quad (bd \neq 0 \text{ because } D \text{ is an integral domain})$$

Proof.

16 Polynomial Rings

Definition. Let R be a commutative ring. The *ring of polynomials* $R[x]$ *over* R is the set of formal expresssions (or sequences) of form

as formal expression	as a sequence
$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$	$(a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, \ldots)$

where $a_i \in R$, $n \in \mathbf{Z}$, $n \geq 0$. (We consider $a_i = 0$ for $i > n$.) Two elements

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad \text{and} \quad g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

are equal if $n = m$ and $a_i = b_i$ for $i = 0, \ldots, n$.

Addition of polynomials is "componentwise:"

$$(f+g)(x) = (a_s+b_s)x^s+(a_{s-1}+b_{s-1})x^{s-1}+\cdots+(a_1+b_1)x+(a_0+b_0), \text{ where } s = \max\{m,n\}$$

Multiplication is defined by

$$(fg)(x) = c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\cdots+c_1x+c_0, \text{ where } c_k = a_kb_0+a_{k-1}b_1+\cdots+a_1b_{k-1}+a_0b_k$$

Proposition. The set $(R[x], +, \cdot)$ is a commutative ring. If R has unity 1, the unity in $R[x]$ is the polynomial 1.

Proof. Involved but not hard. Believable because the operations mimic multiplication of polynomials in the usual way.

Note. Here polynomials are not considered as functions. For example, in $\mathbf{Z}_3[x]$, $f(x) = x^3$ and $g(x) = x$ are the same function $\mathbf{Z}_3 \to \mathbf{Z}_3$, but the polynomials x^3 and x are different, as $(0, 0, 1, 0, \ldots) \neq (1, 0, 0, 0 \ldots)$.

Terminology. For $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ we define:

degree of f	is n if $a_n \neq 0$ and $a_k = 0$ for $k > n$ (the 0-polynomial has no degree)
coefficients of f	are $a_0, \ldots, a_n$
leading coefficient	is a_n
constant polynomial	is $f(x) = a_0$
monic polynomial	is one where $a_n = 1$

Definition. Let $f \in R[x]$, $a \in R$, $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. We define $f(a) = a_na^n + a_{n-1}a^{n-1} + \cdots + a_1a + a_0 \in R$. It is not hard to see that for a fixed $a \in \mathbf{R}$, the map $f \mapsto f(a)$ is a ring homomorphism $R[x] \to R$.

Theorem 16.1. If D is an integral domain, then $D[x]$ is an integral domain.

Proof.

Theorem 16.2. Let F be a field and let $f, g \in F[x]$ with $g \neq 0$. Then there exist unique polynomials $q, r \in F[x]$ such that $f = gq + r$ and $\deg r < \deg g$ or $r = 0$.

The polynomials q and r are called the *quotient and remainder in the division of f by g.*

Proof.

Example. For $f, g \in \mathbf{Z}_5[x]$, determine the quotient and remainder in division of f by g: $f(x) = 2x^4 + 4x^2 + 3x + 1$, $g(x) = x^2 + 3x + 1$. (Essentially, do long division of polynomials.)

Definition. Let D be an integral domain, $f, g \in D[x]$.

1) We say g divides f if there exists a polynomial h such that $f = gh$. We call g a *factor* of f.
2) $a \in D$ is the *zero* of polynomial f if $f(a) = 0$.
3) When $D = F$ is a field, we say *a is a zero of multiplicity k of f* if $(x - a)^k$ is a factor of f and $(x - a)^{k+1}$ is not a factor of f.

Corollary. Let F be a field, $a \in F$, $f \in F[x]$.

1) $f(a)$ is the remainder in the division of f by $x - a$.
2) a is a zero of f if and only if $x - a$ is a factor of f.

Proof.

Theorem 16.3. A polynomial over a field has at most n zeroes, counting multiplicity.

Proof.

Definition. A *principal ideal domain (PID)* is an integral domain R in which every ideal has form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.

Theorem 16.4. Let F be a field. Then $F[x]$ is a principal ideal domain.

Proof.

Theorem 16.5. Let F be a field, I a nonzero ideal in $F[x]$, and $g \in F[x]$. Then $I = \langle g \rangle$ if and only if g is a nonzero polynomial of minimum degree in I.

17 Factorization of Polynomials

In previous mathematical schooling we are taught factorization of polynomials as a way to find their zeroes (i.e. where $f(a) = 0$). We now consider the general question of factoring a polynomial, that is, writing it as a product of polynomials in a nontrivial way.

Definition. Let D be an integral domain. We say that a nonzero polynomial $f \in D[x]$ is *irreducible* over D if, whenever $f = gh$ and $g, h \in D[x]$ then g or h is a unit in $D[x]$. A nonzero, nonunit polynomial is *reducible* over D if it is not irreducible over D, that is, if it can be written as product of two nonunit polynomials.

Note. In $D[x]$, the only unit elements are constant polynomials, where the constant is a unit from D. Since in a field F, every nonzero element is unit, a polynomial $f \in F[x]$ is irreducible if and only if it cannot be expressed as a product of lower-degree polynomials. In particular, polynomials of degree 0 or 1 in $F[x]$ is irreducible.

Note. A polynomial $f \in F[x]$ is irreducible if and only if af is irreducible for some $a \neq 0$ in F.

Example. Consider the polynomials 6, $2x - 6$ and $2x^2 - 6$ as elements of $\mathbf{Z}[x]$ or $\mathbf{Q}[x]$. Are they irreducible over $\mathbf{Z}$ or $\mathbf{Q}$?

Example. Consider the polynomials $2x^2 - 6$ and $2x^2 + 6$ as elements of $\mathbf{R}[x]$ or $\mathbf{C}[x]$. Are they irreducible over $\mathbf{R}$ or $\mathbf{C}$?

Example. Consider the polynomial $x^2 + 1$ as element of $\mathbf{Z}_3[x]$ or $\mathbf{Z}_5[x]$. Is it irreducible over $\mathbf{Z}_3$ or $\mathbf{Z}_5$?

Theorem 17.1. If $f \in F[x]$, where F is a field, and $\deg f = 2$ or 3, then f is reducible over F if and only if f has a zero in F.

Proof.

Note. A degree-4 polynomial may be reducible even if has no zeroes. For example, $x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$, so it is reducible over R, but has no real zeroes.

Definition. The *content* of a nonzero polynomial $a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$ is the greatest common divisor of $a_n, \ldots, a_0$. A *primitive polynomial* in $\mathbf{Z}[x]$ is one whose content is 1.

Example. The content of $24x^3 - 18x^2 + 12x^2 + 30$ is

Gauss' Lemma. The product of two primitive polynomials is primitive.

Proof.

Theorem 17.2. Let $f \in \mathbf{Z}[x]$. If f is reducible over $\mathbf{Q}$, then f is reducible over $\mathbf{Z}$.

Proof.

Example. Follow the proof on the example of $f(x) = 4x^2 + 8x - 5$, which has $\frac{1}{2}$ as its zero.

Theorem 17.3. Let p be a prime and $f \in \mathbf{Z}[x]$ with $\deg f \geq 1$. Let $\overline{f} \in \mathbf{Z}_p[x]$ be the image of f under the $\bmod p$ homomorphism. If $\overline{f}$ is irreducible over $\mathbf{Z}_p$, and $\deg \overline{f} = \deg f$, then f is irreducible over $\mathbf{Q}$.

Proof.

Example. Show that $f(x) = 4x^3 + 5x^2 + 5x - 2$ is irreducible over $\mathbf{Q}$.

Note. For some p, $\overline{f}$ may be reducible over $\mathbf{Z}_p$ while f is irreducible over $\mathbf{Q}$, so it is worth trying several p's. However, $x^4 + 1$ is reducible for every p, but irreducible over $\mathbf{Q}$.

Eisenstein's Criterion Theorem 17.4. Let $a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$. If there is a prime p such that $p \nmid a_n$ while $p | a_{n-1}, \ldots, p | a_1, p | a_0$ but $p^2 \nmid a_0$, then f is irreducible over $\mathbf{Q}$.

Proof.

Corollary. For every prime p, the cyclotomic polynomial $\dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbf{Q}$.

Proof.

Theorem 17.5. Let F be a field, $p \in F[x]$. Then $\langle p \rangle$ is maximal ideal in $F[x]$ if and only if p is irreducible over F.

Proof.

Corollary. Let F be a field.

1) If $p \in F[x]$ is irreducible over F, then $F[x]/\langle p \rangle$ is a field.
2) If $p, a, b \in F[x]$, p is irreducible over F and $p|ab$, then $p|a$ or $p|b$.

Proof.

Example. Let $f(x) = 4x^3 + 5x^2 + 5x + 5 \in \mathbf{Z}_7[x]$. We have already shown that f is irreducible over $\mathbf{Z}_7$, so $\mathbf{Z}_7[x]/I$ is a field, where $I = \langle f \rangle$. How many elements does it have? Multiply $x^2 + 4x + 3 + I$ with $5x + 2 + I$ in $\mathbf{Z}_7[x]/I$.

Theorem 17.6. Every nonzero and nonunit polynomial in $\mathbf{Z}[x]$ can be written in the form $b_1 \ldots b_s p_1 \ldots p_m$, where $b_1, \ldots, b_s$ are irreducible polynomials of degree 0 (that is, primes) and $p_1, \ldots, p_m$ are irreducible polynomials over $\mathbf{Z}$ of positive degree. This factorization is unique up to order and sign of the factors.

Proof. See book.