Chapter 1

Rings

1.1 Definitions and Examples

(III.1, III.2)

Def. *A* **ring** $\langle R, +, \cdot \rangle$ *consists of*

a nonempty set R *and two binary operations* $+$ *and* $\cdot$

that satisfy the axioms:

1. $\langle R, + \rangle$ *is an abelian group;*
2. $(ab)c = a(bc)$ *(associative multiplication);*
3. $a(b + c) = ab + ac$, $(b + c)a = ba + ca$. *(distributive laws)*

Moreover, the ring R *is a*

- **commutative ring** *if* $ab = ba$*;*
- **ring with identity** *if* R *contains an element* 1_R *such that* $1_R\, a = a\, 1_R = a$ *for all* $a \in R$.

Conventions: (1) $ab = a \cdot b$; (2) $na = a + a + \cdots + a$ (n summands) for $n \in \mathbf{Z}$ and $a \in R$; (3) 1_R denotes either the identity of R, or the identity map $1_R : R \to R$.

Ex. *The ring* $\mathbf{Z}$ *of integers is a commutative ring with identity. So are* $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_n$, $\mathbf{R}[x]$, *etc.*

Ex. $3\mathbf{Z}$ *is a commutative ring with no identity.*

Ex. *The ring* $\mathbf{Z}^{2\times 2}$ *of* 2×2 *matrices with integer coefficients is a noncommutative ring with identity.*

Ex. $(3\mathbf{Z})^{2\times 2}$ *is a noncommutative ring with no identity.*

Basic Properties of Rings: Let R be a ring. Then

1. $0a = a0 = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $(na)b = a(nb) = n(ab)$ for all $n \in \mathbf{Z}$ and $a, b \in R$;
5. $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$ for all $a_i, b_j \in R$.

Def. *A nonzero element* $a \in R$ *is a* **left zero divisor** *if there is a nonzero* $b \in R$ *such that* $ab = 0$ *(so* b *is a right zero divisor.) The element* a *is a* **zero divisor** *if* a *is both a left zero divisor and a right zero divisor.*

A ring R has no left/right divisors iff the left/right cancellation laws hold in R: for all $a, b, c \in R$ with $a \neq 0$,

$$ab = ac \quad \text{or} \quad ba = ca \quad \Longrightarrow \quad b = c.$$

Def. *An element* a *in a ring* R *with identity is* **left invertible** *if there is* $c \in R$ *such that* $ca = 1_R$. *An element* a *is* **invertible** *or a* **unit** *if it is both left and right invertible.*

Def. *Let* R *be a ring with identity* $1_R \neq 0$. *Then* R *is a*

integral domain	*commutative ring, with no zero divisor;*
division ring	*every nonzero element is a unit;*
field	*commutative division ring*
	= integral domain + division ring.

Ex. $\mathbf{Z}$ *is an integral domain. So is* $\mathbf{Z}[x]$.

Ex.

1. $\mathbf{Z}_6$ *is a commutative ring with identity.*
   identity: *1*
   units: *1, 5*
   zero divisors: *2, 3, 4*

2. $\mathbf{Z}_7$ *is a field. We have* $1 \cdot 1 = 2 \cdot 4 = 3 \cdot 5 = 6 \cdot 6 = 1$ *in* $\mathbf{Z}_7$.

3. *In general, if* n *is a positive integer and is not a prime, then* $\mathbf{Z}_n$ *has zero divisors; If* p *is a positive prime, then* Z_p *is a field.*

Def. *Let* R *be a ring. If there is a least positive integer* n *such that* $na = 0$ *for all* $a \in R$, *then* R *is said to have* **characteristic** n *(*$\mathrm{char}\, R = n$*). If no such* n *exists, then* R *is said to have* **characteristic zero**.

Ex. $\mathbf{Z}_n$ *has characteristic* n. *In general, if a ring* R *has identity* 1_R, *then* $\mathrm{char}\, R$ *is the least positive integer* n *(if it exists) such that* $n1_R = 0$.

Ex (polynomial ring). *If* R *is a ring, then* $R[x] = \{\sum_{i=0}^{n} r_i x^i \mid n \in \mathbf{Z}\}$ *is the polynomial ring of* R. *The ring* $R[x]$ *is commutative iff* R *is. The ring* $R[x]$ *has identity iff* R *has.* R *can be viewed as a subring of* $R[x]$.

Ex (endomorphism ring). *Let* A *be an abelian group and* $EndA$ *be the set of group homomorphisms* $f : A \to A$. *Define addition in* $EndA$ *by* $(f + g)(a) = f(a) + g(a)$, *and the multiplication in* $EndA$ *by* $(fg)(a) = f(g(a))$. *Then* $EndA$ *is a ring with identity. The matrix ring is a special case of endomorphism ring.*

Ex (external direct product). *Let* R_i $(i \in I)$ *be rings. Then*

$$\prod_{i \in I} R_i = \{(a_i)_{i \in I} \mid a_i \in R_i \ \ for \ \ i \in I\}$$

is a ring under the following operations:

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \qquad (a_i)_{i \in I}(b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

Ex. *Let* $A_1, \cdots, A_n$ *be ideals in a ring* R *such that*

1. $A_1 + \cdots + A_n = R$ *and*

2. *for each* k $(1 \le k \le n)$, $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots + A_n) = 0$

Then there is a ring isomorphism $R \simeq A_1 \times \cdots \times A_n$.

The ring R *is said to be the* **internal direct product** *of the ideals* A_i, *written as* $R = \prod A_i$ *or* $R = A_1 \times \cdots \times A_n$. *Note that each of the* A_i *is contained in* R, *which is slightly different from the external direct product.*

(proof)

Ex (coproduct (direct sum)). *The coproduct (direct sum) of R_i $(i \in I)$ is a subring of the direct product of R_i $(i \in I)$:*

$$\coprod_{i \in I} R_i = \bigoplus_{i \in I} R_i = \{(a_i)_{i \in I} \mid a_i \in R_i \text{ for } i \in I, \text{ only finitely many } a_i \neq 0\}$$

Ex (group ring). *If G is a multiplicative group and R is a ring, we define the group ring $R(G)$, such that every element $\sum_{g \in G} r_g g$ of $R(G)$ has only finitely many nonzero summands, and*

1. *$0g = 0$ for all $g \in G$.*
2. *Given $r_i, s_j \in R$ and $g_i, h_j \in G$,*

$$\begin{aligned} \sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i &= \sum_{i=1}^{n} (r_i + s_i) g_i \\ \left(\sum_{i=1}^{n} r_i g_i \right) \left(\sum_{j=1}^{m} s_j h_j \right) &= \sum_{i=1}^{n} \sum_{j=1}^{m} (r_i s_j)(g_i h_j) \end{aligned}$$

1.2 Subrings, Ideals, and Ring Homomorphisms

(III.1, III.2)

1.2.1 Subrings and Ideals

Def. *Let R be a ring. Let S be a nonempty subset of R that is closed under $+$, $-$, and $\cdot$. Then S has a ring structure and is called a* **subring** *of R.*

Def. *A subring I of R is a* **left ideal** *provided*

$$r \in R \quad \text{and} \quad x \in I \quad \Longrightarrow \quad rx \in I.$$

I is an **ideal** *if it is both a left and right ideal.*

Ex. *The* **center** *of a ring R is the set $C = \{c \in R \mid cr = rc \text{ for all } r \in R\}$ is a subring of R, but may not be an ideal of R. Think about the situation $R = \mathbf{C}^{2\times 2}$ (exercise).*

Ex. *Consider the matrix ring $R = \mathbf{Z}^{2\times 2}$. Then*

1. $I_1 = \begin{bmatrix} 2\mathbf{Z} & \mathbf{Z} \\ 2\mathbf{Z} & \mathbf{Z} \end{bmatrix}$ *is a left ideal (but not a right ideal) of R;*
2. $I_2 = \begin{bmatrix} 2\mathbf{Z} & 2\mathbf{Z} \\ \mathbf{Z} & \mathbf{Z} \end{bmatrix}$ *is a right ideal (but not a left ideal) of R;*
3. $I = (2\mathbf{Z})^{2\times 2} = \begin{bmatrix} 2\mathbf{Z} & 2\mathbf{Z} \\ 2\mathbf{Z} & 2\mathbf{Z} \end{bmatrix}$ *is an ideal of R;*
4. $S = \begin{bmatrix} \mathbf{Z} & 0 \\ 0 & \mathbf{Z} \end{bmatrix}$ *is a subring (but not an ideal) of R.*

A ring R always contains the trivial ideal 0 and the ideal R itself. The other ideals of R are called **proper ideals**.

Thm 1.1. *A nonempty set I of a ring R is a [left] ideal of R iff for all $a, b \in I$ and $r \in R$:*

1. $a, b \in I \quad \Longrightarrow \quad a - b \in I$; *and*
2. $a \in I,\ r \in R \quad \Longrightarrow \quad ra \in I$.

Cor 1.2. *Let R be a ring and each A_i a [left] ideal of R.*

1. *The intersection $\bigcap_{i\in I} A_i$ is a [left] ideal;*

2. *The sum*

$$\sum_{i\in I} A_i = \{a_1 + a_2 + \cdots a_n \mid n \in \mathbf{Z}^+,\ a_j \in \bigcup_{i\in I} A_i \text{ for } j = 1, 2, \cdots, n.\}$$

is a [left] ideal;

3. *Let*

$$A_1A_2\cdots A_n = \{\sum_{j=1}^{m} a_{j1}a_{j2}\cdots a_{jn} \mid m \in \overline{\mathbf{Z}^-},\ a_{jk} \in A_k,\ k = 1, 2, \cdots, n\}.$$

Then $A_1A_2\cdots A_n$ is also a [left] ideal.

Thm 1.3. *If $A, B, C, A_1, \cdots, A_n$ are [left] ideals of a ring R, then*

1. $(A + B) + C = A + (B + C)$;
2. $(AB)C = A(BC)$;
3. $B(A_1 + \cdots + A_n) = BA_1 + \cdots + BA_n$; *and* $(A_1 + \cdots + A_n)C = A_1C + \cdots + A_nC$.

Def. *Let X be a subset of a ring R, let $\{A_i \mid i \in I\}$ be the family of all ideals in R which contain X. Then $\bigcap_{i\in I} A_i$ is called* **the ideal generated by** X, *denoted by (X). The element of X are called the* **generators** *of the ideal (X). If X has finite cardinality, then (X) is a* **finitely generated ideal**. *In particular, an ideal (a) generated by a single element $a \in R$ is called a* **principal ideal**.

Thm 1.4. *For $X \subseteq R$, we have* $(X) = \sum_{a\in X} (a)$.

Thus it is important to describe the principal ideals.

Thm 1.5. *Suppose R is a ring and $a \in R$.*

1. *The principal ideal (a) consists of all elements of the form*

$$na + ra + as + \sum_{i=1}^{m} r_i a s_i, \quad \text{where} \quad r, s, r_i, s_i \in R, \quad m \in \mathbf{Z}^+,\ n \in \mathbf{Z}.$$

2. *If R has an identity, then*

$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in \mathbf{R},\ n \in \mathbf{Z}^+ \right\}$$

3. *If a is in the center of R (e.g. R is a commutative ring), then*

$$(a) = \{na + ra \mid r \in R,\ n \in \mathbf{Z}\}$$

4. *If R has an identity and a is in the center of R, then*

$$(a) = aR = Ra$$

If I is an ideal of R, then the cosets

$$R/I = \{a + I \mid a \in R\}$$

has a well-defined **factor ring** structure by the following operations:

$$\begin{aligned} (a+I)+(b+I) &= (a+b)+I \\ (a+I)(b+I) &= ab+I \end{aligned}$$

Ex. *If I is only a left ideal of R, can we define the factor ring R/I?*

Ex. *Let I be an ideal of R. If R is commutative or has an identity, then so is R/I. The converse is not true. For examples,*

1. $R = \begin{bmatrix} \mathbf{Z} & \mathbf{Z} \\ 0 & \mathbf{Z} \end{bmatrix}$, $I = \begin{bmatrix} 0 & \mathbf{Z} \\ 0 & 0 \end{bmatrix}$.
2. $R = 2\mathbf{Z}$ *and* $I = 6\mathbf{Z}$.

1.2.2 Homomorphisms

Def. *A function $f : R \to S$ between two rings R and S is a* **ring homomorphism** *if f preserves the corresponding operations: for all $a, b \in R$,*

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b).$$

Different kinds of homomorphisms:

monomorphism	injective homomorphism
epimorphism	surjective homomorphism
isomorphism	bijective homomorphism
automorphism	isomorphism of a ring R to R itself

Let $f : R \to S$ be a homomorphism. Then

$$\begin{aligned} \operatorname{Ker} f &= \{r \in R \mid f(r) = 0\} \\ \operatorname{Im} f &= \{s \in S \mid s = f(r) \text{ for some } r \in R\}. \end{aligned}$$

where $\operatorname{Ker} f$ is an ideal of R, and $\operatorname{Im} f$ is a subring of S.

Ideals and ring homomorphisms are closely related to each other. We have seen that $\operatorname{Ker} f$ is an ideal of R above. Conversely, given an ideal I of R, we have the **canonical epimorphism** (or projection)

$$\pi : R \to R/I \quad \text{defined by} \quad \pi(r) = r + I, \quad \text{such that} \quad \operatorname{Ker} \pi = I.$$

The following theorems and proofs are similar to those for the groups.

Thm 1.6 (First Isomorphism Theorem)**.** *If $f : R \to S$ is a ring homomorphism, then f induces a ring isomorphism $R/\operatorname{Ker} f \simeq \operatorname{Im} f$.*

Thm 1.7. *Let I and J be ideals of a ring R.*

1. *(***Second Isomorphism Theorem***) There is a ring isomorphism*

$$I/(I \cap J) \simeq (I + J)/J.$$

2. *(***Third Isomorphism Theorem***) If $I \subset J$, then J/I is an ideal in R/I and there is a ring isomorphism*

$$(R/I)/(J/I) \simeq R/J.$$

Thm 1.8. *Let I be an ideal of R. There is a one-to-one correspondence between the set of all ideals of R which contains I and the set of all ideals of R/I, given by $J \mapsto J/I$. So every ideal in R/I is of the form J/I for $I \subset J \subset R$.*

1.2.3 Prime Ideals and Maximal Ideals

Def. *An ideal P in a ring R is a* **prime ideal** *if $P \neq R$ and for any ideals A, B in R*

$$AB \subset P \quad \Longrightarrow \quad A \subset P \quad \text{or} \quad B \subset P$$

There are several equivalent characterizations of prime ideals (See Ex III.2.14). A very useful one is below

Thm 1.9. *If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$*

$$ab \in P \quad \Longrightarrow \quad a \in P \quad \text{or} \quad b \in P \tag{1.1}$$

then P is prime. Conversely if P is prime and R is commutative, then P satisfies condition (1.1).

(proof)
For commutative ring R, (1.1) is an equivalent condition for prime ideals.

Ex. *The zero ideal of an integral domain is prime.*

Ex. *Let R be a commutative ring with identity $1_R \neq 0$. Then an ideal P is prime iff the quotient ring R/P is an integral domain.*

Def. *An [left] ideal M in a ring R is* **maximal** *if $M \neq R$ and for every [left] ideal N such that $M \subset N \subset R$, either $M = N$ or $N = R$.*

Thm 1.10. *Let R be a ring with identity. Then every ideal in R is contained in a maximal ideal. Moreover, every maximal ideal M in R is prime.*

(proof)

Ex. *What happen if R has no identity. Consider $R = 2\mathbf{Z}$.*

1. *$M_1 = 4\mathbf{Z}$ is a maximal ideal, but M_1 is not a prime ideal.*
2. *$M_2 = 6\mathbf{Z}$ is a maximal ideal as well as a prime ideal. $2\mathbf{Z}/6\mathbf{Z} \simeq \mathbf{Z}_3$. However, the identity of $2\mathbf{Z}/6\mathbf{Z}$ is $4 + 6\mathbf{Z}$.*

Ex. *Let R be a commutative ring with identity $1_R \neq 0$. Then M is a maximal ideal of R iff R/M is a field. In particular, R is a field iff 0 is a maximal ideal in R.*

1.2.4 Chinese Remainder Theorem

Let A be an ideal in a ring R and $a, b \in R$. Then a is **congruent** to b modulo A (denoted $a \equiv b \mod A$) if $a - b \in A$. In other words,

$$a \equiv b \mod A \iff a - b \in A \iff a + A = b + A$$

We have

$$a_1 \equiv a_2 \mod A, \quad b_1 \equiv b_2 \mod A \implies$$
$$a_1 + b_1 \equiv a_2 + b_2 \mod A, \quad a_1 b_1 \equiv a_2 b_2 \mod A.$$

Thm 1.11 (Chinese Remainder Theorem). *Let $A_1, \cdots A_n$ be ideals in a ring R such that*

1. *$R^2 + A_i = R$ for all i and*
2. *$A_i + A_j = R$ for all $i \neq j$.*

Then for any $b_1, \cdots, b_n \in R$, there exists $b \in R$ such that

$$b \equiv b_k \mod A_k \qquad (k = 1, 2, \cdots, n).$$

Furthermore b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \cdots \cap A_n$.

Remark. *If R has identity, then $R^2 = R$, and $R^2 + A_i = R$ always holds.*

Cor 1.12. *Let $m_1, \cdots, m_n$, be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$. If $b_1, \cdots, b_n$ are any integers, then the system of congruences*

$$\begin{aligned} x &\equiv b_1 \mod m_1 \\ x &\equiv b_2 \mod m_2 \\ &\vdots \\ x &\equiv b_n \mod m_n \end{aligned}$$

has an integral solution that is uniquely determined modulo $m = m_1 \cdots m_n$.

Proof of the theorem: We proceed in three steps.

1. Claim: $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

   Clearly $R = A_1 + A_2$. Suppose that $R = A_1 + (A_2 \cap \cdots \cap A_{k-1})$. Then

   $$\begin{aligned} R &= A_1 + R^2 \\ &= A_1 + (A_1 + A_k)[A_1 + (A_2 \cap \cdots \cap A_{k-1})] \\ &\subset A_1 + A_k(A_2 \cap \cdots \cap A_{k-1}) \\ &\subset A_1 + (A_2 \cap \cdots \cap A_k) \subset R \end{aligned}$$

   So $R = A_1 + (A_2 \cap \cdots \cap A_k)$. By induction, $R = A_1 + (A_2 \cap \cdots \cap A_n)$.

2. Similarly, $R = A_k + (\bigcap_{i \neq k} A_i)$ for $k = 1, \cdots, n$. For b_k in the theorem, write $b_k = a_k + r_k$ for $a_k \in A_k$ and $r_k \in (\bigcap_{i \neq k} A_i)$.

3. Denote $r = r_1 + \cdots + r_n$. By $r_i \in A_k$ for $i \neq k$, we can verify that $r \equiv r_k \mod A_k$. The rest is clear.

□

1.3 Factorization in Integral Domain

(III.3) The ring R in this section is an *integral domain.* Some results here may be generalized to commutative rings.

Def. *$a \in R\backslash\{0\}$ is said to* **divide** *$b \in R$ (notation: $a \mid b$) if $ax = b$ for some $x \in R$. $a, b \in R\backslash\{0\}$ are* **associate** *if $a \mid b$ and $b \mid a$.*

Prop 1.13. *Let $a, b, u, r \in R$.*

1. *$a \mid b \iff (b) \subset (a)$.*
2. *a and b are associate $\iff (a) = (b) \iff a = br$ for a unit $r \in R$.*
3. *u is a unit $\iff u \mid r$ for all $r \in R \iff (u) = R$.*

(sketch of proof)

Def. *Suppose $p \in R\backslash\{0\}$ is not a unit. Then p is*
irreducible *if $p = ab \implies a$ or b is a unit*
prime *if $p \mid ab \implies p \mid a$ or $p \mid b$.*

Thm 1.14. *R an integral domain. $p \in R\backslash\{0\}$.*

1. *p is prime $\iff (p) \neq (0)$ is prime;*
2. *p is irreducible $\iff (p)$ is maximal in the set S of all proper principal ideals of R.*
3. *Every prime element of R is irreducible.*

Remark. *An irreducible element in an integral domain may not be a prime. See Ex III.3.3 (exercise).*

(sketch of proof of thm)

Def. *An integral domain R is a* **unique factorization domain** *if every nonzero nonunit element $a \in R$ can be "uniquely" expressed as $a = c_1 \cdots c_n$ with all c_i irreducible.*

The uniqueness in the above definition means that: if $a = c_1 \cdots c_n = d_1 \cdots d_m$, then $n = m$, and there is a permutation σ of $\{1, \cdots, n\}$ such that c_i and $d_{\sigma(i)}$ are associate for every i.

Thm 1.15. *If R is a unique factorization domain, then p is prime if and only if p is irreducible.*

(proof)

An integral domain R is a **principal ideal domain** if every ideal of R is a principal ideal.

Ex. *NOT principal ideal domains:*

1. $\mathbf{Z}[x]$;
2. $F[x, y]$ *where* F *is a field.*

Thm 1.16. *Every principal ideal domain is a unique factorization domain.*

(Proof is skipped. See Theorem III.3.7.)

Remark. *The converse is false.* $\mathbf{Z}[x]$ *is a unique factorization domain, but not a principal ideal domain.*

Def. *An integral domain* R *is a* **Euclidean domain** *if there is a function* $\varphi : R - \{0\} \longrightarrow \mathbf{N}$ *such that:*

1. $\varphi(a) \leq \varphi(ab)$ *for* $a, b \in R - \{0\}$.
2. *if* $a, b \in R$ *and* $b \neq 0$, *then there exist* $q, r \in R$ *such that* $a = qb + r$, *where either* $r = 0$ *or* $\varphi(r) < \varphi(b)$.

Ex. *Examples of Euclidean domains (which are also principal ideal domains):*

1. *The ring* $\mathbf{Z}$ *with* $\varphi(x) = |x|$ *is a Euclidean domain.*
2. *A field* F *with* $\varphi(x) = 1$ *for all* $x \in F - \{0\}$.
3. $F[x]$ *where* F *is a field, with* $\varphi(f(x)) = \deg f(x)$ *for* $f(x) \in F[x] - \{0\}$.
4. $\mathbf{Z}[i]$ *with* $\varphi(a + b\mathbf{i}) = a^2 + b^2$.

Thm 1.17. *Every Euclidean domain is a principal integral domain.*

Proof: Let $I \trianglelefteq R$. If $I = (0)$ then it is principal. Otherwise, choose $x \in I \backslash \{0\}$ such that $\varphi(x) \in \mathbf{N}$ is minimal. Then show that $I = (x)$.

Def. *Let* X *be a nonempty subset of an integral domain* R. *An element* $d \in R$ *is a* **greatest common divisor (gcd)** *of* X *provided:*

1. $d \mid a$ *for all* $a \in X$.
2. $c \mid a$ *for all* $a \in X \Longrightarrow c \mid d$.

If 1_R is the greatest common divisor of $a_1, \cdots, a_n \in R$, then $a_1, \cdots, a_n$ are said to be **relative prime**.

Prop 1.18. *Let R be an integral domain.*

1. *The greatest common divisor of $X \subset R$, if exists, is unique up to association (i.e. up to a multiple of units).*
2. *$d \in R$ is a greatest common divisor of $\{a_1, \cdots, a_n\}$ such that $d = r_1a_1 + \cdots + r_na_n$ for $r_i \in R$ if and only if $(d) = (a_1) + \cdots + (a_n)$.*
3. *If R is a unique factorization domain, then there exists a greatest common divisor for every nonempty $X \subset R$.*
4. *If R is a principal ideal domain, then a greatest common divisor of $X \subset R$ exists and is of the form $r_1a_1 + \cdots + r_na_n$ for some $a_i \in X$ and $r_i \in R$.*

Proof. 1. Easy

2. Interpret the definition of gcd in terms of ideal inclusion.
3. Easy
4. By 2.

□

1.4 Ring of Quotients and Localization

In this section, R denotes a *commutative ring*. Sometimes we require that R has identity.

Ex. *Consider the integral domain* $\mathbf{Z}$. *The field* $\mathbf{Q} = \{a/b \mid a, b \in \mathbf{Z},\ b \neq 0\}$ *can be viewed as constructed from* $\mathbf{Z}$ *by quotients. In* $\mathbf{Q}$, *we have* $a/b = c/d$ *iff* $ad - bc = 0$.

We can define quotients in the other rings.

Def. *A nonempty set* S *of a ring* R *is* **multiplicative** *if*

$$a, b \in S \Longrightarrow ab \in S.$$

Lem 1.19. *Let* S *be a multiplicative subset of a commutative ring* R. *The relation* $\sim$ *defined on* $R \times S$ *by*

$$(r, s) \sim (r', s') \quad \Longleftrightarrow \quad s_1(rs' - r's) = 0 \quad \textit{for some} \quad s_1 \in S$$

is an equivalent relation.

Again, let r/s denote the equivalent class of (r, s).

Thm 1.20. *Let* S *be a multiplicative subset of a commutative ring* R. *Let* $S^{-1}R$ *be the set of equivalent classes of* $R \times S$ *defined in Lemma 1.19. Then* $S^{-1}R$ *is a commutative ring with identity, where* $+$ *and* $\cdot$ *are defined by*

$$r/s + r'/s' = (rs' + r's)/ss' \qquad \textit{and} \qquad (r/s)(r'/s') = (rr')/(ss').$$

The ring $S^{-1}R$ is the **ring of quotients** or **quotient ring** of R by S.

Ex. *If* R *is an integral domain, and* S *consists of all nonzero elements of* R, *then* $S^{-1}R$ *is a field (the* **field of quotients of** R*) where* R *is embedded as a subring. Consider the situations:*

1. $R = \mathbf{Z}$.
2. $R = \mathbf{R}[x]$.

Ex. *If all elements of* S *are units, then* $S^{-1}R \simeq R$.

Ex. S *is a multiplicative set including* 0. *What is* $S^{-1}R$?

Ex. $R = \mathbf{Z}$, $S = 3\mathbf{Z}^+$, *what is* $S^{-1}R$?

Thm 1.21. *Let S be a multiplicative subset of R.*

1. *The map $\varphi_S : R \to S^{-1}R$ given by $r \mapsto rt/t$ (for any $t \in S$) is a well-defined homomorphism such that $\varphi_S(t)$ is a unit in $S^{-1}R$ for every $t \in S$.*
2. *If $0 \notin S$ and S contains no zero divisors, then φ_S is a monomorphism.*
3. *If S consists of units, then φ_S is an isomorphism.*

(sketch of proof)

Thm 1.22. *S a mult subset of comm. ring R. T a comm. ring with identity. If a ring homom. $f : R \to T$ satisfies that $f(s)$ is a unit in T for all $s \in S$, then there exists a unique ring homom. $\bar{f} : S^{-1}R \to T$ such that $\bar{f} \circ \varphi_S = f$. The ring $S^{-1}R$ is completely determined by this property.*

Prop 1.23. *S a mult subset of comm. ring R.*

1. *If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$. Conversely, every proper ideal of $S^{-1}R$ is of the form $S^{-1}I$ for $I \lhd R$ and $I \cap S = \emptyset$.*
2. *$S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \emptyset$.*
3. *If J is another ideal of R, then (exercise)*

$$\begin{aligned} S^{-1}(I+J) &= S^{-1}I + S^{-1}J \\ S^{-1}(IJ) &= (S^{-1}I)(S^{-1}J) \\ S^{-1}(I \cap J) &= S^{-1}I \cap S^{-1}J \end{aligned}$$

4. *If P is a prime ideal of R and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$. If Q is another prime ideal of R with $S \cap Q = \emptyset$ and $P \neq Q$, then $S^{-1}P \neq S^{-1}Q$.*

(proof of 4.)

Let P be a prime ideal of R. Then $S = R - P$ is a multiplicative subset of R. The ring $S^{-1}R$ ($= R_P$) is called the **localization of R by P**. If I is an ideal in R, then $S^{-1}I$ is denoted by I_P.

Thm 1.24. *Let P be a prime ideal of R*

1. *There is a one-to-one correspondence between the set of prime ideals of R which are contained in P and the set of prime ideals of R_P, given by $I \mapsto I_P$.*

2. The ideal P_P is the unique maximal ideal of R_P.

Def. *A* **local ring** *is a commutative ring with identity which has a unique maximal ideal.*

Ex. *If p is prime and $n \geq 1$, then $\mathbf{Z}_{p^n}$ is a local ring with unique maximal ideal (p).*

Prop 1.25. *If R is a local ring with unique maximal ideal M, then M consists of all nonunits of R. Conversely, if all nonunits of a commutative ring R with identity form an ideal, then R is a local ring.*

1.5 Rings of Polynomials and Factorizations

(III.5, III.6) In this section, D is an integral domain; E is an integer domain that contains D; F denotes the quotient field of D.

1.5.1 Rings of Polynomials and Formal Power Series

• Define the **ring of polynomials** over D:

$$D[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in D,\ n \in \mathbf{N}\}$$

with $+$ and $\cdot$ defined in the usual way.
Let $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ with $a_n \neq 0$:

coefficients:	all $a_i \in D$
leading coefficient:	a_n
constant term:	a_0
indeterminate:	x
degree of f:	$\deg f = n$

• The **ring of polynomials in n indeterminates** over D is $D[x_1, \cdots, x_n] := (D[x_1, \cdots, x_{n-1}])[x_n]$. It consists of

$$f = \sum_{(k_1,\cdots,k_n)\in\mathbf{N}^n} a_{k_1,\cdots,k_n} x_1^{k_1} \cdots x_n^{k_n} = \sum_{I\in\mathbf{N}^n, |I|\leq m} a_I \mathbf{x}^I,$$

where $m \in \mathbf{N}$, $\mathbf{x} = (x_1, \cdots, x_n)$, $I = (k_1, \cdots, k_n) \in \mathbf{N}^n$, and

$$|I| := k_1 + \cdots + k_n, \qquad a_I := a_{k_1,\cdots,k_n}, \qquad \mathbf{x}^I := x_1^{k_1} \cdots x_n^{k_n}.$$

The elements a_I are **coefficients**. The elements $x_1, \cdots, x_n$ are **indeterminates**. A polynomial of the form $a x_1^{k_1} \cdots x_n^{k_n}$ is called a **monomial**. We can define **the degree of a polynomial**, and **homogeneous polynomial of degree** k.

Prop 1.26. *Let D be an int dom and $f, g \in D[x_1, \cdots, x_n]$.*

1. $\deg(f + g) \leq \max(\deg f, \deg g)$.
2. $\deg(fg) = \deg f + \deg g$.

(Proof is skipped)

Def. *Let D and E be int dom with $D \subseteq E$. An element $(c_1, \cdots, c_n) \in E^n$ is said to be a* **root** *or a* **zero** *of $f \in D[x_1, \cdots, x_n]$ if $f(c_1, \cdots, c_n) = 0$.*

• The **ring of formal power series** over the ring D is

$$D[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in D \right\}.$$

It forms a ring under the usual $+$ and $\cdot$.

1.5.2 Factorizations over an integer domain

Thm 1.27 (Division Algorithm)**.** *Let $f, g \in D[x]$. If the leading coefficient of g is a unit in D, then there exist unique polynomials $q, r \in D[x]$ such that*

$$f = qg + r \qquad \textit{and} \qquad \deg r < \deg g.$$

Cor 1.28 (Remainder Theorem)**.** *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$. For any $c \in D$ there exists a unique $q(x) \in D[x]$ such that*

$$f(x) = q(x)(x - c) + f(c).$$

In particular, $c \in D$ is a root of $f(x)$ if and only if $(x - c)$ divides $f(x)$.

Prop 1.29. *If $f \in D[x]$ has degree n, then f has at most n distinct roots in any integer domain $E \supseteq D$.*

(sketch of proof)

Def. *The* **formal derivative** *of $f = \sum_{k=0}^{n} a_k x^k \in D[x]$ is*

$$f' = \sum_{k=0}^{n} k a_k x^{k-1} \in D[x].$$

It satisfies the usual derivative properties (sum/product/quotient/chain rules, etc.). For example, $c \in D$ is a multiple root of f iff $f(c) = 0$ and $f'(c) = 0$.

1.5.3 Factorizations over a UFD

$\star$ From now on, we consider polynomial rings over a unique factorization domain (UFD). **Let D be a UFD with quotient field F.**

Def. *Let $f = \sum_{i=0}^{n} a_i x^i \in D[x]$. Every element in $\gcd(a_0, \cdots, a_n)$ is called a* **content** *of f, denoted by $C(f)$. If $C(f)$ is a unit in D, then f is said to be* **primitive**.

- Every polynomial $f \in D[x]$ can be written as $f = C(f)f_1$ with $f_1 \in D[x]$ primitive.
- $C(fg) = C(f)C(g)$ for $f, g \in D[x]$.

We write $a \overset{D}{\sim} b$ to denote that a and b are associate in D.

Prop 1.30. *Let D be a UFD with quotient field F. Let f and g be primitive polynomials in $D[x]$.*

1. *$f \overset{D[x]}{\sim} g$ if and only if $f \overset{F[x]}{\sim} g$.*
2. *f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.*

Proof.

1. If $f \overset{F[x]}{\sim} g$, then $f = gu$ for a unit $u \in F[x]$. Then $u \in F$, say $u = c/d$ for $c, d \in D$. Then $df = cg$. So $dC(f) \overset{D}{\sim} C(df) \overset{D}{\sim} C(cg) \overset{D}{\sim} cC(g)$. Then $c \overset{D}{\sim} d$ since f and g are primitive. So $u = c/d$ is a unit in D and $f \overset{D[x]}{\sim} g$. The converse is trivial.

2. Suppose f is irreducible in $D[x]$ and $f = gh$ with $g, h \in F[x]$ and $\deg g \geq 1$, $\deg h \geq 1$. We can write $g = (a/b)g_0$ and $h = (c/d)h_0$ with $a, b, c, d \in D$, $g_0, h_0 \in D[x]$ primitive. Then $bdf = acg_0h_0$ in $D[x]$. Then $bd \overset{D}{\sim} C(bdf) \overset{D}{\sim} C(acg_0h_0) \overset{D}{\sim} ac$. Then $f \overset{D[x]}{\sim} g_0h_0$, a contradiction!

   Conversely, if f is irreducible in $F[x]$ and $f = gh$ with $g, h \in D[x]$, then one of g and h, say g, is a unit in $F[x]$. So g is a constant. Then $C(f) = gC(h)$. Since f is primitive, g must be a unit in D. Hence f is irreducible in $D[x]$.

□

Note the $F[x]$ for a field F is a Euclid dom/PID/UFD. We use it to prove the following theorem.

Thm 1.31. *If D is a UFD, then $D[x_1, \cdots, x_n]$ is a UFD.*

Proof. It suffices to prove that D is a UFD implies that $D[x]$ is a UFD. Let F be the quotient field of D.

Existence: Every $f \in D[x]$ can be written as $f = C(f)f_1$, where $f_1 \in D[x]$ is primitive. $C(f) = 1$ or $C(f) = c_1 \cdots c_m$, with each c_i irreducible in D and hence irreducible in $D[x]$. If $\deg f_1 > 0$, we write $f_1 = p_1^* p_2^* \cdots p_n^*$ with each p_i^* irreducible in $F[x]$ (a UFD); write $p_i^* = (a_i/b_i)p_i$ with $a_i, b_i \in D$, $p_i \in D[x]$ is primitive in $D[x]$ and irreducible in $F[x]$ (whence p_i is irreducible in $D[x]$); write $a = a_1 \cdots a_n$ and $b = b_1 \cdots b_n$. Then $bf_1 = ap_1 \cdots p_n$. Since f_1 and $p_1, \cdots, p_n$ are primitive, $a \overset{D}{\sim} b$. Then $u = a/b$ is a unit in D and $f = C(f)f_1 = c_1 \cdots c_m(up_1)p_2 \cdots p_n$ is a product of irreducible elements in $D[x]$.

Uniqueness: Suppose $f \in D[x]$ has two decompositions

$$f = c_1 \cdots c_m p_1 \cdots p_n = d_1 \cdots d_r q_1 \cdots q_s,$$

where $c_i, d_j \in D$ are irreducible, and $p_k, q_l \in D[x]$ have positive degree and irreducible. Then $c_1 \cdots c_m \overset{D}{\sim} d_1 \cdots d_r$ as they are contents of f. Then $p_1 \cdots p_n \overset{F[x]}{\sim} q_1 \cdots q_s$. By the uniqueness of decompositions in D and $F[x]$, we get the uniqueness of decomposition of f. □

Thm 1.32 (Eisenstein's Criterion)**.** *Let D be a UFD with quotient field F. If $f = \sum_{i=0}^n a_i x^i \in D[x]$, $\deg f \geq 1$, and p is irreducible in D such that*

$$p \nmid a_n; \qquad p \mid a_i \quad \textit{for} \quad i = 0, 1, \cdots, n-1; \qquad p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Proof. $f = C(f)f_1$ with f_1 primitive in $D[x]$. The coefficients of $f_1 = \sum_{k=0}^{n} a_k^* x^k$ satisfy that:

$$p \nmid a_n^*; \qquad p \mid a_i^* \quad i = 0, 1, \cdots, n-1; \qquad p^2 \nmid a_0^*.$$

It suffices to show that f_1 is irreducible in $D[x]$. Suppose on the contrary, $f_1 = gh$ with $g = \sum_{i=0}^{r} b_i x^i \in D[x]$, $\deg g = r \geq 1$; and $h = \sum_{j=0}^{s} c_j x^j \in D[x]$,

$\deg h = s \geq 1$. The irreducible element p is prime since D is a UFD. $p \mid a_0^* = b_0 c_0$. So $p \mid b_0$ or $p \mid c_0$, say $p \mid b_0$. Then $p \nmid c_0$ since $p^2 \nmid a_0^*$. Some coefficient b_ℓ of g is not divisible by p. Suppose ℓ is the integer such that

$$p \mid b_i \quad \text{for} \quad i < \ell \quad \text{and} \quad p \nmid b_\ell.$$

Then $\ell \leq r < n$ and $p \mid a_\ell^* = b_0 c_\ell + b_1 c_{\ell-1} + \cdots + b_\ell c_0$. So $p \mid b_\ell c_0$, which is a contradiction since p is prime, $p \nmid b_\ell$ and $p \nmid c_0$. Therefore, f_1 must be irreducible in $D[x]$. □

Ex. *Use Eisenstein's Criterion to show that:*

1. $f = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbf{Z}[x]$ *is irreducible in* $\mathbf{Z}[x]$.
2. *Suppose* R *is a UFD. Then* $f = y^3 + x^2y^2 + x^3y + x \in R[x, y]$ *is irreducible in* $R[x, y]$.
3. $x^n - p$ *and* $x^n + p$ *are irreducible if* $p \in D$ *is irreducible.*
4. *Let* $f_n(x) = (x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + x + 1$. *Then* $f_n(x)$ *is irreducible in* $\mathbf{Q}[x]$ *(and* $\mathbf{Z}[x]$*) if and only if* n *is prime. (Hint: When* n *is prime, consider* $g_n(x) = f_n(x + 1)$*).*