Introduction to Rings

Hong-Jian Lai

August 2000

1. Rings and Homomorphisms

(1.1) A ring is a non emptyset $R$ together with two binary operations (denoted as addition ($+$) and multiplication) such that

(R1) $(R, +)$ is an abelian group, (its additive identity is usually denoted by $0$);
(R2) the multiplication is associative;
(R3) $\forall a, b, c \in R, a(b + c) = ab + ac, (a + b)c = ac + bc$.

(1.1a) Suppose $R$ is a ring.

(R4) If $\forall a, b \in R, ab = ba$, then $R$ is a commutative ring.
(R5) if $\exists 1_R \in R$ such that $\forall a \in R, a1_R = 1_Ra = a$, then $R$ is a ring with identity, and this element $1_R$ is a (multiplicative) identity of $R$.

(1.2) (Thm 1.2) Let $R$ be a ring. Then $\forall a, b \in R$ and $\forall n \in \mathbb{Z}$,

(i) $0a = a0 = 0$,
(ii) $a(-b) = (-a)b = -(ab)$ and $(-a)(-b) = ab$,
(iii) $n(ab) = a(nb) = (na)b$, and
(iv) $\left( \sum_{i=1}^{n} a_i \right) \left( \sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_ib_j, \ \forall a_i, b_j \in R$.
(v) If $R$ is a ring with identity, then its multiplicative identity is unique.

(1.3) Let $R$ be a ring. If $a, b \in R - \{0\}$ such that $ab = 0$, then $a$ is a left zero divisor and $b$ is a right zero divisor. Each of $a$ and $b$ is also called a zero divisor.

Example: $M_n(F)$, the set of all $n \times n$ matrices over the field $F$. 

1
(1.4) Let $R$ be a ring with identity $1_R$. If $a, b \in R$ such that $ab = 1_R$, then $a$ is left invertible and $b$ is right invertible. An element $a$ that is both left invertible as well as right invertible is a unit.

Examples: $\mathbb{Z}_n$, $\mathbb{Z}$.

(1.5) A commutative ring $R$ with identity $1_R \neq 0$ is an integral domain if $R$ has no zero divisors; an integral domain in which every element is a unit is a field. A ring $R$ with identity $1_R \neq 0$ is a division ring (also called a skew field) if every element is a unit.

Example: The real quaternions Let $\mathbb{Q}$ denote the set of $\mathbb{R}^4$. Then $(\mathbb{Q}, +)$ is an abelian group. Denote

$$1 = (1, 0, 0, 0), \ i = (0, 1, 0, 0), \ j = (0, 0, 1, 0), \ k = (0, 0, 0, 1).$$

Define $(a_1, a_2, a_3, a_4) = a_1 + a_2i + a_3j + a_4k$. For multiplication, define:

$$1a = a1 = a, \forall a \in \mathbb{Q}, \ i^2 = j^2 = k^2 = -1,$$

and

$$ij = k; \ jk = i; \ ki = j; \ ji = -k; \ kj = -i; \ ik = -j.$$  

“Linearly” expand these to general products in $\mathbb{Q}$. Then $\mathbb{Q}$ forms a skew field (non-commutative division ring).

(1.6) (Thm 1.6) (The binomial formula). Let $R$ be a ring, and let $a, b \in R$. If $ab = ba$, then

$$(a + b)^n = \sum_{i=0}^{n} \left( \begin{array}{c} n \\ i \end{array} \right) a^i b^{n-i}.$$  

(1.7) Ring Homomorphisms and Isomorphisms Let $R$ and $R'$ be rings. A function $f : R \rightarrow R'$ is a homomorphism if $\forall a, b \in R$,

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

If, in addition, $f$ is a bijection, then $f$ is an isomorphism. The kernel of $f$ is the set $\ker(f) = \{a \in R : f(a) = 0\}$.  

2
(1.7a) (Properties of a kernel) Let \( f : R \rightarrow R' \) be a ring homomorphism with \( K = \ker(f) \). Then

(i) \( K \) is a subring of \( R \) (a nonempty subset \( L \) of \( R \) is a subring if \( L \) with the same binary operations of \( R \) forms a ring itself.)

(ii) \( \forall r \in R \) and \( \forall a \in K \), \( ra \in K \) and \( ar \in K \); moreover, for any integer \( n \), \( na \in K \).

Any subring \( I \) of \( R \) is called an ideal if it also satisfies (ii) in (1.7a).

2. Ideals

(2.1) Let \( R \) be a ring and let \( I \subseteq R \) be a subring.

(i) If, \( \forall r \in R, rI \subseteq I \), (resp. \( r \in I \subseteq I \)) then \( I \) is a left ideal (resp. right ideal).

(ii) \( I \) is an ideal if it is both a left ideal and a right ideal.

Two Important Examples: The integers \( \mathbb{Z} \) and \( F[x] \), the ring of polynomials over a field \( F \).

(2.2) (Thm 2.2) Let \( I \subseteq R \) be a nonempty set.

(i) \( I \) is a subring iff \( \forall a, b \in I \), \( a - b \in I \), and \( ab \in I \).

(ii) \( I \) is a left ideal (resp. right ideal) iff \( \forall a, b \in I \), \( a - b \in I \), and \( \forall a \in I, r \in R \), \( ra \in I \) (resp. \( ar \in I \)).

(2.3) (Examples) Let \( R \) be a ring.

(i) Let \( \{I_j : j \in J\} \) be a collection of (left) ideals of \( R \), then \( \bigcap_{j \in J} I_j \) is also a (left) ideal of \( R \).

(ii) The center of \( R \) is

\[
C(R) = \{ a \in R : \forall r \in R, ra = ar \}.
\]

Then \( C(R) \) is a subring but \( C(R) \) may not be an ideal.

Example: Let \( R = M_2(\mathbb{R}) \), all 2 by 2 real matrices with the matrix addition and matrix multiplication.

(2.4) (Ideals generated by elements) Let \( X \subseteq R \) be a subset of a ring \( R \). The smallest ideal containing \( X \) (the intersection of all ideals of \( R \) containing \( X \)) is de-
noted by \((X)\). When \(X = \{a\}\), we use \((a)\) for \((\{a\})\), and call \((a)\) a **principal ideal**. In integral domain in which every ideal is principal is called an **principal ideal domain** (or just **PID**).

(2.5) (Thm 2.5) Let \(R\) be a ring, \(a \in R\) and \(X \subseteq R\).

(i) \((a) = \{ra + as + na + \sum_{i=1}^{m} r_ias_i : r, s, r_i, s_i \in R\) and \(m, n \in \mathbb{Z}, m > 0\}\).

(ii) If \(R\) has an identity, then \((a) = \{m \sum_{i=1}^{n} r_ia_i + s : r_ia_i, s_i \in R\) and \(m \in \mathbb{Z}, m > 0\}\).

(iii) If \(a \in C(R)\), then \((a) = \{ra + na : r \in R\) and \(n \in \mathbb{Z}\}\).

(iv) If \(R\) has an identity and \(a \in C(R)\), then \((a) = \{ra : r \in R\}\).

**PF:** In each case, check (1) the right hand side is an ideal, (2) an ideal containing \(a\) must contain the elements in the set of the right hand side.

(2.6) Let \(A_1, A_2, ..., A_n, A, B \subseteq R\) be non empty subsets. Define

\[A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n : a_i \in A_i, 1 \leq i \leq n\}\]

and

\[AB = \left\{\sum_{i=1}^{m} a_ib_i : a_i \in A, b_i \in B, 1 \leq i \leq n \text{ and } n \in \mathbb{Z}, n > 0\right\}, \text{ and } A_1A_2\cdots A_n = (A_1A_2\cdots A_{n-1})\].

If \(A_1, A_2, ..., A_n, A, B, C\) are (left) ideals of \(R\), then each of the following holds.

(i) \(A_1 + A_2 + \cdots + A_n\) and \(A_1A_2\cdots A_n\) are also (left) ideals of \(R\).

(ii) \((A + B) + C = A + (B + C)\).

(iii) \((AB)C = A(BC)\).

(iv) \(A(B + C) = AB + AC\) and \((A + B)C = AC + BC\).

**PF:** Apply definitions/properties.

(2.7) Let \(R\) be a ring and \(I \subseteq R\) be an ideal. The quotient group \(R/I\) (viewed as cosets of the abelian group \(R\)) with the multiplication

\[(a + I)(b + I) = ab + I, \forall a, b \in R,\]

forms a ring, called a **Quotient Ring** of \(R\). If \(R\) has an identity 1, then \(1 + I\) will be the identity of \(R/I\).
PF: Need to show the multiplication is well defined.

(2.8) Isomorphism Theorems: each of the group isomorphism theorem. The proofs are similar.

(2.9) Let $R$ be a ring and $I \subseteq R$ be an ideal.
   (i) If for any ideas $A, B$ in $R$,

   \[ AB \subseteq I \implies A \subseteq I \text{ or } B \subseteq I, \]

   then $I$ is a prime ideal.

   (ii) If for any (left) ideal $L$ in $R$,

   \[ I \subseteq L \neq R \implies I = L, \]

   then $I$ is a maximal (left) ideal.

(2.10) (Thm 2.15) Let $R$ be a ring and $P \subset R$ be an ideal such that $P \neq R$.
   (i) If $\forall a, b \in R$, $ab \in P \implies a \in P$ or $b \in P$, then $P$ is prime.

   (ii) If $R$ is commutative and $P$ is prime, then

   \[ \forall a, b \in R, ab \in P \implies a \in P \text{ or } b \in P. \]

PF: (i) Pick $a \in A - P$ and $\forall b \in B$ to see $B \subseteq P$.
   (ii) Use principal ideals.

(2.11) (Thm 2.16) Let $R$ be a commutative ring with identity $1 \neq 0$ and $I$ be an ideal in $R$. TFAE
   (i) $I$ is prime.

   (ii) $R/I$ is an integral domain.

PF: Apply Definitions.

(2.12) (Thm 2.20) Let $R$ be a ring with identity $1 \neq 0$, and $M$ be an ideal of $R$. 

(i) If $M$ is maximal and $R$ is commutative, then $R/M$ is a field.

(ii) If $R$ is commutative, then every maximal ideal is prime.

(iii) If $M$ contains a unit, then $M = R$.

(iv) If $R/M$ is a division ring, then $M$ is maximal.

PF: (i) By (2.7), $R/M$ is a commutative ring with identity $1 + M \neq M$. \( \forall a \in R - M, \) $M$ maximal $\implies M + (a) = R$, and so $1 = m + ra$ by (2.5)(iv).

(iii) If $M$ contains an unit, then $1 \in M$ and so $R = (1) \subseteq M$.

(iv) Let $L$ be an ideal in $R$ with $M \subseteq L$. \( \forall a \in L - M, \) $a + M$ has an inverse $b + M$, and so $ab + M = 1 + M \implies ab - 1 \in M \subseteq L$. As $ab \in L$, $1 \in L$ and so $R = L$. 

3. Some Applications

(3.1) **Fermat’s Little Theorem**: If \( n, p \) are integers such that \( p \) is a prime and \( (n, p) = 1 \), then \( p | n^{p-1} - 1 \).

**PF:** Recall that the set of all units form a multiplicative group. (View \( n \in \mathbb{Z}_p - \{0\} \) and use Lagrange in group).

\((3.1a) n^p \equiv n \pmod{p}, \forall n \in \mathbb{Z}, \text{ and prime } p.\)

(3.2) For each \( n \in \mathbb{Z}^+ \) (positive integers), \( \phi(n) \) is the number of integers between 1 and \( n \) that are relatively prime with \( n \).

**Euler’s Generalization:** If \( (m, n) = 1 \), then \( m^{\phi(n)} \equiv 1 \pmod{n} \). (Use the same argument in (3.1a).)

(3.3) Let \( R \) be a ring with identity \( 1 \neq 0 \), and \( U(R) \) be the set of all units in \( R \). If \( a \in U(R) \), then the equation \( ax = b \) has a unique solution \( x = a^{-1}b \) in \( R \).

Example: \( R = \mathbb{Z}_m \).

\((3.3a) \) Let \( a, b \in \mathbb{Z}_m \) and let \( d = (m, a) \). Then

(i) \( ax = b \) has a solution in \( \mathbb{Z}_m \) if and only if \( d | b \).

(ii) When \( d | b \), there are exactly \( d \) solutions.

**PF:** (i) \( ax - b = qm \implies d | b \). Conversely, assume \( a = a_1d, b = b_1d \) and \( m = m_1d \). Note that \( ax - b = qm \iff a_1x - b_1 = qm_1 \). Since \((a_1, m_1) = 1\), by (1.12), \( a_1x - b_1 = qm_1 \) has a unique solution \( s \). (ii) But in \( \mathbb{Z}_m \) (viewed as \{0, ..., \( m - 1\} \)), there are exactly \( d \) elements of the form \( s + km_1, (0 \leq k \leq d - 1) \) that are modulo \( m_1 \).

Example: Solve \( 45x \equiv 15 \pmod{24} \). Note \((45,24)=3\). Consider \( 15x \equiv 5 \pmod{8} \). It becomes \( 7x \equiv 5 \pmod{8} \). Since \( 7^2 \equiv 1 \pmod{8}, x \equiv (7)(5) \equiv 3 \pmod{8} \). Therefore \( x \equiv 3, 11, 19 \pmod{24} \).

(3.4) Notation: Let \( R \) be a ring and \( A \) be an ideal in \( R \). Write \( a \equiv_A b \) or \( A \equiv b \pmod{A} \) if \( a - b \in A \).

(3.5) (Thm 2.25) **Chinese Remainder Theorem** Let \( R \) be a ring and let \( A_1, A_2, ..., A_n \) be ideals in \( R \) such that for all \( i, R^2 + A_i = R \), and for all \( i \neq j, A_i + A_j = R \).
\[(i) \ \forall b_1, b_2, \ldots, b_n \in R, \exists b \in R \text{ such that} \]
\[b \equiv_{A_i} b_i, \ \forall i.\]

(ii) If \( b \) and \( b' \) are two elements in \( R \) satisfying (i), then
\[b \equiv b'( \mod \ \bigcap_{i=1}^n A_i).\]

PF: (Step 1) Apply induction to show for each \( k \),
\[R = A_k + \prod_{i=1, i \neq k}^n A_i.\]

For induction basis, use \( R = A_1 + A_2 = A_1 + A_3 \) to show that
\[R = A_1 + R^2 \subseteq A_1 + (A_2 \cap A_3) \subseteq R,\]
and so equalities must hold. Proceed induction similarly.

(Step 2) By Step 1, \( \forall i, \exists a_i \in A_i \text{ and } r_i \in \bigcap_{i=1}^n A_i \text{ such that } b_i = a_i + r_i \). Let \( b = \sum_{i=1}^n r_i \).

(Use the fact that \( A_i A_j \subseteq A_i \cap A_j \).)

(ii) Note that \( b - b' \in A_i \) for all \( i \).

(3.6) (Cor 2.26) Let \( m_1, m_2, \ldots, m_n \) be positive integers such that \( (m_i, m_j) = 1 \) for all \( i \neq j \). If \( b_1, b_2, \ldots, b_n \) are integers, then the system
\[
\begin{align*}
x &\equiv_{m_1} b_1 \\
x &\equiv_{m_2} b_2 \\
\vdots & \vdots \\
x &\equiv_{m_n} b_n
\end{align*}
\]
has an integral solution \( x \) that is uniquely determined modulo \( m = m_1 m_2 \cdots m_n \).

4. Factorizations in Commutative Rings

(4.1) Let \( R \) be a ring, \( a \in R - \{0\} \) and \( b \in R \).

(i) We say that \( a \) divides \( b \) (written \( a \mid b \)) if the equation \( ax = b \) has a solution in
R. We say \( a \) and \( b \) are **associates** if both \( a|b \) and \( b|a \) hold.

(ii) If \( R \) is commutative with 1, then \( c \in R - \{0\} \) is **irreducible** (or **reduced**) if \( c \not\in U(R) \) and \( c = ab \implies a \in U(R) \) or \( b \in U(R) \).

(iii) If \( R \) is commutative with 1, then \( p \in R - \{0\} \) is a **prime** if if \( p \not\in U(R) \) and \( p|ab \implies p|a \) or \( p|b \).

(4.2) (Thm 3.2) Let \( R \) be a commutative ring with 1, and \( a, b, u \in R \).

(i) \( a|b \iff (b) \subseteq (a) \).

(ii) \( a \) and \( b \) are associates \( \iff \) \( (b) = (a) \).

(iii) \( u \) is a unit \( \iff \) \( (u) = R \).

(iv) \( u \) is a unit \( \iff \) \( u|r; \forall r \in R \).

(v) being associate is an equivalence relation.

(vi) If \( R \) is an integral domain, then \( a \) and \( b \) are associates if and only if \( a = rb \) for some unit \( r \in R \).

PF: (Think about integers)

(4.3) (Thm 3.4) Let \( R \) be an integral domain and let \( p, c \in R - \{0\} \).

(i) \( p \) is a prime iff \( (p) \) is a prime ideal.

(ii) \( c \) is irreducible iff \( (c) \) is maximal in the set of all proper principal ideals of \( R \).

((c) may not be a maximal ideal of \( R \).)

(iii) Every prime element is irreducible.

(iv) If \( R \) is a PID, then \( p \) is prime iff \( p \) is irreducible.

(v) An associate of an irreducible element if also irreducible.

PF: Use the fact that \( x|y \iff (y) \subseteq (x) \) for (i) and (ii). (iii) and (iv): \( c \) irreducible \( \implies \) \( (c) \) maximal \( \implies \) \( (c) \) prime \( \implies \) \( c \) prime if \( \implies c = ab \), then \( c|ab \) and so wma \( c|a \). Thus \( a = cx \) and so \( c = cxb \) resulting \( 1 = xb \), and \( b \in U(R) \). Thus \( c \) is irreducible.

(4.4) An integral domain is a UFD (**uniquely factorization domain**) if both of the following hold.

(UFD1) (Existence of factorization) \( \forall a \in R - (U(R) \cup \{0\}) \), \( a \) can be written as \( a = c_1c_2 \cdots c_n \), where \( c_1, c_2, ..., c_n \) are irreducible.
(UFD2) (Uniqueness of factorization) If \( a = c_1c_2 \cdots c_n \) and \( a = b_1b_2 \cdots b_m \), where each \( c_i \) and \( b_j \) is irreducible, then \( n = m \) and for some permutation \( \sigma \) of \( \{1, 2, \ldots, n\} \) \( c_i \) and \( b_{\sigma(i)} \) are associates for every \( i \).

(4.5) Let \( R \) be a ring. We define the following.

(ACC) The **ascending chain condition (ACC) for ideals** holds in \( R \) if every strictly increasing sequence \( N_1 \subset N_2 \subset N_3 \subset \cdots \) \( (N_i \neq N_j \text{ if } i \neq j) \) of ideals in \( R \) is of finite length.

(MC) The **maximum condition (MC) for ideals** holds in \( R \) if every nonempty set \( S \) of ideals in \( R \) contains an ideal not properly contained in any other ideal of the set \( S \).

(FBC) The **finite basis condition (FBC) for ideals** holds in \( R \) if for each ideal \( N \) in \( R \), there exists a finite set \( B_N \) such that \( N \) is the intersection of all ideals of \( R \) containing \( B_N \). The set \( B_N \) is a **finite basis** for \( N \).

(DCC) The **descending chain condition (DCC) for ideals** holds in \( R \) if every strictly decreasing sequence \( N_1 \subset N_2 \subset N_3 \subset \cdots \) \( (N_i \neq N_j \text{ if } i \neq j) \) of ideals in \( R \) is of finite length.

(mC) The **minimum condition (mC) for ideals** holds in \( R \) if every nonempty set \( S \) of ideals in \( R \) contains an ideal that does not properly contain any other ideal of the set \( S \).

(4.6) ACC holds in a PID.

PF: (1) Union of a nest of ideals is also an ideal. (2) This is a PID.

(4.7) (Thm 3.7) Every PID \( R \) is a UFD. (Axiom of Choice needed?)

PF: (UFD1) Pick \( a \in R - (U(R) \cup \{0\}) \).

(Step 1) Either \( a \) is irreducible, or there exists an irreducible \( p_1 \) such that \( a = p_1c_1 \), where \( c_1 \in R - (U(R) \cup \{0\}) \).

If \( a \) is not irreducible, then \( a = a_1b_1 \), \( a_1, b_1 \in R - (U(R) \cup \{0\}) \). If \( a_1 \) is not irreducible, then \( a_1 = a_2b_2 \), \( a_2, b_2 \in R - (U(R) \cup \{0\}) \). If no such an irreducible element exists,
then we have a strictly increasing chain of ideals

\[(a) \subset (a_1) \subset (a_2) \subset \cdots \]

It must terminate at an \((a_r)\), and so \(a_r\) must be irreducible, a contradiction.

(Step 2) Apply (Step 1) to \(c_1\), we have either \(c_1\) is irreducible, or \(c_1 = p_2c_2\), where \(p_2\) is irreducible and \(C_2 \in R - (U(R) \cup \{0\})\). If (UFD1) fails, then we have a strictly increasing chain of ideals

\[(a) \subset (c_1) \subset (c_2) \subset \cdots \]

It must terminate at a \((c_r)\), and so \(c_r\) must be irreducible. It follows that \(a = p_1p_2 \cdots p_{r-1}c_r\) is a product of irreducibles, a contradiction.

(UFD2) Suppose that \(a = c_1c_2 \cdots c_n\) and \(a = b_1b_2 \cdots b_m\), where each \(c_i\) and \(b_j\) is irreducible. Assume that \(m \geq n\). Then \(c_1|a = b_1b_2 \cdots b_m\), and we may assume that \(c_1|b_1\) (since \(c_1\) is a prime also.) Therefore, \(c_1 = b_1u_1\) for some \(u_1 \in U(R)\), and so

\[b_1u_1c_2 \cdots c_n = a = b_1b_2 \cdots b_m.\]

Since \(R\) is a domain, \(u_1c_2 \cdots c_n = b_2 \cdots b_m\). Repeat this process to get

\[1 = u_1u_2 \cdots u_nb_{n+1} \cdots b_m.\]

Since each \(b_i\) is a non unit, \(m = n\).

(4.8) Let \(N\) denote the set of positive integers and \(R\) a commutative ring. \(R\) is a Euclidean ring if there is a map \(\phi : R - \{0\} \rightarrow N\) such that

1. (ED1) \(\forall a, b \in R\) with \(ab \neq 0\), \(\phi(a) \leq \phi(ab)\).
2. (ED2) If \(a, b \in R\) and \(b \neq 0\), then \(\exists q, r \in R\) such that \(a = qb + r\) with \(r = 0\) or \(r \neq 0\) and \(\phi(r) < \phi(b)\)

If \(R\) is a domain satisfying both (ED1) and (ED2), then \(R\) is a Euclidean domain (ED).

(4.9) (Important Example: Guassian integers) Let \(Z[i]\) denote the subset of complex numbers of the form \(a + bi\), where \(a, b \in Z\) are integers and \(i^2 = -1\). Define \(\phi(a + bi) = a^2 + b^2\), then \(Z[i]\) is an ED.

Other example: \(Z\) with \(\phi(n) = |n|; F[x]\) with \(\phi(f(x)) = \text{degree of } f(x)\).
(4.10) Every ED is a PID (and so a UFD).

PF: Let $R$ be an ED, and $I \subset R$ be an ideal. Assume that $I \neq R$. Choose $a \in I$ so that $\phi(a)$ is minimum in $\{\phi(x) : x \in I\}$. Then (ED1) and (ED2) imply that $I = (a)$. 


5. Rings of Quotients and Localization

Question in mind: Observe and study how to obtain fractions from integers, and consider the more general question: How to obtain a smallest field from an integral domain?

(5.1) A nonempty subset $S$ in a ring $R$ is multiplicative if $\forall a, b \in S$, we have $ab \in S$. Important Reminder: Throughout this section, we always assume that $S$ is a multiplicative set in a commutative ring $R$. (This assumption may not be repeated.)

(5.1a) (Fact and Example) If $P$ is a prime ideal in a commutative ring $R$, then $R - P$ is a multiplicative set. (Definition)

(5.2) (Thm 4.2) The relation on $R \times S$ by

\[(r, s) \sim (r', s') \iff s_1(rs' - r's) = 0, \text{ for some } s_1 \in S\]

is an equivalence relation. Furthermore, if $0 \not\in S$ and $R$ has no zero divisors, then the following is also an equivalence relation:

\[(r, s) \sim (r', s') \iff (rs' - r's) = 0.\]

(5.3) Definition of rings of quotients We use the notations in (5.2). Denote the equivalence class that contains $(r, s)$ by $r/s$, and the set of all equivalence classes by $S^{-1}R$. Then

(i) $r/s = r'/s' \iff s_1(rs' - r's) = 0$, for some $s_1 \in S$.

(ii) $tr/ts = r/s, \forall r \in R$ and $t, s \in S$.

(iii) If $0 \in S$, then $S^{-1}R$ has only one member.

When $S \neq \emptyset$, $S^{-1}R$ is called the complete ring of quotients or the full ring of quotients of $R$.

(5.4) (Thm 4.3) (Continuation of (5.3)) Each of the following holds.

(i) $S^{-1}R$ is a commutative ring with identity (called the ring of quotients), where addition and multiplications are

\[r/s + r'/s' = (rs' + r's)/ss' \text{ and } (r/s)(r'/s') = (rr')/(ss').\]

(ii) If $R \not\in \{0\}$ has no zero divisor, and if $0 \not\in S$, then $S^{-1}R$ is an integral domain.

(iii) If $R \not\in \{0\}$ has no zero divisor, and if $S = R - \{0\}$, then $S^{-1}R$ is a field
(quotient field).

PF: (i) Only need to verify that the definitions are well-defined. Note that $s/s$ will be the multiplicative identity.
(ii)/(iii) Only need to show that $S^{-1}R$ has no zero divisors/(every non zero has an inverse: $(r/s)(s/r) = 1$).

(5.5) (Thm 4.4) (extending the embedding map from $\mathbb{Z}$ to $\mathbb{Q}$)

(i) The map $\phi_S : R \mapsto S^{-1}R$ by $r \mapsto rs/s$ for some $s \in S$ is a well-defined ring homomorphism, such that $\forall s \in S, \phi_S(s)$ is a unit in $S^{-1}R$.
(ii) If $0 \notin S$, and $S$ contains no zero devisors, then $\phi_S$ is a monomorphism. (Thus any integral domain can be embedded in its quotient ring.)
(iii) If $R$ has an identity, and $S$ consists of units, then $\phi_S$ is an isomorphism. (Thus the full ring of quotients of a field $F$ is isomorphic to $F$ itself).

PF: Verify each by definitions.

(5.6) (Thm 4.7) (What happen if the process above is applied to an ideal?)

(i) If $I$ is an ideal in $R$, then $S^{-1}I = \{a/s : a \in I, s \in S\}$ is an ideal in $S^{-1}R$.
(ii) If $J$ is another ideal in $R$, then

$S^{-1}(I + J) = S^{-1}I + S^{-1}J, S^{-1}(IJ) = (S^{-1}I)(S^{-1}J), S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$.

(iii) If $I'$ is an ideal of $S^{-1}R$, then $\phi_S^{-1}(I')$ is an ideal in $R$, (called the contraction of $I'$ in $R$.)

PF: (iii) is old. Note that

$$\sum_{i=1}^{n}(c_i/s) = \left(\sum_{i=1}^{n}c_i\right)/s, \sum_{i=1}^{n}(a_i/b_i/s) = \sum_{i=1}^{n}(a_i/s)(b_i/s), \sum_{i=1}^{n}(c_i/s_i) = \left(\sum_{i=1}^{n}c_i \prod_{k=1}^{n}s_k\right)/\prod_{k=1}^{n}s_k.$$

(5.7) Suppose that $R$ has an identity, and $I$ is an ideal of $R$. Then $S^{-1}I = S^{-1}R \iff S \cap I \neq \emptyset$.

PF: $s \in S \cap I \implies s/s \in S^{-1}I \implies S^{-1}I = S^{-1}R \implies \phi_S^{-1}(S^{-1}I) = R \implies$ for some $a \in I$, $s/s = \phi_S(1_R) = a/s \implies$ for some $s_1 \in S, s^2s_1 = ass_1 \in S \cap I.$
(5.8) (Lemma 4.9) Suppose that $R$ has an identity, and $I$ is an ideal of $R$.

(i) $I \subseteq \phi_{S}^{-1}(S^{-1}I)$.

(ii) If $I = \phi_{S}^{-1}(J)$ for some ideal $J$ in $S^{-1}R$, then $S^{-1}I = J$.

(iii) If $P$ is a prime ideal in $R$ and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal in $S^{-1}R$ and $\phi_{S}^{-1}(S^{-1}P) = P$.

PF: (i) $a \in I \implies \phi_{S}(a) = (as)/s \in S^{-1}I \implies a \in \phi_{S}^{-1}(S^{-1}I)$.

(ii) $I = \phi_{S}^{-1}(J) \implies S^{-1}I = \{r/s : \phi_{S}(r) \in J, s \in S\} \implies r/s = (1/s)(rs/s) \in (1/s)J = J \implies S^{-1}I \subseteq J$. Conversely, $r/s \in J \implies \phi_{S}(r) = rs/s = (s^2/s)(r/s) \in J \implies r \in \phi_{S}^{-1}(J) = I \implies r/s \in S^{-1}I$.

(iii) By (5.7), $P \cap S = \emptyset \implies S^{-1}P \neq S^{-1}R$. Assume $(r/s)(r'/s') = rr'/(ss') = a/t \in S^{-1}P, a \in P$ and $t \in S, \implies s_1trr'/ = s_1ss'a$ for some $s_1 \in S, \implies rr' \in P$ (as $s_1t \in S$ and $S \cap P = \emptyset$), and so $r/s$ or $r'/s' \in S^{-1}P$.

It remains to show $\phi_{S}^{-1}(S^{-1}P) \subseteq P$ (by (i)). $r \in \phi_{S}^{-1}(S^{-1}P) \implies \phi_{S}(r) = a/t \in S^{-1}P, a \in P$ and $t \in S, \implies s_1str = s_1sa \in P$, for some $s_1 \in S, r \in P$ (as $s_1t \in S$ and $S \cap P = \emptyset$).

(5.9) (Thm 4.10) Suppose $R$ has identity. Then there is a one-to-one correspondence between the set $\mathcal{U}$ of prime ideals of $R$ which are disjoint from $S$, and the set $\mathcal{V}$ of prime ideals of $S^{-1}R$, given by $P \mapsto S^{-1}P$.

PF: By (5.8)(iii), only need to show the map $P \mapsto S^{-1}P$ is onto. If $J$ is a prime ideal in $S^{-1}R$, then let $P = \phi_{S}^{-1}(J)$, and then (5.8)(ii) says $\phi_{S}^{-1}(P) = J$. (Show that $P$ is prime). $\forall a, b \in R$ with $ab \in P, \phi_{S}(a)\phi_{S}(b) \in J \implies \phi_{S}(a) \in J$ or $\phi_{S}(b) \in J \implies a$ or $b \in \phi_{S}^{-1}(J) = P$.

(5.10) Let $P$ be a prime ideal in a commutative ring $R$, and let $S = R - P$. Then $S^{-1}P$ is called the localization of $R$ at $P$.

Let $R$ be a commutative ring with identity. If $R$ has a unique maximal ideal, then $R$ is called a local ring.

(5.11) (Thm 4.13) Let $R$ be a commutative ring with identity. TFAE:

(i) $R$ is a local ring.
(ii) \( R - U(R) \) is contained in an idea \( M \neq R \).

(iii) \( R - U(R) \) is an ideal in \( R \).
6. Rings of Polynomials and Factorizations

Questions in mind: How do the roots of a polynomial distributed? When does the division algorithm hold? When a polynomial ring is a UFD?

(6.1) (Thm 5.1) Let $R$ be a ring and let

$$R[x] = \{(a_0, a_1, a_2, \ldots) : a_i \in R, \text{ and } a_j = 0 \text{ for all but finitely many } j \text{'s} \},$$

denote the set of all sequences of elements of $R$ such that $a_i = 0$ for all but finitely many $a_i$’s.

(i) $R[x]$ is a ring with

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$

and

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots),$$

where

$$c_n = \sum_{i=0}^{n} a_{n-i}b_i = \sum_{k+j=n} a_kb_j.$$

(ii) If $R$ is commutative (resp. with identity, without zero divisors), then so is $R[x]$.

(iii) (embedding $R$ into $R[x]$) The map $R \mapsto R[x]$ by $r \mapsto (r, 0, 0, \ldots)$ is an monomorphism.

**Note** One can identify $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ with $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ in the traditional way, by introducing the indeterminate $x$. We shall make no distinction between these two notations. But this can be formally done as in (6.2) below. $R[x]$ is the ring of polynomials, and $a_0, a_1, \ldots$ are coefficients of $f$, $a_0$ is the constant term; and $a_n$, then largest nonzero $a_i$ in the sequence, is the leading coefficient; $f = a_0$ is a constant polynomial. When $R$ has $1_R$, and when $a_n = 1$, then $f = a_0 + x^n$ is a monic polynomial.

In addition to the ring operations, we define the scalar multiplication between $r \in R$ and $(a_0, a_1, a_2, \ldots) \in R[x]$ as

$$r(a_0, a_1, a_2, \ldots) = (ra_0, ra_1, ra_2, \ldots) \text{ and } (a_0, a_1, a_2, \ldots)r = (a_0r, a_1r, a_2r, \ldots).$$
(6.2) (Thm 5.2) Let $R$ be a ring with identity $1_R = 1$. Denote $x = (0, 1, 0, ...)$.

(ii) $x^n = (0, 0, ..., 0, 1, 0, ...)$, where $1$ is the $(n + 1)$th coordinate.

(iii) $\forall r \in R$, $rx^n = x^n r$.

Note This unique $n$ is the degree of $f$, denoted by $\text{deg}(f)$. For convenience, we define $\text{deg}(0) = -\infty$.

(6.3) (Thm 6.1) Let $R$ be a ring and $f, g \in R[x]$.

(i) $\text{deg}(f + g) \leq \max\{\text{deg}(f), \text{deg}(g)\}$.

(ii) $\text{deg}(fg) \leq \text{deg}(f) + \text{deg}(g)$.

(iii) If $R$ has no zero divisor, then $\text{deg}(fg) = \text{deg}(f) + \text{deg}(g)$.

(6.4) (Thm 6.2) Let $R$ be a ring with identity and $f, g \in R[x] - \{0\}$ such that the leading coefficient of $g$ is in $U(R)$. There exist unique $q, r \in R[x]$ such that

$f = qg + r$ and $\text{deg}(r) < \text{deg}(g)$.

PF: $g(x) = b_m x^m + ...$ and $b_m \in U(R)$. Compare the degrees to prove the uniqueness.

(6.5) (Evaluation Homomorphism and The Remainder Theorem) Let $R$ be a ring, $r \in R$, and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Define $f(r) = a_0 + a_1 r + \cdots + a_n r^n$.

(i) The map $f(x) \mapsto f(r)$ is a homomorphism $R[x] \mapsto R$.

(ii) Suppose $R$ has 1. For any $c \in R$, there exists a unique $q(x) \in R[x]$ such that

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

18
(iii) If \( f(c) = 0 \), then \((x-c)|f(x)\). Moreover, if \( R \) is commutative, then that \((x-c)|f(x)\) implies \( f(c) = 0 \). (An element \( c \in R \) is a root of \( f(x) \) if \( f(c) = 0 \)).

(iv) If \( F \) is a field, then \( F[x] \) is an ED.

(6.6) (Thm 6.7) Let \( D, E \) be integral domains such that \( D \subseteq E \). If \( f(x) \in D[x] \) has degree \( n \), then \( f(x) \) has at most \( n \) distinct roots in \( E \).

PF: Induction on \( n \). No zero divisor is needed.

(6.7) Let \( F \) be a field, and let \( G \) be a finite multiplicative subgroup of the multiplicative group \( F^* = U(F) = F - \{0\} \). Then \( G \) is cyclic. In particular, if \( |F| \) is finite, then every subgroup of \( F^* \) is cyclic.

PF: (Apply The Fundamental Theorem of Finitely Generalized Abelian Groups)

(6.8) Suppose that \( R \) is a UFD.

(i) Every irreducible is also a prime.

(ii) Assume further that \( c, d \in R \) are relatively prime (that is, any common divisor of \( c \) and \( d \) must be a unit). If for some \( a \in R \), \( c|ad \), then \( c|a \).

PF (i): Suppose \( p|ab \) and \( p \) is an irreducible. Then \( ab = qc \) for some \( c \in R \). Factor both sides into products of irreducibles

\[
(a_1a_2\cdots)(b_1b_2\cdots) = p(c_1c_2\cdots).
\]

By uniqueness of factorization, as may assume \( a_1 = up \) for some \( u \in U(R) \)

PF (ii): Factor \( ba = cd \) into products of irreducibles.

(6.9) Let \( R \) be a UFD with a quotient field \( F \) (that is, \( (R - \{0\})^{-1}R = F \)). If \( f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x] \), and if \( u = c/d \in F \) is a root of \( f(x) \) such that \( c \) and \( d \), then \( c|a_0 \) and \( d|a_n \).

PF: \( f(c/d) = 0 \iff \)

\[
a_0d^n = -c \left( \sum_{i=1}^{n} a_ic^{i-1}d^{n-i} \right) \quad \text{and} \quad a_nc^n = - \left( \sum_{i=1}^{n} a_ic^{i}d^{n-i} \right) d
\]
Let $R$ be a UFD. $\forall f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, a greatest common divisor of $a_0, a_1, ..., a_n$ is called a content of $f(x)$, and is denoted by $C(f)$. (Note that $C(f)$ is not clearly defined, can be viewed as an equivalence class with $a = b$ iff $a$ and $b$ are associates in $R$). $f$ is primitive if $C(f) \in U(R)$.

(i) If $a \in R$ and $f \in R[x]$, then $C(af) = aC(f)$.

(ii) If $f \in R[x]$, then there exists a primitive $f_1 \in R[x]$ such that $f = C(f)f_1$.

(iii) (Gauss) If $f, g \in R[x]$ are primitive, then $fg$ is also primitive.

(iv) If $f(x), g(x) \in R[x]$, then $C(fg) = C(f)C(g)$.

(v) (uniqueness of content) If $f, g \in R[x]$ are primitive, and if $af(x) = bg(x)$, then $\exists u \in U(R)$ such that $a = ub$.

PF of (iii): Let $f = a_0 + a_1 x + \cdots + a_n x^n$, and $g = d_0 + d_1 + \cdots + b_m x^m$.

Then

$$fg = c_0 + c_1 + \cdots + c_{m+n} x^{m+n}.$$ 

Suppose that $C(fg) \notin U(R)$. Then $\exists p \in R$ is an irreducible, such that $p|C(fg)$. But $C(f) \in U(R) \implies \exists$ a smallest index $s$ such that 

$$p|a_i \text{ for } i < s \text{ and } p \not| a_s.$$ 

Similarly, $\exists$ a smallest index $t$ such that 

$$p|b_j \text{ for } j < t \text{ and } p \not| b_t.$$ 

It follows from 

$$p|c_{s+t} = a_0 b_{s+t} + a_1 b_{s+t-1} + \cdots + a_s b_t + \cdots + a_{s+t} b_0$$

that $p|a_s b_t$. Apply (6.8)(i).

PF of (iv): Write $f = C(f)f_1$ and $g = C(g)g_1$. Then $fg = C(f)C(g)f_1g_1$.

PF of (v): Let $p|a$ be an irreducible (and prime). Then $p|bg(x) \implies p|b$.

(6.11) Let $R$ be a UFD with quotient field $F$. Let $f, g \in R[x]$ be primitive. Then $f$ and $g$ are associates in $R[x]$ iff they are associates in $F[x]$. 

20
such that \( u \in U(F[x]) = F^* \) such that \( f = ug \iff \exists b \in R, c \in R - \{0\} \) such that \( u = b/c, cf = bg \iff \) (as \( C(f), C(g) \in U(R) \), and by (6.10(i)) \( b = cv \) for some \( v \in U(R) \iff f = vg \) for some \( v \in U(R) \).

(6.12) Let \( R \) be a UFD with quotient field \( F \). Let \( f \in R[x] \) with \( \text{deg}(f) > 0 \).
(i) If \( f \) is irreducible in \( R[x] \), then \( f \) is irreducible in \( F[x] \).
(ii) If \( f \) is primitive, then \( f \) is irreducible in \( R[x] \) iff \( f \) is irreducible in \( F[x] \).

PF(ONLY IF): Let \( f = gh \) in \( F[x] \) with \( \text{deg}(g) > 1 \) and \( \text{deg}(h) > 1 \). Then \( \exists d \in R \), and \( g_1, h_1 \in R[x] \) such that
\[
df(x) = g_1(x)h_1(x),
\]
and such that \( \text{deg}(g_1) = \text{deg}(g) \) and \( \text{deg}(h_1) = \text{deg}(h) \). Also, there exist primitive \( f_2, g_2, h_2 \in R[x] \) such that \( f(x) = C(f)f_2, g_1 = C(g_1)g_2 \) and \( h_1 = C(h_1)h_2 \). It follows that
\[
df(x) = C(g_1)C(h_1)g_2(x)h_2(x).
\]
By (6.10(v)), \( \exists u \in U(R) \) such that \( du = C(g_1)C(h_1) \). Thus
\[
df(x) = dC(f)f_2(x) = dug_2(x)h_2(x), \text{ and so } f(x) = C(f)f_2(x) = ug_2(x)h_2(x).
\]

(6.12A) If \( R \) is a UFD and \( F \) is the field of quotients of \( R \), then a nonconstant \( f(x) \in R[x] \) factors into a product of two polynomials of lower degree \( r \) and \( s \) in \( F[x] \) iff \( f(x) \) factors into a product of two polynomials of lower degree \( r \) and \( s \) in \( R[x] \).

(6.13) If \( R \) is a UFD, then \( R[x] \) is also a UFD.

PF: Let \( F \) be the field of quotients of \( R \).
(Step 1) \( F[x] \) is an ED, and so a UFD.
(Step 2) \( \forall f(x) \in R[x] - (\{0\} \cup U(R)) \), \( f(x) \) can be factored into a product of irreducibles in \( R[x] \).
If \( \text{deg}(f) = 0 \), then since \( R \) is UFD, done. Otherwise, \( f(x) = \prod p_i(x) \) in \( F[x] \) by (Step 1). But then \( f(x) = \prod q_i(x) \) in \( R[x] \) by (6.12A).
(Step 3) (uniqueness) Since \( R \) is UFD, we assume that \( f(x) \in R[x] \) has \( \text{deg}(f) > 0 \).
Assume in $F[x]$

$$f(x) = p_1(x) \cdots p_m(x).$$

Then by (6.12A), $f(x) = Cq_1(x) \cdots q_m(x)$ in $R[x]$, where $q_i$’s are irreducible and primitive in $R[x]$, and $C \in R$. But $R$ is a UFD, and so $C$ can be uniquely factored.

(6.14) (Eisenstein’s Criterion) Let $R$ be a UFD with quotient field $F$. If $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with $\deg(f) \geq 1$, and if $p$ is an irreducible in $R$ such that

$$p \not| a_n; p|a_i \text{ for } (0 \leq i \leq n - 1), \text{ and } p^2 \not| a_0.$$  

Then

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

(ii) If, in addition, $f$ is primitive in $R[x]$, then $f$ is irreducible in $R[x].$

PF: Write $f(x) = C(f)f_1(x)$, where $f_1(x)$ is primitive in $R[x]$. As $C(f) \in D \subseteq F = U(F[x])$, we only need to show that $f_1(x)$ is irreducible in $R[x]$. Assume

$$f_1(x) = g(x)h(x) \text{ in } R[x],$$

where

$$g = b_rx^r + \cdots + b_0 \in R[x], \deg(g) = r > 1; \text{ and }$$

$$h = c_sx^s + \cdots + c_0 \in R[x]$$

Then $f_1 = gh = a'_0 + a'_1x + a'_2x^2 + \cdots + a'_nx^n$, where

$$a'_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b kc_0.$$ 

Since $p \not| a_n$, $p \not| C(f)$, and so

$$p \not| a'_n; p|a'_i \text{ for } (0 \leq i \leq n - 1), \text{ and } p^2 \not| a'_0.$$  

(A) $p$ is a prime, and $p|a'_0 = b_0c_0$, we may assume $p|b_0$ and $p|c_0$ (as $p^2 \not| a'_0$).

(B) Choose smallest $k$ such that $p \not| b_k$. Then $1 \leq k \leq r < n$. But then, $p|a'_k \Rightarrow p|b_0c_0$.

(6.14A) Example: $f(x) = x^4 + 3x + 3$ is irreducible in $\mathbb{Z}[x]$. 

22
Example: Let \( f(x) = x^4 + 4kx + 1 \in \mathbb{Z}[x] \). Let \( y = x - 1 \). Then

\[
g(y) = f(y + 1) = y^4 + 4y^3 + 6y^2 + (4k + 4)y + 4k + 2.
\]

Pick \( p = 2 \) and ask Eisenstein.