CHAPTER I

Rings

1.1 Definitions and Examples

Definition 1.1.1. *A **ring** R is a set with two binary operations, addition $+$ and multiplication $\cdot$ satisfying the following conditions for all a, b, c in R :*

(i) *R is an abelian group under addition.*

(ii) *R is a semigroup under multiplication (ie. $a(bc) = (ab)c$)*

(iii) *$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

Definition 1.1.2. *A ring R is **commutative** if $ab = ba$ for all $a, b \in R$. A **ring** R **with identity** is a ring R with an element denoted $1 \neq 0$ satisfying $a \cdot 1 = a = 1 \cdot a$ for all $a \in R \setminus \{0\}$.*

Example 1.1.3.

(i) $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{Z}$ are commutative rings with identity under usual additions and multiplications.

(ii) The integers modulo $n, \mathbb{Z}_n$, is a commutative rings with identity under addition and multiplication modulo n.

(iii) For a ring R, $M_n(R)$, the set of $n \times n$ matrices whose entries are in R, is a noncommutative ring under matrices addition and multiplication.

(iv) Let $\mathcal{F}(\mathbb{R})$ be the set of all functions from $\mathbb{R}$ into $\mathbb{R}$ equipped with the operations of pointwise addition and pointwise multiplication :

For each $f, g \in \mathcal{F}(\mathbb{R}), f+g : \mathbb{R} \to \mathbb{R}$ and $fg : \mathbb{R} \to \mathbb{R}$ are defined by

$$(f+g)(x) = f(x) + g(x) \qquad \text{for all } x \in R, \text{and}$$

$$fg(x) = f(x)g(x) \qquad \text{for all } x \in R.$$

Then $\mathcal{F}(\mathbb{R})$ is a commutative ring with identity I defined by $I(x) = 1$ for all $x \in \mathbb{R}$

(v) Let $H = \{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{R}\}$. Then H is a ring, called the **quaternion ring** where addition is defined componentwise by

$$(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = (a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k$$

and multiplication is defined by expanding

$$(a_1 + b_1i + c_1j + d_1k)(a_2 + b_2i + c_2j + d_2k)$$

using the distributive law and simplifying using the relations

$$i^2 = j^2 = k^2 = -1,$$

and

$$ij = -ji = k, jk = -kj = i, ki = -ik = j$$

It can be show that each nonzero element $a + bi + cj + dk \in H$ is invertible where

$$(a + bi + cj + dk)^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

Remark. Let a be an element of a ring R. An additive inverse of a is denoted $-a$ and $a + (-b)$ is denoted $a - b$. A multiplicative inverse of a (if exists) is denoted a^{-1}.

1.2 Properties of Rings

The following expression follow from the fact that R is an abelian group under addition : For each $a, b \in R$ and $m, n \in \mathbb{Z}$

(i) $0a = 0$, $1a = 1$and $(-1)a = -a$. (Here $0, 1$ and -1 are integers)

(ii) $(m + n)a = ma + na$

(iii) $n(a + b) = na + nb$

(iv) $m(na) = (mn)a$.

Theorem 1.2.1. *Let a, b and c be elements of a ring R. Then*

(i) $a \cdot 0 = 0 = 0 \cdot a$

(ii) $a(-b) = -(ab) = (-a)b$. *In particular,* $a(-a) = -a^2 = (-a)a$.

(iii) $(-a)(-b) = ab$

(iv) $a(b - c) = ab - ac$ *and* $(b - c)a = ba - ca$

(v) $(ma)(nb) = mn(ab)$ *for all* $m, n \in \mathbb{Z}$.

If, in addition, R has an identity 1, then

(v) $(-1)a = -a$

(vi) $(-1)(-1) = 1$.

Definition 1.2.2. *A subset S of a ring R is a* ***subring*** *of R if S is a ring with the operations of R.*

Theorem 1.2.3. *Let S be a nonempty subset of a ring R. Then S is a subring of R iff $a - b$ and ab are in S for all a, b in S.*

Example 1.2.4.

(i) For each positive integer n, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(ii) $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$, called the **rings of Gaussian integers**.

1.3 Integral Domains and Fields

Definition 1.3.1. *Let R be a ring. $x \in R \setminus \{0\}$ is called a* ***left (right) zero-divisor*** *if there is $y \in R \setminus \{0\}$ such that $xy = 0\,(yx = 0)$. x is called a* ***zero-divisor*** *if x is a left or right zero-divisor.*

Remark. Every subring of an integral domain (entire ring) is an integral domain (entire ring).

Definition 1.3.2. *A ring with identity is an* ***entire ring*** *if it has no zero-divisor. A commutative entire ring is called an* ***integral domain*** *(equiv. $ab = 0 \Leftrightarrow a = 0$ or $b = 0$)*

Example 1.3.3.

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.

(ii) $\mathbb{Z}[i]$ is an integral domain.

Theorem 1.3.4. *Let D be an integral domain and $a, b, c \in D$. If $ab = ac$ and $a \neq 0$, then $b = c$.*

Definition 1.3.5. *Let x and y be elements of a commutative ring R with 1. x is said to be a* ***divisor*** *y (or x* ***divides*** *y), denoted $x|y$ if there is $q \in R$ with $y = xq$. In this case y is said to be a* ***multiple*** *of x.*

Proposition 1.3.6. *Let R be a commutative ring with 1 and $x, y, z \in R$.*

(i) *If $x|y$ and $y|z$, then $x|z$.*

(ii) *If $x|y$ and $x|z$, then $x|my + nz$ for all m, n in R.*

Definition 1.3.7. *Let R be a ring with 1. An element u in R is called an* ***unit*** *if there exists $v \in R$ such that $uv = 1 = vu$. v is then called the* ***inverse*** *of u, denoted u^{-1}.*

Remark. If R is a commutative ring with 1, then u is a unit if and only if $u|1$.

Theorem 1.3.8. *Let x and y be nonzero elements of an integral domain D. Then $x|y$ and $y|x$ if and only if $x = uy$ for some unit u in D.*

Theorem 1.3.9. *Let R be a commutative ring with 1. Then the set of all units of R, denoted $\mathcal{U}(R)$, forms a group under multiplication of R. It is called the* ***group of units*** *of R.*

Definition 1.3.10. *A ring with 1 is called a* ***division ring*** *if every nonzero element is a unit. A commutative division ring is called a* ***field****.*

Remark. Every field is an integral domain.

Theorem 1.3.11. *A finite integral domain is a field.*

Theorem 1.3.12. *$\mathbb{Z}_p$ is a field if and only if p is a prime.*

1.4 Characteristic of a Ring

Definition 1.4.1. *Let R be a ring. If there is a positive integer n such that $nx = 0$ for all $x \in R$, then the smallest such integer is called the* ***characteristic*** *of R. if no such positive integer exists, we say that R has characteristic 0. The characteristic of R is denoted char R.*

Example 1.4.2.

1. $\text{char}(\mathbb{Z}) = 0$
2. $\text{char}(\mathbb{Z}_n) = n$.

Theorem 1.4.3. *Let R be a ring with 1. Then*

(i) *Let $k \in \mathbb{N}$. Then $kR = 0$ if and only if $k1 = 0$.*

(ii) *If 1 has order n under addition, then char $R = n$.*

If 1 has infinite order addition, then char $R = 0$

(iii) *If char $R = n > 0$, then $kR = 0$ if and only if n divides k.*

(iv) *If char $R = 0$, then $kR = 0$ if and only if $k = 0$.*

Theorem 1.4.4. *The characteristic of an integral domain is 0 or prime.*

1.5 Ideals and Quotient Ring

Definition 1.5.1. *Let I be a subring of R. I is called a **left ideal** of R if $RI \subseteq I$ (ie. $ra \in I \ \forall r \in R, a \in I$), a **right ideal** of R if $IR \subseteq I$, an **(two sided) ideal** if $RI \subseteq I$ and $IR \subseteq I$.*

Definition 1.5.2. *Let X be a nonempty subset of a ring R. The smallest ideal of R containing X, denoted $\langle X \rangle$, is called the **ideal of** R **generated by** X.*

Theorem 1.5.3. *A nonempty set I of a ring R is an ideal if and only if*

(i) $a - b \in I$ for all $a, b \in I$, and

(ii) ra and $ar \in I$ for all $r \in R, a \in I$.

Theorem 1.5.4. *Let A be a subring of a ring R. The set $R/A = \{r + A \mid r \in R\}$ is a ring under the operations*

$$(r_1 + A) + (r_2 + A) = (r_1 + r_2) + A, \text{ and}$$

$$(r_1 + A) \cdot (r_2 + A) = r_1 r_2 + A$$

if and only if A is an ideal of R.

Definition 1.5.5. *Let I be an ideal of a ring R. The ring R/I in Theorem 1.5.4 is called the **quotient ring** (or **factor ring** of R by I).*

Remark. The quotient ring R/I is commutative if R is commutative. If R has the identity 1, then the identity of R/I is $1 + I$.

Definition 1.5.6. *Let P be an ideal of a commutative ring R with 1. P is called a **prime ideal** if $P \neq R$ and P has the property : If $ab \in P$, then $a \in P$ or $b \in P$.*

Theorem 1.5.7. *Let R be a commutative ring with 1 and $P \neq R$ be an ideal of R. Then P is a prime ideal if and only if R/P is an integral domain.*

Definition 1.5.8. *An ideal M in a ring R ia called a **maximal ideal** of R if $M \neq R$ and there is no ideal which lies between M and R (ie. If I is an ideal of R and $M \subseteq I \subseteq R$, then $I = M$ or $I = R$).*

Theorem 1.5.9. *Let I be an ideal of a ring R. Then $\mathcal{J}$ is an ideal of R/I if and only if $\mathcal{J} = J/I$ for some ideal J of R with $J \supseteq I$.*

Theorem 1.5.10. *Let $I \neq R$ be an ideal of R. Then I is maximal in R if and only if I and R/I are the only ideals in R/I.*

Theorem 1.5.11. *Let R be a commutative ring with 1. Then R is a field if and only if $\{0\}$ and R are the only ideal of R.*

Theorem 1.5.12. *Let $M \neq R$ be an ideal of a commutative ring with 1. Then M is a maximal if and only if R/M is a field.*

Corollary 1.5.13. *Every maximal ideal of a commutative ring with 1 is a prime ideal.*

1.6 Fields of Fractions

Each rational number can be represented as a fraction of two integers in many different ways, under the rule

$$\frac{a}{b} = \frac{c}{d} \quad \text{if and only if} \quad ad = bc.$$

The fraction $\frac{a}{b}$ in a representative of the equivalence class containing the ordered pair (a, b) of integers under the equivalence relation $\sim$ defined on $\mathbb{Z} \times \mathbb{Z}^*$ by

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad ad = bc.$$

The set of the rational numbers $\mathbb{Q}$ is a field under the addition and multiplication defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bc}, \text{ and}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Any nonzero integer m, identified with the class $\frac{m}{1}$, now has an inverse under multiplication $\frac{1}{m}$ in $\mathbb{Q}$. In this way the integral domain $\mathbb{Z}$ can be considered as a subring of $\mathbb{Q}$. Moreover $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$ in the sense that any field containing an isomorphic copy of Z in which all nonzero integers are units must contain an isomorphic copy of $\mathbb{Q}$.

The next theorem gives a generalization for the idea of the smallest field containing an integral domain.

Theorem 1.6.1. *Let R be an integral domain. Define a relation $\sim$ on $S = R \times (R \setminus \{0\})$ by*

$$(r_1, s_1) \sim (r_2, s_2) \Longleftrightarrow r_1 s_2 = r_2 s_1.$$

Then

(i) *$\sim$ is an equivalence relation on S.*

(ii) *$Q(R) = S/\sim$ is a field under the following addition and multiplication :*

$$[(r_1, s_1)] + [(r_2, s_2)] = [(r_1 s_2 + r_2 s_1, s_1 s_2)],$$

$$[(r_1, s_1)] \cdot [(r_2, s_2)] = [(r_1 r_2, s_1 s_2)].$$

(iii) $Q(R)$ *is the smallest field containing* R *in the sense that any field containing an isomorphic copy of* R *in which all nonzero elements of* R *are units must contain an isomorphic copy of* $Q(R)$.

Definition 1.6.2. *The field in Theorem* 1.6.1 *is called the* ***field of fractions*** *or* ***quotient field*** *of* R. *The equivalence class containing* $(r, s), [(r, s)]$ *will be denoted by* $\frac{r}{s}$.

CHAPTER II

Ring Isomorphism Theorems

2.1 Ring and Homomorphisms

Definition 2.1.1. *Let R and S be rings. A mapping $f : R \to S$ is called a* ***ring homomorphism*** *if*

$$f(x+y) = f(x) + f(y), \text{ and}$$

$$f(xy) = f(x)f(y) \quad \text{for all } x, y \in R.$$

The ***kernel*** *of f, denoted* $\ker f$ *is the set*

$$\ker f = \{x \in R \mid f(x) = 0\}.$$

Theorem 2.1.2. *Let $f : R \to S$ be a ring homomorphism. Then*

(i) $f(0) = 0$.

(ii) $f(kr) = kf(r)$ *for all* $r \in R$, $k \in \mathbb{Z}$.

(iii) $f(r^n) = (f(r))^n$ *for all* $r \in R, n \in \mathbb{N}$.

(iv) *If* $u \in \mathcal{U}(R)$, *then* $f(u^k) = (f(u))^k$ *for all* $k \in \mathbb{Z}$.

(v) *If T is a subring of R, then $f[T]$ is a subring of S. In particular, Im f is a subring of S.*

(vi) *If S' is a subring of S, then $f^{-1}[S']$ is a subring of R. In particular,* $\ker f$ *is a subring of R.*

Theorem 2.1.3. *Let $f : R \to S$ be a ring homomorphism. Then f is an injection if and only if* $\ker f = \{0\}$.

Definition 2.1.4. *A ring homomorphism $f : R \to S$ is called a* ***ring isomorphism*** *if f is a bijection. In this case R and S is said to be* ***isomorphic****, denoted $R \cong S$.*

Theorem 2.1.5. *(The First Isomorphism Theorem.)*

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

(i) $\ker f$ *is an ideal of R, and*

(ii) $R/_{\ker f} \cong Imf$.

Theorem 2.1.6. *(The Second Isomorphism Theorem.)*

Let S be a subring of R and I be an ideal of R. Then

(i) $S + I$ *is a subring of R*

(ii) $S \cap I$ *is an ideal of S, and*

(iii) $S + I/_I \cong S/_{S \cap I}$

Theorem 2.1.7. *(The Third Isomorphism Theorem.)*

Let I and A be ideals of R and $I \subseteq A$. Then $A/_I$ is an ideal of $R/_I$ and $R/_A \cong (R/_I)/(A/_I)$.

Theorem 2.1.8. *Let R be a ring with 1. Then mapping $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n1$ for all $n \in \mathbb{Z}$ is a ring homomorphism. Moreover, $\mathbb{Z}/_{ker\phi} \cong S$ where S is the subring of R generated by 1.*

Corollary 2.1.9. *Let R be a ring with 1.*

(i) *If char $R = n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$.*

(ii) *If char $R = 0$, then R contains a subring isomorphic to $\mathbb{Z}$.*

Corollary 2.1.10. *Let F be a field.*

(i) *If char $F = p$, then F contains a subfield isomorphic to $\mathbb{Z}_p$.*

(ii) *If char $F = 0$, then F contains a subfield isomorphic to $\mathbb{Q}$.*

CHAPTER III

Factorization in Integral Domains

3.1 Divisibility

Throughout this chapter D denote an integral domain.

Definition 3.1.1. *Let D be an integral domain and $x, y \in D$. We say that x **divides** y, denoted $x|y$ if $y = xq$ for some $q \in D$.*

Theorem 3.1.2. *Let a, b be elements of an integral domain D. Then TFAE :*

(i) *$a|b$ and $b|a$*

(ii) *$a = ub$ for some unit u in D*

(iii) *$Ra = Rb$.*

Definition 3.1.3. *Let $a, b \in D$. a and b are said to be **associated**, denoted $a \sim b$ if $a = ub$ for some unit u in D.*

Theorem 3.1.4. *$\sim$ is an equivalence relation on D and the equivalence class of a in D is*

$$[a] = \{ua \mid u \text{ is a unit in } D\}.$$

Definition 3.1.5. *Let D be an integral domain and $a, b \in D$. A **greatest common divisor** of a and b is an element d which satisfies:*

(i) *$d|a$ and $d|b$, and*

(ii) *if $d_1|a$ and $d_1|b$, then $d_1|d$.*

*A **least common multiple** of a and b is an element m which satisfies:*

(i) $a|m$ *and* $b|m$, *and*

(ii) *if* $a|m_1$ *and* $b|m_1$, *then* $m|m_1$.

Theorem 3.1.6. *Let* D *be an integral domain and* $a, b \in D$.

(i) *If* d *and* d_1 *are* gcd*'s of* a *and* b, *then* d *and* d_1 *are associated.*

(ii) *If* m *and* m_1 *are* lcm*'s of* a *and* b, *then* m *and* m_1 *are associated.*

Theorem 3.1.7. *Let* D *be an integral domain. If* $Ra + Rb = Rc$, *then* $c = \gcd(a, b)$.

Definition 3.1.8. *An element* p *in* D *is called a* ***prime*** *in* D *if*

(i) $p \neq 0$ *and* p *is not a unit.*

(ii) *if* $p|ab$, *then* $p|a$ *or* $p|b$.

Definition 3.1.9. *An element* a *in* D *is said to be* ***irreducible*** *in* D *if*

(i) $a \neq 0$ *and* a *is not a unit.*

(ii) *If* $a = bc$, *then* b *or* c *is a unit in* R.

3.2 Unique factorization Domains

Definition 3.2.1. *A* ***Unique Factorization Domain (UFD)*** *is an integral domain* D *in which every nonzero nonunit element* $a \in D$ *has the following factorization properties:*

(i) a *is a (finite) product of irreducible elements of* D, *and*

(ii) *the decomposition of (i) is unique up to associates, namely if* $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$ *where* p_i, q_j *are irreducible, then* $m = n$ *and there is a reordering* $q_{j_1}, \dots q_{j_m}$ *of* $q_1, \dots q_m$ *such that* p_i *and* q_{j_i} *are associated.*

Definition 3.2.2. *Let D be an integral domain. Define an equivalence relation on the set of irreducible elements of D by*

$$a \sim b \Leftrightarrow a \text{ and } b \text{ are associated.}$$

Then a ***set of representative irreducible elements*** *of D is a set which contains exactly one irreducible element from each equivalence class.*

Theorem 3.2.3. *Let D be an integral domain and P be a set of representative irreducible elements of R. Then TFAE :*

(i) *D is a UFD.*

(ii) *Every nonzero nonunit element of R can be expressed uniquely (up to ordering) as $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where u is a unit $k \geq 0, \alpha_1 \cdots, \alpha_k > 0$ and $p_1, \ldots, p_k$ are distinct elements of P.*

CHAPTER IV

Polynomial Rings

4.1 Polynomial Rings

Definition 4.1.1. *Let R be a ring and a indeterminate $x \notin R$. The* ***polynomial ring*** *$R[x]$ consists of the set of all expression of the form :*

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \text{ with } n \geq 0 \text{ and each } a_i \in R$$

and addition and multiplication defined as follows : For $f(x) = a_0+a_1x+\ldots+a_nx^n$ and $g(x) = b_0 + b_1x + \ldots + b_mx^m$, with $a_n \neq 0, b_m \neq 0$ and $n \leq m$,

$$f(x) + g(x) = \sum_{i=0}^{m}(a_i + b_i)x^i$$

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_ib_{k-i}\right)x^k$$

An element $f(x)$ in $R[x]$ is called a ***polynomial*** *over R. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \neq 0$. a_n is called the* ***leading coefficient*** *of $f(x)$. The* ***degree*** *of $f(x)$, denoted deg $f(x)$, is defined to be n and deg 0 is $-\infty$. $f(x)$ is said to be* ***monic*** *if $a_n = 1$. $f(x)$ is a* ***non-constant polynomial*** *if deg $f(x) \geq 1$.*

Theorem 4.1.2. *Let R be a ring and $f(x), g(x) \in R[x]$. Then*

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

(ii) *deg $(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.*

Theorem 4.1.3. *Let R be an integral domain (entire ring) and $f(x), g(x) \in R[x]$. Then*

(i) *deg* $(f(x)g(x)) = deg\ f(x) + deg\ g(x)$ *for all* $f(x), g(x) \in R[x] \setminus \{0\}$.

(ii) $R[x]$ *is an integral domain (entire ring).*

(iii) $U(R[x]) = U(R)$.

Definition 4.1.4. *The polynomial ring in the variables* $x_1, x_2, \ldots, x_n$ *with coefficients in* R *is denoted by* $R[x_1, \ldots, x_n]$ *and defined inductively by* $R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

Theorem 4.1.5. (Division Algorithm). *Let* R *be a ring with 1 (not necessary commutative). Let* $f(x)$ *be a monic polynomial of degree* n *in* $R[x]$. *Then for any* $g(x) \in R[x]$, *there exist unique polynomials* $q(x)$ *and* $r(x)$ *in* $R[x]$ *satisfying*

(i) $g(x) = f(x)q(x) + r(x)$.

(ii) *deg* $r(x) < n$.

Theorem 4.1.6. *Let* R *be a commutative ring with 1,* $a \in R$ *and* $f(x) \in R[x]$. *Then*

(i) *There exists* $g(x) \in R[x]$ *such that* $f(x) = (x - a)g(x) + f(a)$.

(ii) $(x - a)|f(x)$ *if and only if* $f(a) = 0$.

Definition 4.1.7. *Let* $f(x) \in R[x]$ *and* $a \in R$. *Then* a *is called a* ***root*** *of* $f(x)$ *if* $f(a) = 0$. *The root* a *of* $f(x)$ *is said to have* ***multiplicity*** $m \geq 1$ *if* $f(x) = (x - a)^m g(x)$, *where* $g(a) \neq 0$.

Theorem 4.1.8. *Let* R *be an integral domain and* $f(x) \in R[x] \setminus \{0\}$.

(i) *If* $a_1, a_2, \ldots, a_k$ *are distinct roots of* $f(x)$, *then* $(x - a_1)(x - a_2) \cdots (x - a_k)|f(x)$.

(ii) $f(x)$ *has at most* n *root in* R *if deg* $f(x) = n$.

4.2 Factorization of Polynomials over a Field

Definition 4.2.1. *Let F be a field and $p(x) \in F[x]$. $p(x)$ is said to be* ***irreducible*** *if :*

(i) *deg $p(x) \geq 1$*

(ii) *$p(x) = f(x)g(x)$ in $F[x]$ implies deg $f(x) = 0$ or deg $g(x) = 0$*

$p(x)$ is ***reducible*** *if it is not irreducible.*

Theorem 4.2.2. *Let F be a field and $p(x) \in F[x]$.*

(i) *If $p(x)$ is irreducible and deg $p(x) \geq 2$, then $p(x)$ has no root in F.*

(ii) *If deg $p(x) = 2$ or 3, then $p(x)$ is irreducible if and only if it has no root in F.*

Theorem 4.2.3. *For a field F, $F[x]$ is a Euclidean domain.*

Theorem 4.2.4. *For a field F, $F[x]$ is a PID.*

Theorem 4.2.5. *Let F be a field and $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal if and only if $p(x)$ is irreducible.*

4.3 Factorization of Polynomials over $\mathbb{Q}$

Definition 4.3.1. *The* ***content*** *of $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x] \setminus \{0\}$ is the greatest common divisor of $a_0, a_1, ..., a_n$ If the content is 1, $f(x)$ is said to be* ***primitive****.*

Lemma 4.3.2. *If $f(x)$ and $g(x)$ are primitive polynomials in $\mathbb{Z}[x]$, then $f(x)g(x)$ is primitive.*

Theorem 4.3.3. ***(Gauss's Lemma)***

Let $f(x)$ be a primitive polynomial. If $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Q}[x]$, then $f(x) = s(x)r(x)$ for some $s(x), r(x) \in \mathbb{Z}[x]$.

Theorem 4.3.4. ***(Eisenstein Criterion)***.

Let $f(x) = a_0 + a_1x + ... + a_nx^n$ *be a polynomial in* $\mathbb{Z}[x]$. *Assume that there is a prime* p *such that* (i) $p \mid a_i$ *for all* $i, 0 \leq i < n$

(ii) $p \nmid a_n$ *and* $p^2 \nmid a_0$.

Then $f(x)$ *is irreducible over* $\mathbb{Q}[x]$.