

BASIC RING THEORY

J. K. VERMA

CONTENTS

1. DEFINITIONS AND EXAMPLES

We are familiar with the binary operations of addition and multiplication among many objects: complex numbers, square matrices with entries in a field, real or complex valued functions defined on a set, polynomials and power series with coefficients in a field, integers with modular arithmetic, etc. Ring theory deals with such objects. Groups are sets of objects with one binary operation while rings are sets of objects with two binary operations, addition and multiplication, inter related to each other by distributive laws. The theorems obtained as a result of abstract study of rings apply to these diverse objects mentioned above which can then be used to solve problems arising in number theory, geometry and many other fields.

Definition 1.1. *A nonempty set R is called a **ring**, if it has two binary operations called addition denoted by $a + b$ and multiplication denoted by ab for $a, b \in R$ satisfying the following axioms:*

- (1) $(R, +)$ is an abelian group.
- (2) Multiplication is associative, i.e. $a(bc) = (ab)c$ for all $a, b, c \in R$.
- (3) Distributive laws hold: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Definition 1.2. *Let R be a ring.*

- (1) *If multiplication in R is commutative, it is called a **commutative ring**.*
- (2) *If there is an identity for multiplication, then R is said to have identity.*

Notes for the lectures on basic ring theory in the *Advanced Training in Mathematics School for Lecturers in Algebra and Linear Algebra* at IIT Bombay, 5 June-1 July, 2006. The author thanks Manoj Keshari and Mousumi Mandal for assistance in preparing this manuscript.

- (3) A nonzero element $a \in R$ is said to have a **left (resp. right) inverse** b if $ba = 1$ (resp. $ab = 1$.) We say that a is **invertible** or a **unit** in R if it has a left and a right inverse. The set of invertible elements of R is denoted by $U(R)$.
- (4) If $1 \neq 0$ in R , and all nonzero elements are invertible, then R is called a **division ring**.
- (5) A commutative division ring is called a **field**.
- (6) An element a of a commutative ring R is called a **zerodivisor** if there is a nonzero $b \in R$ such that $ab = 0$. An element $a \in R$ that is not a zerodivisor is called a **nonzerodivisor**. If all nonzero elements of a commutative ring are nonzerodivisors, then R is called an **integral domain**.
- (7) A nonempty subset S of a ring R is called a **subring** of R if S is a ring with respect to addition and multiplication in R .

Examples of rings

Example 1.3. The set of integers \mathbb{Z} , the set of rational numbers \mathbb{Q} , the set of real numbers \mathbb{R} and the set of complex numbers \mathbb{C} are commutative rings with identity.

Example 1.4. Let n be a positive integer. Let $a, b \in \mathbb{Z}$. We write $a \equiv b \pmod{n}$ if and only if $n \mid a - b$. The equivalence class of an integer m for the equivalence relation \equiv is denoted by $[m]$. The set $\mathbb{Z}/n\mathbb{Z} = \{[m] \mid m = 0, 1, \dots, n-1\}$ is a commutative ring with identity with respect to the operations $[i] + [j] = [i + j]$ and $[i][j] = [ij]$. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

Example 1.5. Matrix rings. Let R be a ring. Let $M_n(R)$ denote the set of all $n \times n$ matrices with entries in R . Under usual addition and multiplication of matrices, $M_n(R)$ is a noncommutative ring with nonzero zerodivisors for $n \geq 2$. Indeed, let

$$A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 0 & ab \\ 0 & 0 \end{bmatrix} \text{ and } BA = 0.$$

Hence if $ab \neq 0$ then $AB \neq BA$. It is easy to verify that the scalar matrices and upper triangular matrices form subrings of $M_n(R)$.

Example 1.6. Rings of quaternions. One of the first examples of a noncommutative division ring was found by W. R. Hamilton. This is called

the ring of real quaternions $H(\mathbb{R})$. The elements of $H(\mathbb{R})$ are $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ and i, j, k satisfy the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ki.$$

We add two quaternions componentwise and multiply them using distributive laws. Similarly we may define the ring of rational or integral quaternions. Define the **norm** $N(x)$, of $x = a + bi + cj + dk$, to be $N(x) = a^2 + b^2 + c^2 + d^2$ and **conjugate** \bar{x} of x to be $a - bi - cj - dk$. Both $H(\mathbb{R})$ and $H(\mathbb{Q})$ are division rings since for a nonzero element $x = a + bi + cj + dk$, $x\bar{x} = N(x)$ is nonzero. Hence $x^{-1} = \bar{x}/N(x)$.

We can realize $H(\mathbb{R})$ as a subring of $M_2(\mathbb{C})$. It is easy to see that

$$R = \left\{ M(a, b) = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} : a, b \in \mathbb{C} \right\}$$

is a subring of $M_2(\mathbb{C})$. Let $a = x + iy$ and $b = z + iu$ where $x, y, z, u \in \mathbb{R}$. Then $\det M(a, b) = a\bar{a} + b\bar{b} = x^2 + y^2 + z^2 + u^2$. Hence $\det M(a, b) = 0$ if and only if $M(a, b) = 0$. Thus for a nonzero $M(a, b)$ we have

$$M(a, b)^{-1} \det M(a, b) = \text{adj } M(a, b) = \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} \in R.$$

Therefore if either a or b is nonzero, then $M(a, b)^{-1} \in R$. Hence $H(\mathbb{R})$ is a division ring. Write $M(a, b)$ as:

$$\begin{aligned} M(a, b) &= \begin{bmatrix} x + iy & z + iu \\ -z + iu & x - iy \end{bmatrix} \\ &= x \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + y \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + z \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + u \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}. \end{aligned}$$

Put

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Verify that $A^2 = B^2 = C^2 = -I$ and $AB = C = -BA$, $BC = A = -CB$ and $CA = B = -AC$. Hence A, B, C satisfy the same relations as i, j, k . Later we will make this precise by proving that R is isomorphic to $H(\mathbb{R})$.

Using the above decomposition of $M(a, b)$, it follows that R is a four dimensional real vector space. A division ring that is also a finite dimensional real vector space, is called a **finite dimensional division algebra**. Frobenius proved the following beautiful characterization of finite dimensional division algebras.

Theorem 1.7. [Frobenius] *Any finite dimensional division algebra is isomorphic to either \mathbb{R}, \mathbb{C} or $H(\mathbb{R})$.*

Example 1.8. Rings of functions. Let A be any set and $R = F(A, \mathbb{R})$ denote the set of all functions $f : A \rightarrow \mathbb{R}$. If $f, g \in R$, define $f + g$ and fg by the equations $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in A$. Then R is a commutative ring with identity. The identity is the constant function $I(x) = 1$ for all $x \in A$. We say that a function $f \in F(\mathbb{R}, \mathbb{R})$ has compact support if $f(x) = 0$ for all x outside a compact subset of \mathbb{R} . Functions in $F(\mathbb{R}, \mathbb{R})$ with compact support form a subring of R without identity. The set $C(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous}\}$ is a subring of the ring R .

Example 1.9. Quadratic integer rings. Let d be a square free integer. The set $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a field called the **quadratic field generated by \sqrt{d}** . The set $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{d})$. When $d \equiv 1 \pmod{4}$, then the set

$$\mathbb{Z}[(1 + \sqrt{d})/2] = \{a + b(1 + \sqrt{d})/2 \mid a, b \in \mathbb{Z}\}$$

is also a subring of $\mathbb{Q}(\sqrt{d})$. Let $\omega = \sqrt{d}$ when $d \equiv 2, 3 \pmod{4}$ and $\omega = (1 + \sqrt{d})/2$ when $d \equiv 1 \pmod{4}$. The subring $\mathbb{Z}[\omega]$ is called the **ring of integers** in the quadratic field $\mathbb{Q}(\sqrt{d})$. We will study this ring in detail later and use its structure to prove some classical theorems in number theory.

Define the **field norm** $N : \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}$ by $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d$. It is easy to show that the norm function N is multiplicative, i.e. $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Q}(\sqrt{d})$. Moreover $N(x)$ is an integer for all $x \in \mathbb{Z}[\omega]$.

Proposition 1.10. *The group of units in $\mathbb{Z}[\omega]$ is:*

$$U(\mathbb{Z}[\omega]) = \{\alpha \in \mathbb{Z}[\omega] \mid N(\alpha) = \pm 1\}.$$

Proof. Let α be a unit. Then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[\omega]$. Then $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. Hence $N(\alpha) = \pm 1$. Conversely let $N(\alpha) = \pm 1$. Let $\bar{\omega} = -\sqrt{d}$ if $d \equiv 2, 3 \pmod{4}$ and $\bar{\omega} = (1 - \sqrt{d})/2$ if $d \equiv 1 \pmod{4}$. Let $\alpha = a + b\omega$. then

$$N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 - db^2, & \text{if } d \equiv 2, 3 \pmod{4}. \\ a^2 + ab + \frac{1-d}{4}b^2, & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Hence $N(\alpha)\mathbb{Z}$ for all $\alpha \in \mathbb{Z}[\omega]$. Thus $(a + b\omega)^{-1} = \pm(a + b\bar{\omega})$. □

Remark 1.11. If $d \equiv 2, 3 \pmod{4}$, then $N(a + b\omega) = a^2 - db^2$. Hence finding the units in the quadratic integer ring is equivalent to finding integer solutions to the *Pell's equation* $x^2 - dy^2 = \pm 1$.

Example 1.12. Polynomial rings. Let R be a commutative ring with identity. Let x be an indeterminate. The formal sum $f(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_0, a_1, \dots, a_n \in R$ is called a polynomial in x with coefficients

in R . We add and multiply these polynomials in the usual way. Under these operations, the set $R[x]$ of polynomials in x with coefficients in R is a commutative ring with identity. If $f(x)$ is a nonzero polynomial and $a_n \neq 0$ then we say that $f(x)$ has degree n and we write this as $\deg(f(x)) = n$. The degree of the zero polynomial is defined to be $-\infty$. The units in $R[x]$ are the units of R . If R is an integral domain then so is $R[x]$.

Example 1.13. Formal power series rings. Let R be a commutative ring with identity. Let x be an indeterminate. The formal power series ring $R[[x]]$ is the set of formal sums $\sum_{n=0}^{\infty} a_n x^n$ where $a_n \in R$ for all n . The addition and multiplication are defined as follows:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{j+k=n} a_j b_k \right) x^n.$$

It is easy to see that the units of $R[[x]]$ are power series whose constant term is a unit.

2. IDEALS AND HOMOMORPHISMS

Definition 2.1. Let R and S be rings. A map $f : R \rightarrow S$ is called a **ring homomorphism** if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$. If f is also a bijection then it is called an **isomorphism** and we say that R and S are isomorphic rings.

It is easy to see that $f(0) = 0$ and $f(-a) = -f(a)$ for all $a \in R$. When R and S have identity, one also requires $f(1) = 1$. The set $f^{-1}(s)$ is called the **fiber of f** over $s \in S$. Note that the fiber $I = f^{-1}(0)$ is closed under addition and for all $r \in R$, and $a \in I$, we have $ra, ar \in I$.

Definition 2.2. A subset I of a ring R is called a **left ideal** if it is an additive subgroup of R and for all $r \in R$ and $a \in I$, we have $ra \in I$. Similarly I is called a **right ideal** if for all $a \in I$ and $r \in R$, $ar \in I$. An additive subgroup I of R is called an **ideal** if it is a left and right ideal.

Definition 2.3. The fiber $f^{-1}(0)$ of f over 0 is called the **kernel** of the ring homomorphism $f : R \rightarrow S$. It is denoted by $\text{Ker } f$.

Let us determine the conditions for a ring homomorphism $f : R \rightarrow S$ to be injective. Suppose that $a, b \in R$. Then $f(a) = f(b)$ if and only if $f(a - b) = 0$ if and only if $a - b \in \text{Ker} f$. Hence f is injective if and only if $\text{Ker} f = 0$.

Example 2.4. Let R be a commutative ring and x an indeterminate. Let $b \in R$ be fixed. Define the evaluation map $f : R[x] \rightarrow R$ by $f(g(x)) = g(b)$. Then f is a ring homomorphism. The kernel of f is the set of all $f(x) \in R[x]$ such that $f(b) = 0$. This is the set of all multiples of $(x - b)$ by the Remainder Theorem. In fact any $f : R[x] \rightarrow R$ which is identity on R is an evaluation map.

Example 2.5. The map $f : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ given by $f(m) = [m]$ is a ring homomorphism whose kernel is the ideal $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$.

Definition 2.6. An ideal I of a commutative ring R is called a **principal ideal** if there exists an $a \in I$ such that $I = \{ab \mid b \in R\}$. We say that I is generated by a and write this as $I = (a)$. Let $a_1, a_2, \dots, a_n \in R$. The smallest ideal I of R containing these elements is denoted by (a_1, a_2, \dots, a_n) . We say that I is generated by $\{a_1, a_2, \dots, a_n\}$.

Proposition 2.7. Every ideal of \mathbb{Z} or the polynomial ring $k[x]$ over a field k is principal.

Proof. Let I be an ideal of \mathbb{Z} . If $I = (0)$ or \mathbb{Z} then we are done. Let $(0) < I < \mathbb{Z}$. Let $n \in I$ be the smallest positive integer. We show that $I = n\mathbb{Z}$. By division algorithm, any $m \in I$ can be written as $m = nq + r$ where $q \in \mathbb{Z}$ and $r = 0$ or $0 < r < n$. If $r \neq 0$ then $r = m - nq \in I$ is a smaller positive integer than n in I . This is a contradiction. Hence $r = 0$ and consequently $I = n\mathbb{Z}$. A similar proof can be given for $k[x]$ by using division algorithm in $k[x]$. \square

Example 2.8. Let R be a commutative ring with identity. Let $n > 1$ be an integer. Consider the ring $A = M_n(R)$ of all $n \times n$ matrices with entries in R . Let J any ideal of R . Then the set $M_n(J)$ of matrices in A with entries in J is an ideal of A . In fact any ideal of A has this form. Indeed, let $E_{ij} \in A$ be the matrix whose only nonzero entry is 1 in the i^{th} row and j^{th} column. Let $B = (b_{ij}) \in A$. Then $E_{ij}B$ is the matrix whose i^{th} row is the j^{th} row of B and all other rows are zero. Similarly BE_{ij} is the matrix whose j^{th} column is the i^{th} column of B and all other columns are zero. Then $E_{pq}BE_{rs}$ is the matrix whose (p, s) entry is b_{qr} . This shows that the set of entries in the matrices in an ideal of A is an ideal of R .

Operations on ideals

For the sake of simplicity, we assume, henceforth, that the rings we consider will be commutative with identity. The following are some of the standard operations on ideals:

- (1) The **intersection** of a family $\{I_\alpha\}$ of ideals of R is an ideal and it is denoted by $\cap_\alpha I_\alpha$.
- (2) Let I and J be ideal of a ring R . The smallest ideal of R containing I and J is called the **sum of I and J** . The sum of I and J is denoted by $I + J$. It is easy to verify that $I + J = \{a + b \mid a \in I, b \in J\}$.
- (3) The **product of I and J** , denoted by IJ is the ideal generated by elements of the type ab where $a \in I$ and $b \in J$. Therefore

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_1, a_2, \dots, a_n \in I, b_1, b_2, \dots, b_n \in J\}.$$

- (4) The **radical of an ideal I** of R is defined as $\sqrt{I} = \{a \in R \mid a^n \in I, \text{ for some } n \in \mathbb{N}\}$. We say I is a **radical ideal** if it is its own radical.

Example 2.9. Let $m, n \in \mathbb{Z}$. Then $(m, n) = (d)$ where d is the greatest common divisor of m and n . The intersection $(m) \cap (n) = (l)$ where l is the least common multiple of m and n .

Example 2.10. Let k be a field and let $R = k[x_1, x_2, \dots, x_n]$ be the polynomial ring in n variables x_1, x_2, \dots, x_n . Let m_1, m_2, \dots, m_g be monomials in R and $I = (m_1, m_2, \dots, m_g)$. Then a polynomial $f \in I$ if and only if each term of f is a multiple of some m_i . Let n_1, n_2, \dots, n_h be monomials in R and $J = (n_1, n_2, \dots, n_h)$. Then

$$I \cap J = (\{LCM(m_i, n_j) \mid i = 1, 2, \dots, g, j = 1, 2, \dots, h\}).$$

3. QUOTIENT RINGS AND HOMOMORPHISM THEOREMS

Recall that integers x and y are congruent modulo n for $n \in \mathbb{N}$ if $x - y$ is divisible by n . In other words $x \equiv y \pmod{n}$ if and only if $x - y \in n\mathbb{Z}$. This can be generalized to arbitrary rings. Let I be an ideal of a ring R . We write $x \equiv y \pmod{I}$ if $x - y \in I$. The equivalence classes are $\bar{x} = x + I = \{x + a \mid a \in I\}$ for $x \in R$. Let R/I denote the set of the equivalence classes $x + I, x \in R$. Define addition and multiplication by

$$\bar{x} + \bar{y} = \overline{x + y} \text{ and } \bar{x} \bar{y} = \overline{xy}.$$

It can be proved that addition and multiplication are well-defined and R/I is a ring under these operations. Consider the map $f : R \rightarrow R/I$ defined as $f(a) = \bar{a}$. Then f is a surjective ring homomorphism. The Kernel of f is I .

Theorem 3.1 (Homomorphism Theorems). *Let $f : R \rightarrow S$ be a surjective ring homomorphism with kernel K .*

- (1) **The First Homomorphism Theorem.** The map $\bar{f} : R/K \rightarrow S$ given by $\bar{f}(\bar{r}) = f(r)$ is an isomorphism.
- (2) **The Second Homomorphism Theorem.** There is a 1-1 correspondence between the sets:

$$\{I \mid I \text{ is an ideal of } R \text{ and } K \subset I\} \leftrightarrow \{\text{ideals of } S\}$$

given by $f^{-1}(J) \leftrightarrow J$. In particular, given an ideal I of R , the ideals of R/I are of the form J/I where J is an ideal of R containing I .

- (3) **The Third Homomorphism Theorem.** Let J be an ideal of S . Then $R/f^{-1}(J) \simeq S/J$. In particular, if $I \subset K$ are ideals of R then $(R/K)/(I/K) \simeq R/I$.

Proof. (1) By the definition of addition and multiplication in R/I , \bar{f} is a homomorphism. Surjectivity of f implies that of \bar{f} . Let $\bar{f}(\bar{r}) = \bar{f}(\bar{s})$ for $r, s \in R$. Then $\bar{f}(\bar{r} - \bar{s}) = 0$. Hence $r - s \in K$. Thus $\bar{r} = \bar{s}$. Hence \bar{f} is an isomorphism.

(2) If J is an ideal of S then $f^{-1}(J)$ is an ideal of R . Since $f(x) = 0$ for all $x \in K$, $K \subset f^{-1}(J)$. If I is an ideal of R then $f(I)$ is an ideal of S . Let I_1 and I_2 be ideals of R containing K and $f(I_1) = f(I_2)$. Let $a \in I_1$, then $f(a) = f(b)$ for some $b \in I_2$. Hence $f(a - b) = 0$. Therefore $a - b \in K \subset I_2$. Hence $a \in I_2$. By symmetry $I_2 \subset I_1$. Hence $I_1 = I_2$. Let J_1 and J_2 be ideals of S . If $f^{-1}(J_1) = f^{-1}(J_2)$ then clearly $J_1 = J_2$.

(3) Let $\pi : S \rightarrow S/J$ be the map $\pi(s) = \bar{s}$. Consider the ring homomorphism $\pi \circ f : R \rightarrow S/J$. Then $\text{Ker}(\pi \circ f) = \{r \in R \mid \pi(f(r)) = 0\} = f^{-1}(J)$. By the First Homomorphism Theorem, $R/f^{-1}(J) \simeq S/J$. In particular if $S = R/I$ and $J = K/I$ for some ideal K of R , $I \subset K$ then $f^{-1}(J) = K$ where $f : R \rightarrow R/I$ is the canonical homomorphism $f(r) = \bar{r}$. Thus $R/K \simeq (R/I)/(K/I)$. \square

Example 3.2. Let p be a prime number. Consider the set

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid (a, b) = 1, p \nmid b \right\}.$$

Then $\mathbb{Z}_{(p)}$ is a ring. The subset $I = \left\{ \frac{pa}{b} \in \mathbb{Z}_{(p)} \right\}$ is an ideal of $\mathbb{Z}_{(p)}$. Let $\pi : \mathbb{Z}_{(p)} \rightarrow \mathbb{Z}_{(p)}/I$ be the canonical homomorphism $\pi\left(\frac{a}{b}\right) = \frac{a}{b} + I$. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}_{(p)}$ be the homomorphism $f(m) = \frac{m}{1}$. Then $\pi \circ f : \mathbb{Z} \rightarrow \mathbb{Z}_{(p)}/I$ is surjective and $\text{Ker } \pi \circ f = p\mathbb{Z}$. Hence $\mathbb{Z}_{(p)}/I = \mathbb{F}_p$.

Example 3.3. Consider the subring

$$S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$$

of $M_2(\mathbb{R})$. Define $f : S \rightarrow \mathbb{C}$ by $f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + bi$. Then f is an isomorphism.

Example 3.4. Let $R = \{f : [0, 1] \rightarrow \mathbb{R} \text{ is continuous}\}$. Let $c \in \mathbb{R}$ be fixed. Define $e : R \rightarrow \mathbb{R}$ by $e(f) = f(c)$. Then e is a surjective homomorphism. Moreover, $\text{Ker } e = \{f \in R \mid f(c) = 0\}$. Hence $R/\text{Ker } e \simeq \mathbb{R}$.

Example 3.5. Consider the ring $\mathbb{Z}[i]/(1+3i)$. Define $f : \mathbb{Z} \rightarrow \mathbb{Z}[i]/(1+3i)$ by $f(n) = \bar{n} = n + (1+3i)$. Since $\overline{1+3i} = \bar{0}$, we have $\overline{3i} = \overline{-1}$. Hence $\bar{i} = \bar{3}$. Thus $f(a+3b) = \bar{a} + \overline{3b} = \bar{a} + \bar{i}b = \overline{a+ib}$ for any $a, b \in \mathbb{Z}$. Hence f is onto. We claim that $\text{Ker } f = 10\mathbb{Z}$. Since $10 = (1+3i)(1-3i)$, $10\mathbb{Z} \subset \text{Ker } f$. If $n \in \text{Ker } f$ then $n = (a+bi)(1+3i)$ for some $a, b \in \mathbb{Z}$. Hence $n = (a-3b) + i(b+3a)$. Therefore $b = -3a$ and $n = 10a \in 10\mathbb{Z}$. Thus $\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/10\mathbb{Z}$. Note that $N(1+3i) = 10$.

4. INTEGRAL DOMAINS AND QUOTIENT FIELDS

We continue to assume that rings are commutative with identity. Recall that a nonzero ring is an integral domain if it has no nonzero zerodivisors.

Definition 4.1. An ideal I of a ring R is a **prime ideal** if $I \neq R$ and if $ab \in I$ for some $a, b \in R$, then either $a \in I$ or $b \in I$.

Proposition 4.2. Let I be an ideal of a ring R . Then I is a prime ideal if and only if R/I is an integral domain.

Proof. Let I be a prime ideal. Let $a, b \in R$ and $\bar{a}\bar{b} = \bar{0}$ in R/I . Then $ab \in I$. Thus either $a \in I$ or $b \in I$ which gives $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Hence R/I is an integral domain.

Conversely let R/I be an integral domain. Then $R/I \neq 0$. Hence I is a proper ideal. Let $ab \in R$ and $ab \in I$. Then $\bar{a}\bar{b} = \bar{ab} = \bar{0}$. Hence either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$ which implies either $a \in I$ or $b \in I$. Hence I is a prime ideal. \square

Example 4.3. Nonzero prime ideals of \mathbb{Z} are $p\mathbb{Z}$ where p is a prime number. Non-zero prime ideals of the polynomial ring $k[x]$, where k is a field, are $(f(x))$ where $f(x)$ is an irreducible polynomial.

Example 4.4. Let $a, b \in \mathbb{C}$. Define $\phi : \mathbb{C}[x, y] \rightarrow \mathbb{C}$ by $\phi(f(x, y)) = f(a, b)$. Then ϕ is a surjective homomorphism. If $f(x, y) \in (x-a, y-b)$ then $f(a, b) = 0$. Conversely if $f(a, b) = 0$ then by Taylor series of $f(x, y)$ near (a, b) , we see that $f(x, y) \in (x-a, y-b)$. Hence $\mathbb{C}[x, y]/(x-a, y-b) \simeq \mathbb{C}$. Since \mathbb{C} is an integral domain, $(x-a, y-b)$ is a prime ideal.

Example 4.5. Consider the ring of Gaussian integers $\mathbb{Z}[i]$. Since $2 = (1+i)(1-i)$, $2\mathbb{Z}[i]$ is not a prime ideal. But $(1+i) = (1-i)$ is a prime ideal.

To prove this, Let $f : \mathbb{Z} \rightarrow \mathbb{Z}[i]/(1+i)$ be the map $f(n) = \bar{n}$. Since $\overline{1+i} = \bar{0}, \bar{i} = -\bar{1}$. Hence $\overline{a+ib} = \overline{a-b}$ for all $a, b \in \mathbb{Z}$. Hence f is surjective. Since $2 = (1+i)(1-i)$, $2\mathbb{Z} \subset \text{Ker } f$. Conversely if $\bar{n} = \bar{0}, n = (1+i)(a+bi)$ for some $a, b \in \mathbb{Z}$. Hence $n = (a-b) + i(a+b)$. Hence $a = -b$ and $n = 2a \in 2\mathbb{Z}$. Therefore $\mathbb{F}_2 \simeq \mathbb{Z}[i]/(1+i)$. Hence $(1+i)$ is a prime ideal.

Quotient field of an integral domain

We are familiar with the construction of the field \mathbb{Q} from \mathbb{Z} and the field $k(x) = \{f(x)/g(x) \mid f(x), g(x) \in k[x] \text{ and } g(x) \neq 0\}$, from $k[x]$, called the field of rational functions in one variable over k . These constructions can be carried out for any integral domain R . Let

$$P = \{(a, b) \mid a \in R, 0 \neq b \in R\}$$

Let $(a, b), (c, d) \in P$. Define $(a, b) \sim (c, d)$ if $ad = bc$. The relation \sim is an equivalence relation. The equivalence class of (a, b) is denoted by $\frac{a}{b}$. Put $K = \{\frac{a}{b} \mid (a, b) \in P\}$. Define addition and multiplication in K by

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

The identities for addition and multiplication are $\frac{0}{1}$ and $\frac{1}{1}$ respectively. If $\frac{a}{b} \neq \frac{0}{1}$, then $a \neq 0$. Hence $\frac{b}{a} = (\frac{a}{b})^{-1}$. Hence K is a field.

Definition 4.6. *The field K is called the **quotient field** of R .*

Example 4.7. \mathbb{Q} is the quotient field of \mathbb{Z} . The quotient field of polynomial ring $k[x]$ over a field k is the field of rational functions $k(x)$.

Example 4.8. Let k be a field, $R = k[[x]]$ be the ring of formal power series with coefficients in k . Let $f(x), g(x) \in R$ and $g(x) \neq 0$. Let $g(x) = a_mx^m + a_{m+1}x^{m+1} + \dots$ where $a_m \neq 0$ and $m \in \mathbb{N}$. Then $g(x) = x^m(a_m + a_{m+1}x + \dots)$. Let $h(x) = g(x)/x^m$. Then $h(x)$ is a unit in R . Hence $f(x)/g(x) = f(x)/(x^mh(x)) = f(x)l(x)/x^m$ where $l(x) = h(x)^{-1}$. Hence $f(x)/g(x) = \sum_{n \geq -N} a_n x^n$ for some $N \in \mathbb{N}$ and $a_n \in k$ for all n . Hence the quotient field of $k[[x]]$ called the field of meromorphic series, is given by

$$k((x)) = \left\{ \sum_{n \geq -N} a_n x^n \mid a_n \in k \text{ for all } n, \text{ and } N \in \mathbb{N} \right\}.$$

Proposition 4.9. *Let R be an integral domain with quotient field K . Let $f : R \rightarrow L$ be an injective homomorphism (embedding) of R into a field L . Then there is a unique embedding $f^* : K \rightarrow L$ whose restriction to R is f .*

Proof. (Existence) Define $f^* : K \rightarrow L$ by $f^*(a/b) = f(a)/f(b)$. Let $a/b = c/d$. Then $ad = bc$. Hence $f(a)f(d) = f(b)f(c)$. Thus $f(a)/f(b) = f(c)/f(d)$. Hence f^* is well-defined. If $f^*(a/b) = 0$ then $f(a) = 0$ and hence $a = 0$. Therefore f^* is an embedding.

(Uniqueness) Let $g : K \rightarrow L$ be an embedding extending f . Then for any $a/b \in K$, $g(a/b) = g(ab^{-1}) = g(a)g(b)^{-1} = f(a)f(b)^{-1} = f^*(\frac{a}{b})$. Hence $g = f^*$. \square

5. MAXIMAL IDEALS

Let R be a commutative ring with identity.

Definition 5.1. An ideal $I < R$ is called a **maximal ideal** if whenever $I \subset J \subset R$ where J is an ideal of R then $J = I$ or $J = R$.

Proposition 5.2. The following hold:

- (1) Maximal ideals exist in non-zero rings.
- (2) An ideal \mathfrak{m} of R is a maximal ideal if and only if R/\mathfrak{m} is a field. In particular every maximal ideal is a prime ideal.
- (3) The zero ideal is a maximal ideal of R if and only if R is a field.

Proof. (1) Consider the set $\mathcal{S} = \{I \mid I \text{ is a proper ideal of } R\}$. Under inclusion \mathcal{S} is a partially ordered set. Let T be a totally ordered subset of \mathcal{S} , i.e. for all $I, J \in T$, either $I \subset J$ or $J \subset I$. Let $U = \cup\{I \mid I \in T\}$. Then U is an ideal of R and it is proper. By Zorn's lemma, \mathcal{S} has maximal elements.

(2) Let \mathfrak{m} be a maximal ideal. Then R/\mathfrak{m} has only two ideals (0) and R/\mathfrak{m} . If $x \notin \mathfrak{m}$ then $(\bar{x}) = R/\mathfrak{m}$. Thus $\bar{1} = \bar{x}\bar{y}$ for some $y \in R$. Thus R/\mathfrak{m} is a field. The converse is similar.

(3) Follows from (2). \square

Example 5.3. Let k be a field and $R = k[x]$ and $f(x) \in R$. Let $I = (f(x))$. be a maximal ideal. Then I is a prime ideal. This implies $f(x)$ is irreducible. Conversely let $f(x)$ be irreducible. Let $g(x) \in R \setminus I$. Then $f(x)$ and $g(x)$ are coprime. Hence $1 = g(x)h(x) + f(x)l(x)$ for some $h(x), l(x) \in R$. Thus $\bar{1} = \bar{g}\bar{h}$ in R/I . Therefore R/I is a field and I be a maximal ideal. By the fundamental theorem of algebra, any polynomial $f(x) \in \mathbb{C}[x]$ of positive degree is a product of linear polynomials. Hence the maximal ideals of $\mathbb{C}[x]$ are of the form $\mathfrak{m}_a = (x - a)$ where $a \in \mathbb{C}$. Hence there is a 1 - 1 correspondence between \mathbb{C} and the set of maximal ideals in $\mathbb{C}[x]$ given by $a \mapsto \mathfrak{m}_a = (x - a)$.

Example 5.4. Let $a = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n$. Put $R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Consider the homomorphism $\phi : \mathbb{C}[x_1, x_2, \dots, x_n] \rightarrow \mathbb{C}$ defined by $\phi(f) = f(a)$. Then ϕ is surjective and $\text{Ker } \phi = \{f(x_1, \dots, x_n) \in R \mid f(a) = 0\}$.

By the Taylor series of f around a , we see that $f(a) = 0$ if and only if $f \in (x_1 - a_1, \dots, x_n - a_n) = \mathfrak{m}_a$. Hence $R/(\text{Ker}\phi) \simeq \mathbb{C}$. Thus \mathfrak{m}_a is a maximal ideal. We will show that all maximal ideals of $\mathbb{C}[x_1, x_2, \dots, x_n]$ are of this form.

Example 5.5. Let us show that the ideal $3\mathbb{Z}[i]$ is a maximal ideal of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2 + 1)$, $\mathbb{Z}[i]/(3) \simeq \mathbb{Z}[x]/(3, x^2 + 1)$. By the Third Homomorphism Theorem

$$\frac{\mathbb{Z}[x]}{(3, x^2 + 1)} \simeq \frac{\mathbb{Z}[x]/(3)}{(3, x^2 + 1)/(3)} \simeq \frac{\mathbb{F}_3[x]}{(x^2 + 1)}.$$

Since $(x^2 + 1)$ is irreducible polynomial in $\mathbb{F}_3[x]$, the ideal $(x^2 + 1)$ is a maximal ideal in $\mathbb{F}_3[x]$. Therefore (3) is a maximal ideal of $\mathbb{Z}[i]$. Using the same argument we can see that for a prime number p , (p) is a maximal ideal of $\mathbb{Z}[i]$ if and only if -1 not a square in \mathbb{F}_p . It will be proved later that -1 is a square in \mathbb{F}_p for odd prime p if and only if $p \equiv 1 \pmod{4}$. Hence for an odd prime p , (p) is a maximal ideal in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod{4}$.

Example 5.6 (Nullstellensatz for function spaces). Let X be a compact Hausdorff space and let

$$C(X) = \{f : X \rightarrow \mathbb{R} \mid f \text{ is continuous}\}.$$

$C(X)$ is a commutative ring with identity. For each $x \in X$, let

$$\mathfrak{m}_x = \{f \in C(X) \mid f(x) = 0\}.$$

Then \mathfrak{m}_x is the kernel of surjective homomorphism $\phi : C(X) \rightarrow \mathbb{R}$ defined by $\phi(f) = f(x)$. Hence $C(X)/\mathfrak{m}_x \simeq \mathbb{R}$. Thus \mathfrak{m}_x is a maximal ideal. In fact any maximal ideal of $C(X)$ is of the form \mathfrak{m}_x for some $x \in X$. Indeed, let \mathfrak{m} be a maximal ideal of $C(X)$. Consider the set

$$V(\mathfrak{m}) = \{x \in X \mid f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose $y \in V(\mathfrak{m})$. Then $\mathfrak{m} \subset \mathfrak{m}_y$. Thus $\mathfrak{m} = \mathfrak{m}_y$. Therefore it is enough to show $V(\mathfrak{m})$ is nonempty. Suppose $V(\mathfrak{m}) = \emptyset$. Then for any $x \in X$, there is an $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. By continuity of f , there is an open set $U_x \ni x$ such that $f_x(y) \neq 0$ for all $y \in U_x$. Since X is compact there exist $x_1, x_2, \dots, x_n \in X$ such that $X = U_{x_1} \cup U_{x_2} \cup \dots \cup U_{x_n}$. Let $g = f_{x_1}^2 + f_{x_2}^2 + \dots + f_{x_n}^2$. Then $g(y) \neq 0$ for any $y \in X$. Hence g is a unit in $C(X)$. But $g \in \mathfrak{m}$. This is a contradiction. Hence we have a one-to-one correspondence between X and the set of maximal ideals of $C(X)$.

6. HILBERT'S NULLSTELLENSATZ

Let $R = \mathbb{C}[x_1, x_2, \dots, x_n]$ be the polynomial ring over \mathbb{C} in the indeterminates x_1, x_2, \dots, x_n . Hilbert's Nullstellensatz establishes a one-to-one correspondence between points in \mathbb{C}^n and maximal ideals in R .

Let $a = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n$. Then $\mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal of R as seen before. Hilbert's Nullstellensatz establishes that each maximal ideal of R is of the form \mathfrak{m}_a for some $a \in \mathbb{C}^n$.

Lemma 6.1. *Let V be a vector space and W be a subspace which is linear span of a countable set of vectors $\{v_1, v_2, \dots\}$. Then any subset of W of linearly independent vectors is either finite or countable.*

Proof. Let $W_n = L(v_1, v_2, \dots, v_n)$, the linear span of v_1, v_2, \dots, v_n . Let S be a subset of W . Then $S = \bigcup_{n=1}^{\infty} S \cap W_n$. Since $S \cap W_n$ has at most n linearly independent vectors, S is either finite or countable. \square

Lemma 6.2. *The set $\{\frac{1}{x-a} \mid a \in \mathbb{C}\} \subset \mathbb{C}(x)$ is linearly independent over \mathbb{C} .*

Proof. Let $b_1, b_2, \dots, b_n, a_1, a_2, \dots, a_n \in \mathbb{C}$ so that a_1, a_2, \dots, a_n are distinct. Let

$$\frac{b_1}{x-a_1} + \frac{b_2}{x-a_2} + \dots + \frac{b_n}{x-a_n} = 0.$$

Then

$$\sum_{i=1}^n (x-a_1)(x-a_2)\dots(x-a_{i-1})b_i(x-a_{i+1})\dots(x-a_n) = 0.$$

Put $x = a_i$ to get $b_i = 0$ for $i = 1, 2, \dots, n$. Hence S is linearly independent. \square

Theorem 6.3 (Hilbert's Nullstellensatz). *There is a one-to-one correspondence between \mathbb{C}^n and the set of maximal ideals in the polynomial ring $\mathbb{C}[x_1, x_2, \dots, x_n]$ given by*

$$a = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n \longmapsto \mathfrak{m}_a = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n).$$

Proof. Put $R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Let M be a maximal ideal of R . We claim that $N = M \cap \mathbb{C}[x_1]$ is a maximal ideal of $\mathbb{C}[x_1]$. Since $N = \ker \pi$ where $\pi : \mathbb{C}[x_1] \rightarrow R/M$ is the map $\pi(f(x_1)) = f(x_1) + M$, it is a prime ideal of $\mathbb{C}[x_1]$. If $N \neq (0)$ then it is generated by a linear polynomial say $x - a_1 \in \mathbb{C}[x_1]$. If $N = (0)$ then $\pi : \mathbb{C}(x_1) \rightarrow R/M$ is an injective map. Since R/M is a field, π has a unique extension to an embedding $\mu : \mathbb{C}(x_1) \rightarrow R/M$. Since R/M is a \mathbb{C} -vector space of countable dimension, so is $\mathbb{C}(x_1)$. But $\{\frac{1}{x_1-a} \mid a \in \mathbb{C}\}$ is an uncountable linearly independent set in $\mathbb{C}(x_1)$. This is a contradiction. Hence $N \neq (0)$. Therefore $x_1 - a_1 \in M$. Similarly there are complex numbers a_2, \dots, a_n such that $x_i - a_i \in M$ for $i = 2, 3, \dots, n$. Hence

$(x_1 - a_1, \dots, x_n - a_n) \subset M$. But $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal of R . Thus $M = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$. \square

Corollary 6.4. *Let $f_1, f_2, \dots, f_t \in R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Let Z be the set of common zeros of f_1, f_2, \dots, f_t in \mathbb{C}^n and let $I = (f_1, f_2, \dots, f_t)$. Then there is a one-to-one correspondence between Z and the set of maximal ideals of R/I .*

Proof. Let $f_1(a) = f_2(a) = \dots = f_t(a) = 0$ for some $a \in \mathbb{C}^n$. Using Taylor series, we see that $f_i \in \mathfrak{m}_a$ for $i = 1, 2, \dots, t$. Hence $I \subset \mathfrak{m}_a$ which gives the maximal \mathfrak{m}_a/I in R/I . Conversely any maximal ideal of R/I has the form M/I where M is a maximal ideal of R and $I \subset M$. By Nullstellensatz $M = \mathfrak{m}_a$ for some a . Thus $f_i(a) = 0$ for all $i = 1, 2, \dots, t$. \square

7. ALGEBRAIC GEOMETRY

The main objects of study in algebraic geometry are the sets of solutions of a system of polynomial equations called algebraic varieties. We restrict ourselves to complex polynomials. Let $R = \mathbb{C}[x_1, x_2, \dots, x_n]$ be the polynomial ring over \mathbb{C} in n indeterminates x_1, x_2, \dots, x_n . Let $f_1, f_2, \dots, f_t \in R$. The zero set of f_1, f_2, \dots, f_t is the set

$$Z(f_1, f_2, \dots, f_t) = \{a \in \mathbb{C}^n \mid f_i(a) = 0 \text{ for } i = 1, 2, \dots, t\}.$$

Note that if $g \in (f_1, f_2, \dots, f_t) = I$ then any common zero of f_1, f_2, \dots, f_t is a zero of g . Therefore $Z(I) = \{a \in \mathbb{C}^n \mid g(a) = 0 \text{ for all } g \in I\} = Z(f_1, f_2, \dots, f_t)$.

Definition 7.1. *An algebraic variety in \mathbb{C}^n is the set $Z(I)$ for some ideal I of $\mathbb{C}[x_1, x_2, \dots, x_n]$. An algebraic variety V is called **irreducible** if $V \neq V_1 \cup V_2$ where $V_1, V_2 < V$ are algebraic varieties.*

Example 7.2. Let $f \in \mathbb{C}[x_1, x_2, \dots, x_n]$ be a non-constant polynomial. Then $Z(f)$ is called a **hypersurface**. If $n = 3$ then $Z(f)$ is called a **surface**. A hypersurface of \mathbb{C}^2 is called a **plane algebraic curve**.

Example 7.3. The zero set of finitely many linear equations in R is called a linear variety. These are the objects of study in linear algebra.

Example 7.4. The conics are the plane curves defined by a quadratic polynomial in $\mathbb{C}[x_1, x_2]$.

Example 7.5. An algebraic variety V defined by a homogeneous polynomial is called a **cone**. If $0 \neq a \in V$ then the line $\{ta \mid t \in \mathbb{C}\}$ is a subset of V .

Now we show that any algebraic variety is intersection of finitely many hypersurfaces. This is a consequence of the Hilbert basis theorem for Noetherian rings.

Definition 7.6. *If all ideals of a ring R are finitely generated then R is called a **Noetherian ring**.*

Proposition 7.7. *A commutative ring with identity is Noetherian if and only if given any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there exists an m such that $I_m = I_{m+i}$ for all $i \geq 0$.*

Proof. Let R be Noetherian. Since $\{I_n\}_{n=1}^{\infty}$ is an ascending chain, $I = \cup_{n=1}^{\infty} I_n$ is an ideal of R . Hence we can find $a_1, a_2, \dots, a_g \in I$ such that $I = (a_1, a_2, \dots, a_g)$. It is easy to see that there is an m such that $a_i \in I_m$ for all $i = 1, 2, \dots, g$. Hence $I \subseteq I_m$ which implies that $I_m = I_{m+i}$ for all $i \geq 0$.

Conversely let every ascending chain of ideals be stationary. Let I be an ideal of R which is not finitely generated. Then I is nonzero and $I < R$. Inductively, we can find $a_1, a_2, \dots \in I$ such that $I_n = (a_1, a_2, \dots, a_n)$ and the chain $I_n, n = 1, 2, \dots$ is not stationary. This is a contradiction. Hence I is finitely generated. □

Theorem 7.8 (Hilbert basis theorem). *Let R be a Noetherian ring. Then the polynomial ring $R[x]$ is Noetherian.*

Proof. Let I be an ideal of $R[x]$ which is not finitely generated. Let f_1 be a polynomial of least degree among polynomials in I . Since $I \neq (f_1)$, we can choose a polynomial $f_2 \in I \setminus (f_1)$ which has smallest degree among all polynomials in $I \setminus (f_1)$. Inductively we select $f_1, f_2, \dots, f_n \in I$ such that f_n has smallest degree among polynomials in $I \setminus (f_1, f_2, \dots, f_{n-1})$. Let $\deg f_i = d_i$ for $i = 1, 2, \dots$. Then $d_1 \leq d_2 \leq d_3 \leq \dots$ and

$$(f_1) < (f_1, f_2) < \dots < (f_1, f_2, f_3, \dots, f_n) < \dots$$

Write $f_n = a_n x^{d_n} + \dots$ for $n = 1, 2, 3, \dots$. We claim that the chain of ideals

$$(a_1) < (a_1, a_2) < (a_1, a_2, a_3) < \dots$$

does not terminate. Let $(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{n+1})$ for some n . Then $a_{n+1} = a_n b_n + a_{n-1} b_{n-1} + \dots + a_1 b_1$ for some $b_1, b_2, \dots, b_n \in R$. Consider the polynomial

$$g(x) = f_{n+1}(x) - \sum_{i=1}^n b_i f_i(x) x^{d_{n+1} - d_i}.$$

Then $g(x) \in I \setminus (f_1, f_2, \dots, f_n)$ and $\deg g(x) < d_{n+1}$. This is a contradiction. Therefore the chain $\{(a_1, a_2, \dots, a_n)\}_{n=1}^{\infty}$ is strictly ascending. But R is Noetherian. Hence we get a contradiction. Thus $R[x]$ is Noetherian. □

Corollary 7.9. (1) *Let $g_1, g_2, \dots, g_t \in R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Then*

$$V(g_1, g_2, \dots, g_t) = V(g_1) \cap V(g_2) \cap \dots \cap V(g_t).$$

(2) Any algebraic variety in \mathbb{C}^n is a finite intersection of hypersurfaces.

Proof. (1) It is enough to prove this for $t = 2$. Let $f, g \in R$. Then

$$a \in V(f, g) \iff f(a) = g(a) = 0 \iff a \in V(f) \cap V(g).$$

(2) Let $V = Z(I)$ for an ideal I in $\mathbb{C}[x_1, x_2, \dots, x_n]$. Since \mathbb{C} is Noetherian, $\mathbb{C}[x_1, x_2, \dots, x_n]$ is Noetherian by Hilbert basis theorem. Hence $I = (f_1, f_2, \dots, f_n)$ for some $f_1, f_2, \dots, f_n \in \mathbb{C}[x_1, x_2, \dots, x_n]$. Therefore $V = V(f_1, f_2, \dots, f_n) = V(f_1) \cap V(f_2) \cap \dots \cap V(f_n)$. \square

Definition 7.10. Let $V \subset \mathbb{C}^n$ be an algebraic variety. The **ideal of V** , is the ideal

$$I(V) = \{f \in \mathbb{C}[x_1, x_2, \dots, x_n] \mid f(a) = 0 \text{ for all } a \in V\}.$$

Proposition 7.11. Let $R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Let $V, W \subseteq \mathbb{C}^n$ be algebraic varieties. Then

- (1) $I(V)$ is a radical ideal of R .
- (2) $I(V \cup W) = I(V) \cap I(W)$.
- (3) $Z(I(V)) = V$.
- (4) V is irreducible if and only if $I(V)$ is a prime ideal.

Proof. (1) Let $f \in R$ and $f^m \in I(V)$ for some m . Then $f^m(a) = 0$ for all $a \in V$. Hence $f(a) = 0$ for all $a \in V$. This means $f \in I(V)$. Thus $\sqrt{I(V)} = I(V)$.

(2) $f \in I(V \cup W) \iff f(a) = 0$ for all $a \in V \cup W \iff f(a) = 0$ for all $a \in V$ and $a \in W \iff f \in I(V) \cap I(W)$.

(3) Left as an exercise.

(4) Suppose V is irreducible. Let $fg \in I(V)$ for some $f, g \in R$. Then $V(fg) = V(f) \cup V(g) \supset V$. Hence $V = (V \cap V(f)) \cup (V \cap V(g))$. Since V is irreducible, $V = V \cap V(f)$ or $V = V \cap V(g)$. Without loss of generality, let $V = V \cap V(f)$. Then $V \subset V(f)$ and hence $f \in I(V(f)) \subset I(V)$. Therefore $I(V)$ is a prime ideal.

Conversely let $I(V)$ be a prime ideal. Suppose that $V = V_1 \cup V_2$ where V_1 and V_2 are algebraic varieties properly contained in V . Then $I(V) = I(V_1) \cap I(V_2)$. Since $I(V_1)I(V_2) \subset I(V)$, either $I(V_1) \subset I(V)$ or $I(V_2) \subset I(V)$. Without loss of generality let $I(V_1) \subset I(V)$. Then $V_1 = Z(I(V_1)) \supset V = Z(I(V))$. Thus $V = V_1$ and therefore V is irreducible. \square

Theorem 7.12 (Strong Nullstellensatz). Let J be an ideal of $R = \mathbb{C}[x_1, x_2, \dots, x_n]$. Then

- (1) $Z(J) = \emptyset$ if and only if $J = R$

- (2) $I(Z(J)) = \sqrt{J}$
(3) The maps $J \mapsto Z(J)$ and $V \mapsto I(V)$ are inverses of each other:

$$\begin{aligned} \{\text{algebraic varieties } \subset \mathbb{C}^n\} &\leftrightarrow \{\text{radical ideals of } R\} \\ V &\mapsto I(V) \\ J &\mapsto Z(J) \end{aligned}$$

- (4) The one-to-one correspondence $V \mapsto I(V)$ maps irreducible algebraic varieties in \mathbb{C}^n to prime ideals of R .

Proof. (1) Let $Z(J) = \emptyset$. If $J \neq R$ then there is a maximal ideal \mathfrak{m} of R containing J . By Hilbert's Nullstellensatz $\mathfrak{m} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ for $a = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n$. Hence $f(a) = 0$ for all $f \in J$. Thus $a \in Z(J)$ which is a contradiction. Conversely let $J = R$. Then $1 \in J$. If $a \in Z(J)$ then $1(a) = 1 = 0$, a contradiction.

(2) $J \subset I(Z(J))$ is clear. Let $0 \neq g \in I(Z(J))$. Let t be a new variable. Consider the ideal $I = (f_1, f_2, \dots, f_m, tg - 1) \subset R[t]$ where $J = (f_1, f_2, \dots, f_m)$. Let $b = (b_1, b_2, \dots, b_n, b_{n+1}) \in \mathbb{C}^{n+1}$ be in $Z(I)$. Then $f_1(b) = \dots = f_m(b) = 0$. Since $g \in I(Z(J))$, $g(b_1, \dots, b_n) = 0$. Since $b \in Z(I)$, $(tg - 1)(b) = -1 = 0$. This contradiction shows that $Z(I) = \emptyset$. Hence by (1), $I = R[t]$. Hence

$$1 = g_1 f_1 + g_2 f_2 + \dots + g_m f_m + g_{m+1}(tg - 1)$$

for some $g_1, g_2, \dots, g_{m+1} \in R[t]$. Put $t = 1/g$ to get

$$1 = g_1(x_1, \dots, x_n, 1/g)f_1 + g_2(x_1, \dots, x_n, 1/g)f_2 + \dots + g_m(x_1, \dots, x_n, 1/g)f_m$$

After clearing the denominators we see that there is an r such that $g^r \in (f_1, f_2, \dots, f_m) = J$. Thus $g \in \sqrt{J}$.

(3) Let J be a radical ideal of R . Then $I(Z(J)) = J$. Let $V \subset \mathbb{C}^n$ be an algebraic variety. Then $Z(I(V)) = V$. Hence the maps $J \mapsto Z(J)$ and $V \mapsto I(V)$ are inverses of each other.

(4) Let $V \subset \mathbb{C}^n$ be an algebraic variety. Then V is irreducible if and only if $I(V)$ is a prime ideal. Hence in the correspondence in (3), prime ideals of R correspond to irreducible algebraic varieties of \mathbb{C}^n . \square

8. UNIQUE FACTORIZATION DOMAINS

Definition 8.1. Let R be an integral domain. A nonzero element $a \in R$ is called **irreducible** if it is not a unit and whenever $a = bc$ then either b or c is a unit. We say a is a **prime** if (a) is a prime ideal.

Proposition 8.2. Let R be an integral domain and $0 \neq a \in R$. If a is a prime element then it is irreducible.

Proof. Suppose (a) is a prime ideal. If $a = bc$ for some $b, c \in R$ then either b or $c \in (a)$. Without loss of generality let $b \in (a)$. Then $b = ad$ for some $d \in R$. Hence $a = adc$. Since R is an integral domain $dc = 1$. Therefore c is a unit. Hence a is irreducible. \square

Example 8.3. It is clear that irreducible elements of \mathbb{Z} are $\pm p$ where p is a prime number. The irreducible elements of a polynomial ring $k[x]$ over a field k are $cf(x)$ where $c \in k^\times = k \setminus \{0\}$ and $f(x) \in k[x]$ is a monic irreducible polynomial.

Example 8.4. Irreducible elements need not be prime. Consider the ring $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Recall that the norm of $a + b\sqrt{-5}$ is $N(a + b\sqrt{-5}) = a^2 + 5b^2$. If $x \in R$ is a unit then there is a $y \in R$ such that $xy = 1$. Let $x = a + b\sqrt{-5}$ and $y = c + d\sqrt{-5}$. Hence $N(xy) = N(x)N(y) = 1 = (a^2 + 5b^2)(c^2 + 5d^2)$. It follows that $x, y = \pm 1$. Therefore the units in R are ± 1 . Consider the following factorizations of 9 in R .

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Using the norm function we see that $3, 2 + \sqrt{-5}$ and $2 - \sqrt{-5}$ are irreducible elements. But none of them are prime. Note that

$$\frac{\mathbb{Z}[\sqrt{-5}]}{(3)} \simeq \frac{\mathbb{Z}[x]/(x^2 + 5)}{(3)} \simeq \frac{\mathbb{F}_3[x]}{(x^2 + 5)}$$

1 and -1 are roots of $x^2 + 5$ in \mathbb{F}_3 . Hence $(x + 1)(x - 1) = (x^2 + 5)$ in $\mathbb{F}_3[x]$. Thus $\mathbb{F}_3[x]/(x^2 + 5)$ is not an integral domain. Hence 3 is not a prime in R .

Definition 8.5. A non-zero element a of an integral domain R is said to have a **unique factorization into irreducible elements** if $a = up_1p_2 \dots p_n$ for a unit $u \in R$ and irreducible elements p_1, p_2, \dots, p_n of R and if $a = vq_1q_2 \dots q_m$ is another factorization where v is a unit and q_1, q_2, \dots, q_m are irreducible then $m = n$ and there is a permutation $\sigma \in S_n$ such that $p_i = u_iq_{\sigma(i)}$ for units u_i and $i = 1, 2, \dots, m$. We say R is a **unique factorization domain** if every non-zero element has a unique factorization.

Proposition 8.6. Irreducible elements in a UFD are prime.

Proof. Let R be a UFD and $p \in R$ be an irreducible element. Let $a, b \in R$ and $ab \in (p)$. Then $ab = cp$ for some $c \in R$. Let $a = up_1p_2 \dots p_m$ and $b = vq_1q_2 \dots q_n$ be the unique factorization of a and b into irreducibles respectively. By uniqueness $p = u_i p_i$ or $p = v_j q_j$ for some units $u_i, v_j \in R$. Hence $a \in (p)$ or $b \in (p)$. Therefore p is prime. \square

Definition 8.7. Let R be an integral domain. If $a, b \in R^\times$ and $a = bc$ for some $c \in R$ then we say b **divides** a or a is a **multiple** of b and write this

as $b \mid a$. If c is a unit then we say a and b are **associates** and write this as $a \sim b$. If b and c are not units then they are called **proper divisors** of a .

Proposition 8.8. *Let R be an integral domain and $a, b \in R$. Then*

- (1) a is a unit in R if and only if $(a) = R$.
- (2) a and b are associates if and only if $(a) = (b)$
- (3) $a \mid b$ if and only if $(b) \subset (a)$
- (4) a is a proper divisor of b if and only if $(b) < (a) < R$.
- (5) a is irreducible if and only if (a) is maximal among proper principal ideals.

For an integral domain R to be a UFD, each non-zero element must have a factorization into irreducible elements and the factorization must be unique. We now discuss the existence of factorization into irreducibles in terms of principal ideals.

Definition 8.9. *An integral domain R is called a **factorization domain**, abbreviated as **FD**, if every non-zero element of R can be expressed as a product of irreducible elements.*

Definition 8.10. *A ring R is said to satisfy **ascending chain condition** (acc) on principal ideals if for any chain $(a_1) \subset (a_2) \subset \dots$ of principal ideals of R , there exists an n such that $(a_n) = (a_{n+i})$ for all $i = 1, 2, 3, \dots$*

Proposition 8.11. (1) *A Noetherian domain is a factorization domain.*
 (2) *If an integral domain satisfies ascending chain condition on principal ideals then it is an FD.*
 (3) *Let R be an integral domain. If there is a function $g : R^\times \rightarrow \mathbb{N} = \{0, 1, 2, \dots\}$ such that if a is a proper divisor of b then $g(a) < g(b)$, then R is an FD.*

Proof. (1) Suppose there is an element $a \neq 0$ which is not a unit and it does not have a factorization into irreducibles. Let S be the set of all principal ideals (a) such that a is not a unit and it has no factorization into irreducible. Then S has a maximal element say (b) . Then b is reducible. Hence $b = cd$ where c and d are not units. Thus (c) and (d) properly contain (a) . Hence c and d are products of irreducibles. Therefore a is so. This is a contradiction. Hence R is an FD.

(2) Suppose R is an integral domain satisfying acc (ascending chain condition) on principal ideals. This implies that any nonempty collection of principal ideals has a maximal member. Now we argue as in (1).

(3) Let $(a_1) < (a_2) < \dots$ be an ascending chain of principal ideals. Then

$$g(a_1) > g(a_2) > \dots$$

This is a contradiction. Hence R satisfies acc on principal ideals. By (2), R is a FD. \square

Proposition 8.12. *Let R be an FD. Then it is a UFD if and only if every irreducible element of R is a prime element.*

Proof. We have already proved that irreducible elements in a UFD are prime. Conversely let irreducible elements of R be primes. Suppose $a \in R^\times$ be not a unit and

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

where p_1, \dots, p_m and q_1, \dots, q_n are primes. We may assume $m \leq n$. Since (p_1) is a prime ideal, there exists q_j such that $q_j \in (p_1)$. Hence $q_j = p_1 r_j$ for some $r_j \in R$. Substitute $q_j = p_1 r_j$ into the above expression of a and cancel p_1 to obtain $p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{j-1} r_j q_{j+1} \cdots q_n$. Since q_j is irreducible, r_j is a unit. We are done by induction on m . \square

Corollary 8.13. *The polynomial ring $k[x]$ over a field k and \mathbb{Z} are unique factorization domains.*

Proof. Since \mathbb{Z} and $k[x]$ are Noetherian, they are factorization domains. Let p be an irreducible integer. Let $p \mid ab$ and $p \nmid a$. Then $\gcd(p, a) = 1$. By Euclid's division algorithm $1 = pr + as$ for some $r, s \in \mathbb{Z}$. Hence $b = pbr + abs$. Therefore $p \mid b$. A similar argument shows that irreducible polynomials in $k[x]$ are primes. Hence \mathbb{Z} and $k[x]$ are UFDs. \square

Example 8.14. Let k be a field and $R = k[[x]]$ be the formal power series ring. Since $R/(x) \simeq k$, x is a prime element. Let $f(x) \in R$. Then $f(x) = x^r(a_0 + a_1x + \cdots)$ where $a_0 \neq 0$. Hence x is the only irreducible element of R and R is a UFD.

Example 8.15. Rings of integers in quadratic fields $\mathbb{Q}(\sqrt{d})$ where d is a square free integer, are Noetherian. Hence they are factorization domains. We will later discuss unique factorization in some of them.

9. PRINCIPAL IDEAL DOMAINS AND EUCLIDEAN DOMAINS

Definition 9.1. *An integral domain R is called **principal ideal domain** (PID) if every ideal of R is principal.*

Theorem 9.2. *A principal ideal domain is a UFD.*

Proof. Let R be a PID. Then it is Noetherian. Hence it is an FD. To show R is a UFD, we need to show that irreducible elements are prime. Let p be an irreducible element. Let $p \mid ab$ where $a, b \in R$. Let $p \nmid a$. Then $(p) < (p, a)$. Since (p) is maximal among proper principal ideals, $(p, a) = R$. Thus $1 = pc + ad$ for some $c, d \in R$. Therefore $b = bpc + abd$. Hence $p \mid b$. \square

Definition 9.3. An integral domain R is called a **Euclidean domain** if there exists a map $\delta : R^\times \rightarrow \mathbb{N}$ such that for all $a, b \in R, b \neq 0$ $a = bq + r$ where $q, r \in R$ and $r = 0$ or $\delta(r) < \delta(b)$.

Example 9.4. Define $\delta : \mathbb{Z} \rightarrow \mathbb{N}$ by $\delta(n) = |n|$. With respect to δ, \mathbb{Z} is a Euclidean domain.

Example 9.5. Let $R = k[x]$ be the polynomial ring over a field k . Define $\delta(f) = \deg f$ for $0 \neq f \in \mathbb{R}$. By Euclid's division algorithm R is a Euclidean domain.

Example 9.6. Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Define $N(a + bi) = a^2 + b^2$. Then $N(xy) = N(x)N(y)$ for all $x, y \in R$. Let $x, y \in \mathbb{Z}[i], y \neq 0$. Let $x/y = a + bi$. Let $a, d \in \mathbb{Z}$ such that $|a - c| \leq \frac{1}{2}$ and $|b - d| \leq \frac{1}{2}$. Then

$$\frac{x}{y} = (a - c) + (b - d)i + c + di.$$

Hence $x = (c + di)y + (a - c + (b - d)i)y$.

$$N((a - c)y + (b - d)yi) = N(y)N((a - c) + i(b - d)) \leq \frac{1}{2}N(y)$$

Thus $\mathbb{Z}[i]$ is a Euclidean domain.

Theorem 9.7. Euclidean domain are principal ideal domains.

Proof. Let I be a nonzero ideal of a Euclidean domain R . Consider the set $S = \{\delta(a) \mid a \in I, a \neq 0\}$. By well-ordering principle, S has a minimal element say $\delta(b)$. We claim that $I = (b)$. Let $a \in I$. Then $a = bq + r$ for $q, r \in R$ and $r = 0$ or $\delta(r) < \delta(b)$. Since $r \in I$, and $\delta(b)$ is minimal in S , so $r = 0$. Hence $I = (b)$. □

10. PRIME IDEALS IN $\mathbb{Z}[i]$ AND FERMAT'S TWO SQUARE THEOREM

Recall that by using the Euclidean norm $N(a + bi) = a^2 + b^2$, we proved that $\mathbb{Z}[i]$ is a Euclidean domain. If $u \in \mathbb{Z}[i]$ is a unit then $N(u) = 1$. Hence $u = \pm 1, \pm i$.

In this section we determine all the prime ideals of $\mathbb{Z}[i]$. As a consequence we will prove Fermat's two-square theorem which asserts that an odd prime p is a sum of two squares in \mathbb{N} if and only if $p \equiv 1 \pmod{4}$.

Definition 10.1. A prime number will be called a **rational prime**. A prime element in $\mathbb{Z}[i]$ will be called a **Gaussian prime**.

Proposition 10.2. (1) If $N(a + ib) = a^2 + b^2 = p$ is a rational prime then $a + ib$ is a Gaussian prime.

- (2) If π is a Gaussian prime then $N(\pi) = \pi\bar{\pi}$ is either a rational prime or square of a rational prime.

Proof. (1) Let $\alpha = a + bi$ and $\alpha = \beta\gamma$ for $\beta, \gamma \in \mathbb{Z}[i]$. Then $N(\alpha) = N(\beta)N(\gamma) = p$. Hence either $N(\beta)$ or $N(\gamma)$ is ± 1 . Hence either β or γ is a unit in $\mathbb{Z}[i]$. Thus α is a Gaussian prime.

(2) Let π be a Gaussian prime. Then $(\pi) \cap \mathbb{Z} = (p)$ where p is a rational prime. Indeed, $N(\pi) = \pi\bar{\pi}$ is a nonzero integer. Hence $(\pi) \cap \mathbb{Z} \neq (0)$. Since $(\pi) \cap \mathbb{Z}$ is a prime ideal, $(\pi) \cap \mathbb{Z} = (p)$ for some prime. Thus $p = \pi\mu$. Hence $N(\pi)N(\mu) = N(p) = p^2$. Therefore $N(\pi) = p$ or p^2 . \square

Theorem 10.3. *The following are equivalent for a rational prime p .*

- (1) $p = \pi\bar{\pi}$ where π is a Gaussian prime.
- (2) $p = a^2 + b^2$ for some $a, b \in \mathbb{N}$.
- (3) $x^2 \equiv -1 \pmod{p}$ has an integer solution.
- (4) $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. (1) \implies (2) Let $\pi = a + bi \in \mathbb{Z}[i]$. Then $\pi\bar{\pi} = a^2 + b^2 = p$.

(2) \implies (3) If $p = a^2 + b^2$ then $a, b \neq 0$. Hence $a^2 \equiv -b^2 \pmod{p}$. Therefore $(ab^{-1})^2 \equiv -1 \pmod{p}$.

(3) \implies (4) Let p be an odd prime. Let $a \in \mathbb{N}$ and $a^2 \equiv -1 \pmod{p}$. Then $o(\bar{a}) = 4$ in the multiplicative group \mathbb{F}_p^\times if p is odd. Hence $4 \mid p - 1$. Thus $p \equiv 1 \pmod{4}$.

(4) \implies (3) For $p = 2$, 1 is a solution to $x^2 \equiv -1 \pmod{p}$. Now let $p \neq 2$ and $p \equiv 1 \pmod{4}$. Then \mathbb{F}_p^\times has a Sylow 2-subgroup of order at least 4. Thus it has a subgroup H of order 4. Since the elements of order 2 satisfy the equation $x^2 = 1$ which has only two solutions 1 and -1 , the subgroup H is a cyclic group of order 4. Hence there is an integer a such that $a^4 \equiv 1 \pmod{p}$. Thus $a^2 \equiv -1 \pmod{p}$.

(3) \implies (1) Note that $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2 + 1)$. Let $a^2 \equiv -1 \pmod{p}$. Then

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[x]}{(p, x^2 + 1)} \simeq \frac{\mathbb{F}_p[x]}{(x^2 + \bar{1})} \simeq \frac{\mathbb{F}_p[x]}{(x + \bar{a})(x - \bar{a})}.$$

Thus p is not irreducible. Let π be an irreducible factor in $\mathbb{Z}[i]$ of p . Then $\pi\delta = p$ for some non unit $\delta \in \mathbb{Z}[i]$. Thus $N(\pi)N(\delta) = p^2$. Since $N(\delta) \neq 1$, $N(\pi) = p = \pi\bar{\pi}$. \square

Corollary 10.4 (Fermat's two square theorem). *Let p be a prime number. Then p is a sum of two squares if and only if $p \equiv 1 \pmod{4}$.*

Corollary 10.5. *The irreducible Gaussian integers are*

- (1) $1 + i$ and its associates.
- (2) Rational primes p such that $p \equiv 3 \pmod{4}$.

- (3) Any irreducible factor $a+bi$ and its associates where $(a+bi)(a-bi) = p = a^2 + b^2$ where p is a prime and $p \equiv 1 \pmod{4}$.

Proof. (1) Let $x = u(1+i)$ where u is a unit in $\mathbb{Z}[i]$. Then $N(x) = N(1+i) = 2$ is a prime. Thus x is irreducible.

(2) If p is not irreducible then $p = \pi\bar{\pi}$ where π is irreducible in $\mathbb{Z}[i]$. But then $p \equiv 1 \pmod{4}$. Thus if $p \equiv 3 \pmod{4}$, p is irreducible in $\mathbb{Z}[i]$

(3) Let $p \equiv 1 \pmod{4}$ then for some $a, b \in \mathbb{N}$, $(a+bi)(a-bi) = p$. Since $N(a+bi) = p$ is a prime $a+bi$ is irreducible. \square

If $a+bi$ is irreducible then $(a+bi)(a-bi) = a^2+b^2$ is a product of rational primes, hence it divides some rational prime. Hence the list in (1), (2), (3) exhausts all Gaussian primes.

Pythagorean Triplets

The solutions in integers of the Diophantine equation $x^2 + y^2 = z^2$ are called the Pythagorean triplets. Using unique factorization in $\mathbb{Z}[i]$ we find all the Pythagorean triplets.

Suppose that $x^2 + y^2 = z^2$ has a solution in \mathbb{Z} . Then we can find one in which $(x, y) = 1$. Thus one of x and y is odd and hence z is odd. We can rewrite $x^2 + y^2 = z^2$ in $\mathbb{Z}[i]$ as

$$(x+iy)(x-iy) = z^2 \quad (1)$$

We claim that $(x+iy, x-iy) = 1$. Indeed, let $\pi \in \mathbb{Z}[i]$ be irreducible and let π divide $x+iy$ and $x-iy$. Then $\pi \mid 2x$ and $\pi \mid 2y$. If $\pi \mid 2$ then $(\pi) = (1+i)$ which is not possible since z is odd. Hence $\pi \mid x$ and $\pi \mid y$. Take norms to conclude that $N(\pi) \mid x^2$ and $N(\pi) \mid y^2$. But $(x, y) = 1$. Hence $x+iy$ and $x-iy$ are coprime in $\mathbb{Z}[i]$. Hence $x+iy = u(a+ib)^2$ for some unit u and $a, b \in \mathbb{Z}$. Hence $x+iy = u(a^2 - b^2 + 2abi)$. By taking $u = 1$ we get $x = a^2 - b^2$, $y = 2ab$ and therefore $z = a^2 + b^2$. By taking other values of u we get similar expressions for x, y, z .

Conversely $x = a^2 - b^2$, $y = 2ab$ and $z = a^2 + b^2$ satisfy $x^2 + y^2 = z^2$ for any $a, b \in \mathbb{Z}$. Thus we have found all the Pythagorean triplets.

11. POLYNOMIAL RINGS OVER UNIQUE FACTORIZATION DOMAINS

In this section, we will prove that the polynomial ring $R[x]$ over a UFD R is again a UFD. Let K be the quotient field of R . Then $R[x]$ is a subring of $K[x]$. Since $K[x]$ is a UFD we try to relate factorization in $R[x]$ and $K[x]$. This analysis leads to a proof of this important theorem.

Definition 11.1. Let R be a UFD. The **content** of $f(x) \in R[x]$, denoted by $c(f)$, is the greatest common divisor of coefficients of $f(x)$. If $c(f) = 1$ we say $f(x)$ is **primitive**.

Theorem 11.2 (Gauss' Lemma). *Let R be a UFD. If $f(x), g(x) \in R[x]$ are primitive then so is $f(x)g(x)$.*

Proof. Suppose p is a prime in R dividing the coefficients of $f(x)g(x)$. Consider the natural map $\pi : R[x] \rightarrow R/(p)[x]$ given by $\pi(a_0 + a_1x + \dots + a_nx^n) = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n$ where “ $\bar{}$ ” denotes residue class in $R/(p)$. Thus $\bar{f}(x)\bar{g}(x) = \overline{f(x)g(x)} = 0$ in $R/(p)[x]$. Since $R/(p)[x]$ is an integral domain, either $\bar{f}(x) = 0$ or $\bar{g}(x) = 0$. Hence either $p \mid c(f)$ or $p \mid c(g)$ which is a contradiction. \square

Corollary 11.3. *For $f, g \in R[x]$ we have $c(fg) = c(f)c(g)$.*

Proof. Let $c(f) = a$ and $c(g) = b$. Then $f(x) = af_1(x)$ and $g(x) = bg_1(x)$ where $f_1(x)$ and $g_1(x)$ are primitive. Hence $f_1(x)g_1(x)$ is primitive. Since $f(x)g(x) = abf_1(x)g_1(x)$ we conclude that $c(f(x)g(x)) = ab$. \square

Proposition 11.4. *Let R be a UFD with quotient field K . If $f(x), g(x) \in R[x]$ are primitive and associates in $K[x]$ then they are associates in $R[x]$.*

Proof. The units in $K[x]$ are nonzero elements of K . Let $f(x) = (a/b)g(x)$ where $a, b \in R, b \neq 0$. Then $bf(x) = ag(x)$. Since $f(x)$ and $g(x)$ are primitive $c(bf) = b$ and $c(ag) = a$. Hence $a = ub$ where u is a unit in R . Hence $f(x) = ug(x)$. \square

Proposition 11.5. *Let R be a UFD with quotient field K . Let $f(x) \in R[x]$ be irreducible. Then $f(x)$ is irreducible in $K[x]$.*

Proof. Since $f(x)$ is irreducible in $R[x]$, it is a primitive polynomial. Suppose $f(x) = g(x)h(x)$ where $g(x), h(x) \in K[x]$ are of positive degree. Write $g(x) = \frac{a}{b}g_1(x), h(x) = \frac{c}{d}h_1(x)$ where $g_1(x), h_1(x) \in R[x]$ are primitive and $a, b, c, d \in R$. Then $bdf(x) = acg_1(x)h_1(x)$. Therefore $ubd = ac$ where $u \in R$ is a unit. Hence $f(x) = ug_1(x)h_1(x)$. This contradicts irreducibility of $f(x)$. \square

Theorem 11.6. *If R is a UFD then $R[x]$ is a UFD.*

Proof. We need to show $R[x]$ is a factorization domain and every irreducible element of $R[x]$ is a prime element. Let $f(x) \in R[x]$ and $\deg f(x) = d$. Let $d = 0$. Then $f(x) = a \in R$. Since R is a UFD, a is a product of prime elements. If p is an irreducible factor of a then p is irreducible in $R[x]$. Now let $d > 0$. Assume that every $f(x) \in R[x]$ of degree $< d$ factors as a product of irreducibles. Write $f(x) = af_1(x)$ where $f_1(x)$ is primitive and $a = c(f)$. If $f_1(x)$ is irreducible then we are done. Otherwise $f_1(x) = g(x)h(x)$ where $g(x), h(x)$ have positive degree. By induction $g(x)$ and $h(x)$ are products of irreducible elements in $R[x]$. Hence so is $f_1(x)$.

It remains to prove that irreducible elements in $R[x]$, are prime. If $a \in R$ is irreducible in $R[x]$ then it is so in R too. Thus a is prime in R . But $R[x]/(a) \simeq R/(a)[x]$, hence $R[x]/(a)$ is an integral domain. Thus (a) is a prime ideal of $R[x]$. Therefore a is a prime element of $R[x]$. Now consider an irreducible polynomial $f(x) \in R[x]$ of positive degree. Then $f(x)$ is irreducible in $K[x]$. Hence $(f(x))$ is a prime ideal of $K[x]$. Let $f(x)|g(x)h(x)$ where $g(x), h(x) \in R[x]$ and $(f(x), g(x)) = 1$. Then $f(x)|h(x)$ in $K[x]$. Let $h(x) = f(x)a(x)$ where $a(x) \in K[x]$. Write $a(x) = \frac{c}{d}a_1(x)$ where $a_1(x) \in R[x]$ is primitive and $c, 0 \neq d \in R$. Then $dh(x) = cf(x)a_1(x)$. Let $h(x) = eh_1(x)$ where $e \in R$ and $h_1(x) \in R[x]$ is primitive. Therefore $h_1(x) \sim f(x)a_1(x)$ which means $f(x)$ divides $h_1(x)$. Since $h_1(x)|h(x)$, $f(x)|h(x)$ and we are done. \square

Proposition 11.7 (Eisenstein's Criterion). *Let R be an integral domain and let P be a prime ideal of R . Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ and $n \geq 1$. Suppose $a_0, a_1, \dots, a_{n-1} \in P, a_0 \in P \setminus P^2$ and $a_n \notin P$. Then $f(x)$ has no divisors of degree d such that $1 \leq d \leq n-1$.*

Proof. Let $f(x) = g(x)h(x)$ where $g(x), h(x) \in R[x]$ have positive degrees. Reduce the coefficients modulo P and let $\bar{f}(x)$ denote the polynomial obtained from $f(x)$ by reducing the coefficients of $f(x)$ modulo P . Then $\bar{f}(x) = \bar{a}_nx^n = \bar{g}(x)\bar{h}(x)$. Thus the leading coefficients of $g(x)$ and $h(x)$ do not belong to P . It also follows that $g(0), h(0) \in P$ which implies $f(0) = g(0)h(0) \in P^2$ which is a contradiction. \square

Example 11.8. Let P be a prime number. Consider the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x - 1)$. Put $x = y + 1$ to get

$$f(y) = [(y+1)^p - 1]/y = y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \cdots + p.$$

By Eisenstein's criterion $f(y)$ and hence $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 11.9. Let k be a field and $R = k[x_1, x_2, \dots, x_n], n \geq 3$. Let

$$f(x_1, x_2, \dots, x_n) = a_1x_1^{r_1} + a_2x_2^{r_2} + \cdots + a_nx_n^{r_n}$$

where $r_1, r_2, \dots, r_n \geq 2$ and $a_1, a_2, \dots, a_n \in k^\times$. If $\text{char } k = p > 0$ then we further assume that p does not divide r_1 . We show that f is irreducible. First note that f is square free. Indeed, let $g \in R$ be irreducible of positive degree and $g^2h = f$ for some $h \in R$. Then

$$\frac{\partial f}{\partial x_1} = r_1a_1x_1^{r_1-1} = 2g\frac{\partial g}{\partial x_1}h + g^2\frac{\partial h}{\partial x_1} = g\left(2h\frac{\partial g}{\partial x_1} + g\frac{\partial h}{\partial x_1}\right)$$

Thus $g \sim x_1$. But $x_1 \nmid f$. Therefore f is square free. Let $R = S[x_n]$ where $S = k[x_1, x_2, \dots, x_{n-1}]$. Let $f = a_n x_n^{r_n} + f_1$ where $f_1 = f - a_n x_n^{r_n}$. Then f satisfies the conditions for Eisenstein's criterion. Thus f is irreducible.

Algebraic varieties of the complex plane

Theorem 11.10. *Let V be a nonempty irreducible algebraic variety in the complex plane \mathbb{C}^2 . Then V is either a point or a plane curve.*

Proof. Let $P = I(V)$. Then P is a prime ideal of $\mathbb{C}[x, y] = R$. The ring R is a Noetherian UFD. Let $P = (f_1, f_2, \dots, f_t)$ where f_1, \dots, f_t are irreducible polynomials. Then $V = Z(P) = V(f) \cap \dots \cap V(f_t)$. If $t = 1$, we are done. Let $t \geq 2$. We show $Z(f, g)$, where f and g are irreducible coprime polynomials in R , is a finite set. If $f, g \in \mathbb{C}[x]$ or $\mathbb{C}[y]$ then it is clear. So let $f, g \in \mathbb{C}[x, y]$ be nonconstant polynomials involving both x and y . Since f, g are irreducible in $\mathbb{C}[x, y]$, they are so in $\mathbb{C}(x)[y]$. Hence $1 = rf + sg$ for some $r, s \in \mathbb{C}(x)[y]$. Clear the denominators of r and s to get a polynomial $h(x)$ such that $h(x) = r_1 f + s_1 g$ where r_1 and $s_1 \in \mathbb{C}[x, y]$. Let $(a, b) \in Z(f, g)$. Then $h(a) = 0$. Hence a has finitely many values. Similarly b has finitely many values. Therefore $Z(f, g)$ is a finite set. Therefore V is a point since V is irreducible. \square

Corollary 11.11. *The nonzero prime ideals of $\mathbb{C}[x, y]$ are the principal prime ideals and maximal ideals.*

EXERCISES

Definition and examples of rings

- (1) An element a of a ring R is called **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$. Show that if u is a unit and a is nilpotent in R , then $u + a$ is a unit.
- (2) Let R be a ring and $x, y, z \in R$. Prove the following:
 - (a) $0x = 0$, $(-x)y = -xy$, $(-x)(-y) = xy$.
 - (b) If $1 = 0$ then $R = \{0\}$.
 - (c) If a nonzero element $a \in R$ has a left inverse b and a right inverse c , then $b = c$.
- (3) Show that in the axioms for a ring with identity, commutativity of addition follows from the two distributive laws.
- (4) A ring R is called a **Boolean ring** if $x^2 = x$ for all $x \in R$. Show that a Boolean ring is commutative.
- (5) Let E be the set of all integer sequences $a = (a_1, a_2, a_3, \dots)$. We add sequences componentwise. Let R be the set of all mappings $f : E \rightarrow E$ such that $f(a + b) = f(a) + f(b)$ for all $a, b \in E$. Let $T : E \rightarrow E$ be the shift operator $T(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots)$. Show that T has a left inverse but not a right inverse.
- (6) Let R be the ring of all continuous real valued functions defined on the closed interval $[0, 1]$. Find the units of R . Show that functions in R with only finite number of zeros are not zerodivisors.
- (7) Show that the group of units in $\mathbb{Z}[(1 + \sqrt{-3})/2]$ is $\{\pm 1, \pm \rho, \pm \rho^2\}$ where $\rho = (-1 + \sqrt{-3})/2$.
- (8) Find all the units in the ring of quadratic integers for $d < 0$ and $d \neq -3$.
- (9) Find infinitely many units in the ring $\mathbb{Z}[\sqrt{2}]$.
- (10) Let R be an integral domain and $R[x]$ the polynomial ring. Show that $R[x] = R[g(x)]$ for some $g(x) \in R[x]$ if and only if $g(x) = ax + b$ for some unit $a \in R$.
- (11) Show that $f(x) \in R[[x]]$ is a unit if and only if $f(0)$ is a unit in R .

Homomorphisms and ideals

- (12) Prove that every nonzero ideal in $\mathbb{Z}[i]$ contains a nonzero integer.
- (13) Describe the kernels of the homomorphisms:
 - (a) $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$ given by $\phi(f(x)) = f(2 + i)$.
 - (b) $\phi : \mathbb{C}[x, y, z] \rightarrow \mathbb{C}[t]$ defined by $\phi(x) = t$, $\phi(y) = t^2$, $\phi(z) = t^3$ and $\phi(a) = a$ for all $a \in \mathbb{C}$.

- (c) $\phi : \mathbb{C}[x, y] \rightarrow \mathbb{C}[t]$ defined by $\phi(x) = t^3$ and $\phi(y) = t^5$ and $\phi(a) = a$ for all $a \in \mathbb{C}$.
- (14) An isomorphism of a ring R is called an **automorphism** of R . Determine all automorphisms of $\mathbb{Z}[x]$ and \mathbb{R} .
- (15) Let R be a ring and x and y be indeterminates. Let $f(y) \in R[y]$. Define $\phi : R[x, y] \rightarrow R[x, y]$ by $\phi(x) = x + f(y)$, $\phi(y) = y$ and $\phi(r) = r$ for all $a \in R$. Show that ϕ is an automorphism of $R[x, y]$.
- (16) Show that nilpotent elements of a ring R form an ideal. This ideal, denoted by $\text{nil}(R)$, is called the **nilradical** of R . Determine the nilradical of $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ and $R[x]$.
- (17) Show that all ideals of the power series ring $\mathbb{R}[[x]]$ are principal.
- (18) Let I and J be ideals of a ring R . The sum $I + J$ of I and J is defined by $I + J = \{x + y \mid x \in I, y \in J\}$. Show that $I + J$ is an ideal of R .
- (19) The product IJ of I and J is defined to be the set

$$IJ = \left\{ \sum_i x_i y_i \mid x_i \in I, y_i \in J \text{ for all } i \right\}.$$

Show that IJ is an ideal and $I \cap J \subseteq IJ$. Show by an example that IJ need not be equal to $I \cap J$.

Integral domains and quotient fields

- (20) Prove that a finite integral domain is a field.
- (21) Let R be an integral domain. Prove that units in the polynomial ring $R[x]$ are units of R .
- (22) Is there an integral domain containing exactly 10 elements?
- (23) Find the quotient field of the power series ring $\mathbb{R}[[x]]$.
- (24) Find integral domains among the rings $R = \mathbb{F}_5[x]/(x^2 + x + 1)$ and $S = \mathbb{F}_3[x]/(x^3 + x + 1)$.

Maximal ideals

- (25) Find maximal ideals of $\mathbb{Z}[x]$, $F[[x]]$ where F is a field.
- (26) Determine the maximal ideals of each of the rings: (a) $\mathbb{R} \times \mathbb{R}$ (b) $\mathbb{R}[x]/(x^2)$ (c) $\mathbb{R}[x]/(x^2 + x + 1)$.
- (27) Prove that $\mathfrak{m} = (x + y^2, y + x^2 + 2xy^2 + y^4) \subset \mathbb{C}[x, y]$ is a maximal ideal.
- (28) Consider the ideal $I = (y^2 + x^3 - 17)$ of $R = \mathbb{C}[x, y]$. Find generators of all maximal ideals in the quotient ring R/I .
- (29) Let M be an ideal of a ring R . Suppose that all the nonzero elements of $R \setminus M$ are units. Show that M is the only maximal ideal of R .

- (30) Let R be a commutative ring with identity in which $a^n = a$ for some $n \in \mathbb{N}$. Show that every prime ideal of R is a maximal ideal.

Algebraic Geometry

- (31) Suppose that $f, g \in \mathbb{C}[x, y]$ are quadratic polynomials such that no polynomial of positive degree is a common factor of f and g . Find the number of maximal ideals in $\mathbb{C}[x, y]/(f, g)$.
- (32) Let \mathbb{C} be a subring of a ring R and let R be a finite dimensional vector space over \mathbb{C} . Show that R has finitely many maximal ideals.
- (33) The zero set of a nonconstant polynomial in $\mathbb{C}[x, y]$ is either a point or has infinitely many points.
- (34) Show that every algebraic variety in \mathbb{C}^2 is the union of finitely many points and algebraic curves.
- (35) Determine the points of intersection of the algebraic curve $y^2 = x^3 - x^2$ with the line $y = \lambda x$.
- (36) Show that the locus of $y = \sin x$ does not lie on any algebraic curve.

UFDs, PIDs and Euclidean Domains

- (37) Let F be a field. Show that there are infinitely many monic irreducible polynomials in $F[x]$. Find all the irreducible elements of $R = F[[x]]$. Show that R is *UFD*.
- (38) Prove that every rational function in $\mathbb{C}(x)$ can be written as a sum of a polynomial and \mathbb{C} -linear combination of functions of the form $1/(x - a)^i$. Find a basis of $\mathbb{C}(x)$ as a \mathbb{C} -vector space.
- (39) Let F be a subfield of \mathbb{C} . Show that an irreducible polynomial in $F[x]$ has no multiple roots.
- (40) Show that $\mathbb{R}[x, y]$ and $\mathbb{Z}[x]$ are not *PIDs*.
- (41) Let $\omega = e^{2\pi i/3}$. Show that $\mathbb{Z}[w]$ and $\mathbb{Z}[\sqrt{-2}]$ are Euclidean domains.
- (42) Prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

Gauss's Lemma

- (43) Let $F = \mathbb{C}(x)$ and let $f, g \in \mathbb{C}[x, y]$. Prove that f and g have a common factor in $F[y]$ if and only if they also have a common factor in $\mathbb{C}[x, y]$.
- (44) Let $f \in \mathbb{C}[x, y]$ be an irreducible polynomial. Let $g \in \mathbb{C}[x, y]$. Show that if $Z(f) \subseteq Z(g)$ then $f|g$.
- (45) Prove that $f, g \in \mathbb{Z}[x]$ are relatively prime in $\mathbb{Q}[x]$ if and only if $(f, g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$.

- (46) Prove that $xy - zw$ is irreducible in $\mathbb{C}[x, y, z, w]$.

Factorization of Polynomials

- (47) Prove that the polynomials $f(x) = x^2 + 26x + 213$, $g(x) = 8x^3 - 6x + 1$ and $h(x) = x^5 = 3x^4 + 3$ are irreducible in $\mathbb{Q}[x]$.
- (48) Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and $\mathbb{F}_2[x]$.
- (49) Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$, when $p = 2, 3, 5$.
- (50) Let p be a prime number and A be an $n \times n$ integer matrix such that $A \neq I$ and $A^p = I$. Prove that $n \geq p - 1$.
- (51) Let $f(x)$ be a monic integer polynomial of positive degree having a rational root r . Show that r is an integer.
- (52) Find the number of monic irreducible quadratic polynomials in $\mathbb{F}_p[x]$.

The ring of Gaussian integers

- (53) Prove that every Gaussian prime divides exactly one integer prime.
- (54) Factor $30, 10, 1 - 3i$ into product of Gaussian primes.
- (55) Show that an integer prime p is a prime element of $\mathbb{Z}[\sqrt{3}]$ if and only if $x^2 - 3$ is irreducible in $\mathbb{F}_p[x]$.
- (56) Let $R = \mathbb{Z}[w]$ where $w = e^{2\pi i/3}$.
- Decompose 3 into irreducible factors in R .
 - Let $p \neq 3$ be a rational prime. Show that if $x^2 + x + 1$ has a root in \mathbb{F}_p , then $p \equiv 1 \pmod{3}$.
 - Show that (p) is a prime ideal of R if and only if $p \neq a^2 - ab + b^2$, for some integers a and b .

REFERENCES

- [1] M. Artin, *Algebra*, Prentice Hall of India, 1992.
- [2] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Wiley, 1999.
- [3] N. Jacobson, *Basic Algebra*, Vol. I, Second Edition, Freeman, 1985.
- [4] I. S. Luthar and I. B. S. Passi, *Algebra*, Vol 1-4, Narosa, 1997-2004.

DEPARTMENT OF MATHEMATICS, IIT BOMBAY, MUMBAI 400 076
E-mail address: jkv@math.iitb.ac.in