People's Democratic Republic of Algeria

Ministry of higher Education and Scientific

Research

Higher Normal School of Tecnological Education

Skikda

Departement of Mathematics

Dissertation

Presented to obtain a degree in Mathematics as a teacher of middle school

Entitled

Ring Theory

Presented by :

Rahal Kawther

Ziadi Rayene

Board of Examiners :

Supervisor: FerragAzouz	MCB	ENSET SKIKDA
Chairwoman: Mziri Imane	MCB	ENSET SKIKDA
Examiner: Ayach Mosaab	MAA	ENSET SKIKDA
Examiner: Gouassmia Okba	MCB	ENSET SKIKDA

June's session 2024

Acknowledgments

In the name of Allah, the Most Gracious, the Most Merciful, I dedicate this thesis with profound gratitude and thanks to Allah for His countless blessings and for granting me the strength and guidance to complete this work.

For my dad, who taught me the love of stories, and my mom, who lived them. To my parents, who planted the seed of knowledge in my mind and nurtured it. For Mom and Dad, who always reminded me that words have the power to change the world.

I extend my deepest appreciation to my beloved parents whose unwavering support, constant belief in my abilities, prayers, and encouragement have been the cornerstone of my success. Their sacrifices and love have been instrumental in my academic journey.

To my dear siblings : Abd el Fattah, Ikram, Roukaya, Abd el Djalil, Yahya, I extend my gratitude. You have been a source of inspiration and motivation. thank you for your constant encouragement, patience, and understanding. Your support have been invaluable to me.

I would like to write to all those who have contributed to the completition of this work. A special thanks goes to our supervisor, Mr. Azzouz Ferrag, for his advices, comments, helpful informations, and exeptional patience throughout this year. His immense knowledge and profound experience has enabled us to complete this research sucssusfully. It is my honor to work with him.

Additionally, I would like to express my sincere gratitude to my freind and my partner in this work Ziadi Rayen, for her collaboration, help, and efforts. Her hard work have been crucial to the sucsses of this project.

I am also profoundly grateful to my esteemed proffessors and teachers, whose wisdom, knowledge, invaluable guidance, and insightful feedback have contributed to my growth and sucsses. Their dedication and expertise have been pivotal in shaping my academic and professional path.

To my mathematics teachers at secondary school: Mrs. Mekhannia Warda and Mr. Merrikhy Mohammed Lamin, my role model and idol, the best teachers and the greatest humans. I would like to thank you infinitely for your commitement to education. I hope to become a sucssesful teacher like you.

Last but not least, to those who participated to help me fulfill my dreams and be where I am today.

I stand to express my profound gratitude for them, even those whose names my pen has not mentioned. Every unspoken moment of support and every silent word of motivation has had a significiant impact in my deep hard.

Names may not be engraved on paper, but your imprints are etched in my memory.

Within all thanks and appreciation, KAWTHER.

In the name of Allah, the Most Gracious, the Most Merciful, I dedicate this thesis with profound gratitude and thanks to Allah for His countless blessings and for granting me the strength and guidance to complete this work.

As I stand here on the precipice of a new chapter in my life, I cannot help but reflect on the incredible journey that has brought me to this moment. Today is not just a celebration of my achievements, but a testament to the unwavering support, love, and guidance of those who have stood by my side through every triumph and challenge.

First and foremost, I want to dedicate this milestone to my beloved father, **Toufik**, whose wisdom, strength, and sacrifices have been the cornerstone of my journey. Your unwavering belief in me has been my guiding light, and I carry your values and teachings with me as I embark on this new adventure.

To my mother, **Nadjette**, whose boundless love, resilience, and selflessness have shaped me into the person I am today. Your endless sacrifices and unwavering encouragement have been my source of strength, and I am endlessly grateful for your presence in my life.

Though they may no longer be with us in body, I carry the cherished memories and enduring love of my dear grandmother **Lekhal Hada** and my grandfather **Slim Rebai** in my heart always. Their legacy of love, kindness, and perseverance continues to inspire me each day.

To my big brother, **Hamid** who ventured afar to Canada, your presence and support, though miles apart, have always felt close to home. Your belief in my abilities and your encouragement have fueled my determination to reach for the stars.

I also want to take a moment to recognize my uncle **Slim Bilel** and my cousin **Ziadi Saloua**, who have been a constant source of encouragement and support from afar. Though miles may separate us, your love knows no bounds, and I am endlessly grateful for your unwavering belief in me.

To my twin, **Nihel**, who has been my partner in every adventure, your presence in my life is a constant reminder of the strength that comes from shared experiences and unbreakable bonds.

To my younger siblings, **Yacine** and **Bayene**, your laughter, innocence, and endless love have brought light into my life even on the darkest of days. I am endlessly proud to be your sibling, and I carry your dreams and aspirations alongside mine.

To my extended family, cousins, aunts specially **Dorsaf** and **Sabrina** and uncles, your love, encouragement, and shared laughter have made every moment of this journey richer and more meaningful. I am grateful for the sense of belonging and support that you have always provided.

I would like to write to all those who have contributed to the completition of this work. A special thanks goes to our supervisor, **Mr. Azzouz Ferrag**, for his advices, comments, helpful informations, and exeptional patience throughout this year. His immense knowledge and profound experience has enabled us to complete this research sucssusfully. It is my honor to work with him.

To my partner, **Rahal Kawther**, your unwavering love, understanding, and support have been my rock through every challenge and triumph. Your belief in me has given me the courage to pursue my dreams fearlessly, and I am endlessly grateful for your presence in my life.

And finally, to my best friends, **Mourakeb Yousra**, **Siad Safa**, **Labiod Amina**, **Chebira Hind**, **Lina**, **Chahed**, **Khansaa**, **Ikram** and **Oumaima**, your laughter, companionship, and unwavering support have been the highlight of my journey. Your friendship is a gift that I treasure deeply, and I am grateful for the countless memories we have shared.

As I step into the next chapter of my life, I carry each of you in my heart, knowing that your love, support, and guidance will continue to light my path. Today is not just my graduation, but a celebration of the village that has raised me, and for that, I am eternally grateful.
With love and gratitude. RAYENE.

ملخص المذكرة

في هذا العمل سنتطرق إلى المفاهيم الأساسية للحلقات و المثاليات في الجبر المجرد.
بداية سنقدم تعريفا للحلقة و بعضا من خصائصها، بما في ذلك الحلقة التبديلية ذات العنصر الواحدي. تتناول الدراسة بعد ذلك المثاليات، و هي الهياكل الفرعية التي تلعب دورا حيويا في نظرية الحلقات. بعد ذلك سنستعرض بعض أشهر و أهم أنواع الحلقات.
سوف نقوم بتسليط الضوء على حلقة كثيرات الحدود باعتبارها كائنا مركزيا في الجبر، حيث سنهتم بدراسة البنى و الخصائص و العمليات داخلها.
كما سنقدم في هذا العمل بعض النظريات و الأمثلة لتوضيح النتائج النظرية.
الكلمات المفتاحية: حلقة، مثالي، حلقة كثير حدود ، حقل.

Abstract

In this work, we will explore the fondamental concepts of rings and ideals in abstract algebra.
It begins with the definition and properties of rings, including commutative rings with unity. The study then delves into ideals, substructures that play a crucial role in ring theory.
After that, we will introduce some of the most famous classes of rings.
A significiant portion is dedicated to the polynomial ring, a central object in algebra. We will discuss about the properties , constraction, and operations within this last. The study includes some essencial theorems and examples to illustrate the theorical findings.
Key words: ring, ideal, polynomial ring, field.

Résumé

Ce mémoire explore les concept fondamentaux des anneaux et des idéaux en algèbre abstraite.
Il commence par la définition et les propriétés des anneaux, y compris les anneaux commutatifs avec unité. L'étude se penche ensuite sur les idéaux, des sous-structures jouant un rôle crucial dans la théorie de anneaux.
Après cela, nous présenterons quelques-uns des types d'anneaux les plus célèbres.
Une partie significative est dédiée à l'anneau des polynômes, un objet central en algèbre.
Nous discutons sur les propriétés, construction, et opérations au sein de ces derniers.
L'étude contient également quelques exemples et théorèmes pour illustrer les résultats théoriques.
Mots clés: anneau, idéal, anneau de polynôme, corps.

Contents

Some notations will be used throughout this final dissertation that we list below:

- $\mathbb{N}$: The set of nature numbers.
- $\mathbb{Z}$: The set of integer numbers.
- $\mathbb{Q}$: The set quotiont numbers.
- $\mathbb{R}$: The set of real numbers.
- $\mathbb{C}$: The set of complex numbers.
- $\mathbb{Z}_n$: The cyclic ring of order n.
- M_n : The set of all $n \times n$ matrices.
- ϕ : The empty set.
- $a \in A$: a is an element of the set A.
- $A \subseteq B$: The set A is a subset of the set B.
- $A \subset B$: The set A is a proper subset of the set B.
- $A \cup B$: The union of the sets A and B.
- $A \cap B$: The intersection of the sets A and B.
- $A \backslash B$: $\{a \in A, a \notin B\}$ where A and B are sets.
- $R[x]$: The polynomial ring witk coefficient in the ring R.
- $R \leq S$: R is a subgroup (subring) of S.
- $R \cong S$: The rings R and S are isomorphic.
- $a \mid b$: The element a devides the element b.
- A/B : $\{a/b,\, a \in A,\, b \in B\}$.
- $R \trianglelefteq S$: The ring R is cyclic in S.

I Introduction

The origins of algebra are usually traced back to Muhammad ben Musa al-Khawarizmi, who worked at court of the Caliph al-Ma'mun in Baghdad in the early 9^{th} Centry. The word drives from the Arabic al-jabr, which refers to the process of adding the same quantity to both sides of an equation. The work of arabic scholars was known in Italy by the 13^{th} century, and a lively school of algebraists arose there. Much of their work was concerned with the solution of polynominal equations.

This preoccupation of mathematicians lasted until the beginning of the 19^{th} century, in the work of Joseph Louis Lagrange (1736-1813), Paulo Ruffini (1765-1822), and Evariste Galois (1811-1832) on the theory of algebric equations. Their group consisted of permutations of the variables of the roots of polynomials, and indeed for much of the ninteeth centrury all groups were finite permutation groups. Nevertheless many of the fundamental ideas of group theory were introduced by these early workers and their successors, Augustin Louis Cauchy (1789-1857), Ludwig Sylow (1832-1918), Camille Jordan(1838-1922) among others.

These works led to the intoduction of some of the main structures of modern abstract algebra, rings and fields. These structures have been intensively studied over the past two hundred years.

Until quite recently, algebra was very much the domain of the pure mathematics; applications were few and far between. But all this has changed as a result of the rise of information technology, where the precision and power inherent in the language and concepts of algebra gave proved to be invaluable. Today specialists in computer science and engineering, as well as physics and chemistry, routinely take courses in abstract algebra.

Ring theory is a branch of abstract algebra that studies algebraic structures called rings. Rings generalize many fundamental concepts from arithmetic and algebra, providing a framework to understand properties of numbers and algebraic systems beyond the familiar integers and real numbers.

The study of rings encompasses a diverse array of structures, ranging from familiar number systems like integers and polynomials to more abstract constructs such as matrices and functions. Rings serve as a fundamental tool in various branches of mathematics, including algebraic geometry, number theory, and representation theory, providing powerful methods to analyze and solve problems in these fields.

Key concepts in ring theory include ideals, subrings, homomorphisms, and quotient rings, each playing a crucial role in understanding the structure and behavior of rings. Furthermore, ring theory often intersects with other areas of mathematics, such as group theory and field theory, leading to fruitful connections and applications in diverse mathematical contexts.

Overall, ring theory provides a rich framework for exploring algebraic structures and uncovering deep connections between seemingly disparate mathematical concepts, making it a fundamental area of study with wide-ranging applications in both pure and applied mathematics.

In this research, will be our main focus:
The first chapter is intended as an introduction to the meaning of the Group and Ring with few examples, and some basic properties. After that we got onto the definition of homomorphism and ideal, introducing some operations on this last, then moving to quotient ring .
The second chapter speaks principally about some special classes of rings with more details. Within the realm of rings, there are various classes that arise, such as commutative rings, integral domains, fields, etc. Each class has its own defining properties, which can greatly influence the behavior of elements within the ring. Also we talk about the relationship between them .
The last chapter introduces specific type of rings wich is polynomial ring. Polynomial rings extend the concept of polynomials over a field or a ring, understanding their properties, such as irreducibility and factorization is essential for many applications, giving some important properties and theorems.

II Ring

II.1 Inroduction to ring theory

II.1.1 Binary operations

Definition II.1.1 *[1]*
A binary operation on a set is a rule for combining two elements of the set. More precisely, if S is a nonempty set, a binary operation on S is a function $\alpha : S \times S$.

Thus α associates with each ordred pair (x, y) of elements of S an element $\alpha(x, y)$ of S. It is better notation to write $x \circ y$ for $\alpha(x, y)$, referring to "$\circ$ "as the binary operation.

II.1.2 Semigroups

Definition II.1.2 *[1]*
If $\circ$ is associative, that is, if $(x \circ y) \circ z = x \circ (y \circ z)$ is valid for all x, y, z in S, the pair $(S, \circ)$ is called a semigroup.

II.1.3 Groups

Here we are concerned with a very special type of semigroup.

Definition II.1.3 *[1]*
A semigroup $(G, \circ)$ is called a group if it has the following properties.

1. *There exists in G an element e, called a right identity, such that $x \circ e = x$ for all x in G.*
2. *To each element x of G there corresponds an element y of G, called a right inverse of x, such that $x \circ y = e$.*

If the group operation is commutative, that is, if $x \circ y = y \circ x$ is always valid, the group $(G, \circ)$ is called abelian.

Remark II.1.1

1. *While it is clear how to define left identity and left inverse, the existence of such elements is not presupposed; indeed this is a consequence of the group axioms.*
2. *It is customary not to distinguish between the group $(G, \circ)$ and its underlying set G provided there is no possibility of confusion as to the intended group operation. However it should be borne in mind that there are usually several possible group operations on a given set.*

Example II.1.1
$(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are commutative groups.

Notation II.1.1
The operation $(+)$ could refer to any binary operations, not necessarly "simple addition".

II.1.4 Ring

Definition II.1.4 *[2]*
A ring is a set R together with two operations on R called addition $((a, b) \longmapsto a + b)$ and multiplication $((a, b) \longmapsto ab)$ such that the following axioms are satisfied :

(i) $(a + b) + c = a + (b + c)$ *for all $a, b, c \in R$. (addition is associative).*

(ii) *There is an element $0 \in R$ such that $a + 0 = 0 + a = a$ for all $a \in R$. (there is a zero element).*

(iii) *For each $a \in R$ There is $b \in R$ such that $a + b = b + a = 0$. (each element has a negative).*

(iv) $a + b = b + a$ *for all $a, b \in R$. (addition is commutative).*

(v) $(ab)c = a(bc)$, $\forall a, b, c \in R$. *(multiplication is associative).*

(vi) $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$, $\forall a, b, c \in R$. *(both destributive laws hold).*

Examples II.1.1

(1). $(\mathbb{R}, +, .)$

(2). $(\mathbb{Z}, +, .)$

(3). $(Mat(2, \mathbb{R}), +, .)$

(4). $(2\mathbb{Z}, +, .)$

(5). $(\mathbb{R}[X], +, .)$

Definition II.1.5 *[2]*
A commutative ring is a ring wich satisfies

$$ab = ba, \ \forall a, b \in R.$$

Definition II.1.6 *[2]*
If R is a ring, an element $e \in R$ is called an identity if

$$ea = ae = a, \ \forall a \in R.$$

Notation II.1.2
we will almost always use the symbol $'1'$ rather than $'e'$ to denote an identity element. Not all rings have identity element, for example: $2\mathbb{Z}$ does not have one .

Example II.1.2
R is the set of integers mod 7 under the addition and miltiplication mod 7 . that is the elements of R are the seven symbols $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$, where:

1. *$\bar{i} + \bar{j} = \bar{k}$ where k is the remainder of $i + j$ on division by 7 (thus, for instance, $\bar{4} + \bar{5} = \bar{2}$ since $4 + 5 = 9$, which, when divided by 7, leaves a remainder of 2)*
2. *$\bar{i}.\bar{j} = \bar{m}$ where m is the remainder of i.j on devision by 7 (thus, $\bar{5}.\bar{3} = \bar{1}$ since $5 \times 3 = 15$ has 1 as remainder on devision by 7).*
   This ring is commutative.

Examples II.1.2 *The following rings are commutative.*

1. $(\mathbb{R}, +, .)$.
2. $(\mathbb{Z}, +, .)$.
3. $(2\mathbb{Z}, +, .)$.
4. $(\mathbb{R}[X], +, .)$.

Theorem II.1.1 *Let R be any ring and $a, b, c \in R$:*

1. *If $a + b = a + c$ then, $b = c$.*
2. $-(a + b) = (-a) + (-b)$.
3. $-(-a) = a$.
4. $a.0 = 0.a = 0$.
5. $a(-b) = -(ab) = (-a)b$.
6. $(-a)(-b) = (ab)$.
7. $a(b - c) = ab - ac$.
8. $-1(a) = -a$.
9. $-1 \times -1 = -1$.

Proof II.1.1
1. Assuming that $a+b=a+c$, then, we have:

$$\begin{aligned}(-a)+(a+b) &= (-a)+(a+c)\\ ((-a)+a)+b &= ((-a)+a)+c\\ 0+b &= 0+c\\ b &= c.\end{aligned}$$

2. In view of uniqueness of negatives it is sufficient to prove that $(-a)+(-b)$ is a negative of $a+b$, that is, it is sufficient to prove that

$$((-a)+(-b)(a+b)=0=(a+b)+((-a)+(-b).$$

Furthermore, if we prove only the first of these equations, the other will follow as a consequence of Axiom (iv) in the definition of ring, but use of the first four axioms readily gives:

$$\begin{aligned}((-a)+(-b)+(a+b) &= (-a)+((-b)+(a+b))\\ &= (-a)+((-b)+(b+a))\\ &= (-a)+(((-b)+b)+a)\\ &= (-a)+(0+a)\\ &= (-a)+a\\ &= 0.\end{aligned}$$

3. By the definition, a negative of $(-a)$ is an element b wich satisfies $(-a)+b=0=b+(-a)$. But these equations are satisfied if we put $b=a$; so it follows that a is a negative of $-a$. Since negatives are unique we have poved that $-(-a)=a$.
4.

$$\begin{aligned}a0 &= a(0+0)\\ &= a0+a0.\end{aligned}$$

and since R is a group under addition, this equation implies that $a0=0$.
Similarly,

$$\begin{aligned}0a &= (0+0)a\\ &= 0a+0a.\end{aligned}$$

using the left distributive law, and so here too, $0a=0$ follows.
5. In order to show that $a(-b)=-(ab)=(-a)b$ we must demonstrate that $ab+a(-b)=0$. We have:

$$\begin{aligned}ab+a(-b) &= a(b+(-b))\\ &= a0\\ &= 0\end{aligned}$$

By use of the destributive law and the result of part 4 *of this theorem, similarly* $(-a)b = a(-b)$.
6. That $(-a)(-b) = ab$ *is a really special case of part 5, we single it out since its analog in the case of real numbers has been so stressed in our early education. So on with it:*

$$\begin{aligned}(-a)(-b) =& -(a(-b))\\ =& -(-(ab))\\ =& ab.\end{aligned}$$

7.By using the destributive law, we find that: $a(b+c) = ab + ac$.
We change c by $(-c)$*; we find:* $a(b + (-c)) = ab + a(-c)$.
And using the previous property, we find: $a(b - c) = ab - ac$.
8. Supposing that R has a unit element 1, *then,*

$$\begin{aligned}a + (-1)a =& 1a + (-1)a\\ =& (1 + (-1))a\\ =& 0a\\ =& 0.\end{aligned}$$

so, $(-1)a = -a$.
9. In particular, if $a = -1$ *we find* $(-1)(-1) = -(-1) = 1$. □

Direct product of rings

We suppose that $R, \cdots, R_n$ are rings. Then,
the set $R_1 \times \cdots \times R_n = \{(r_1, \cdots, r_n),\ r_1 \in R_1, \cdots, r_n \in R_n\}$ with operations:

$$(r_1, \cdots r_n) + (r'_1, \cdots, r'n) = (r_1 + r'_1, \cdots, r_n + r'_n)$$

$$(r_1, \cdots, r_n).(r'_1, \cdots, r'_n) = (r_1.r'1, \cdots, r_n.r'_n)$$

is a ring, and it is called the direct product of R_i. We notice that the operations in the i^{th} composent are done in R_i.

Example II.1.3 *We want to compute* $(2,2).(3,3)$ *in* $\mathbb{Z}_5 \times \mathbb{Z}_6$.
We notice that $2.3 = 1$ *in* $\mathbb{Z}_5$ *and* $2.3 = 0$ *in* $\mathbb{Z}_6$. *Hence we have* $(2,2).(3,3) = (1,0)$ *in* $\mathbb{Z}_5 \times \mathbb{Z}_6$.

II.2 Subring

Definition II.2.1 *[2]*
If R is a ring and S is a subset of R, we will say that S is a subring if:

1. *S is a subgroup of R under $(+)$.*
2. *S is closed under multiplication.*
3. $1 \in S$.

Examples II.2.1

* $2\mathbb{Z} \leq \mathbb{Z}$.
* $(\mathbb{Z}, +, .) \leq (\mathbb{R}, +, .)$.
*

$$S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} a, b, c \in \mathbb{Z} \right\}.$$

is a subring of $Mat(2, \mathbb{Z})$.
1). $S \neq \phi$; since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$.
2). Let $\alpha = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and $\beta = \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$ be arbitrary elements of S. Then,

$$\alpha + \beta = \begin{pmatrix} a+d & b+e \\ 0 & c+f \end{pmatrix} \in S,$$
$$\alpha\beta = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in S,$$
$$-\alpha = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} \in S.$$

Hence, the closure properties hold.

Remark II.2.1
Each ring is itself subring (the proof is very easy) .

II.3 Ring homomorphisms

Definition II.3.1 *[3]*
Let R and R' be rings. A mapping $\phi : R \longrightarrow R'$ is said to be homorphism if:
(a) $\forall x, y \in R$, $\phi(x+y) = \phi(x) + \phi(y)$.
(b) $\forall x, y \in R$, $\phi(xy) = \phi(x)\phi(y)$.
Usually, we require that if R and R' are rings with 1, then,
(c) $f(1_R) = 1_{R'}$.

Example II.3.1 *Let*

$$\begin{aligned} \theta : \mathbb{C} &\longrightarrow Mat(2, \mathbb{R}) \\ (a+bi) &\longrightarrow \theta(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \end{aligned}$$

defines a map.
Since we have:

$$\begin{aligned} \theta((a+bi)+(c+di)) &= \theta((a+c)+(b+d)i) \\ &= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= \theta(a+bi) + \theta(c+di). \end{aligned}$$

$$\begin{aligned} \theta((a+bi)(c+di)) &= \theta((ac-bd)+(ad+bc)i) \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= \theta(a+bi)\theta(c+di). \end{aligned}$$

It follows that θ is a homomorphism.

Theorem II.3.1 *Let R and S be two rings and let the homomorphism $\phi : R \mapsto S$, then:*
1. $\phi(0_R) = 0_S$.
2. $\phi(-a) = -\phi(a)$, $\forall a \in R$.

Proof II.3.1
1.

$$\begin{aligned}\phi(0_R) =& \phi(0+0)\\ =& \phi(0)+\phi(0)\\ =& 0_S.\end{aligned}$$

2. By 1.

$$\begin{aligned}0 =& \phi(0)\\ =& \phi(r+(-r)), \forall r \in R\\ =& \phi(r)+\phi(-r).\end{aligned}$$

But this says that $\phi(-r)$ is the additive inverse of $\phi(r)$, i.e. $\phi(-r) = -\phi(r)$. □

Theorem II.3.2
Let R, S and T be rings and let $f : R \longrightarrow S$ and $g : S \longrightarrow T$ be ring maps. Then, the composite $gof : R \longrightarrow T$ is a ring homomorphism.

Proof II.3.2 *Let $x, y \in R$. Then:*

$$\begin{aligned}(g.f)(x+y) =& g(f(x+y))\\ =& g(f(x)+f(y))\\ =& g(f(x))+g(f(y))\\ =& (g.f)(x)+(g.f)(y).\end{aligned}$$

$$\begin{aligned}(g.f)(x.y) =& g(f(x.y))\\ =& g(f(x).f(y))\\ =& g(f(x)).g(f(y))\\ =& (g.f)(x).(g.f)(y).\end{aligned}$$

In addition, if R, S, and T are rings with identity, then:

$$\begin{aligned}(g.f)(1_R) =& g(f(1_R))\\ =& g(1_S)\\ =& 1_T.\end{aligned}$$

Therefore $g.f$ is a ring homomorphism. □

Definition II.3.2 *[2]*
Let R and S be two rings.
A ring homomorphism which is bijective called an isomorphism. If there exists an isomorphism $\theta : R \longrightarrow S$ then, R and S are said to be isomorphic, and we write $'R \cong S'$.

Notation II.3.1
Let $f : A \mapsto B$ be a ring homomorphism.
f ENDOMORPHISM $\Leftrightarrow$ f surjection.
f MONOMORPHISM $\Leftrightarrow$ f injection.
f ISOMORPHISM $\Leftrightarrow$ f bijection.
f AUTOMORPHISM $\Leftrightarrow$ f bijective and $B = A$.

Kernel and image of a ring homomorphism

Let R and S be two rings and let the map $f : R \mapsto S$,

1. $\mathbf{ker(f)} = \{x \in R,\ f(x) = 0_S\}$.
2. $\mathbf{Im(f)} = \{f(x),\ x \in R\}$.

II.4 Ideals

Definition II.4.1 *[3]*
A nonempty subset U of R is said to be (a two sided) ideal of R if :
1. U is a subgroup of R.
2. $\forall u \in U, \forall r \in R$; both ru and ur are in U.
Condition 2 asserts that U "swallows up" multiplication from the right and left by arbitrary ring elements. For this reason U is usually called a two-sided ideal.

Example II.4.1
The set

$$T = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \quad a \in \mathbb{Z} \right\}$$

is an ideal of the ring

$$S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} a, b, c \in \mathbb{Z} \right\}.$$

1).Clearly $T \neq \phi$, since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$.
2). Let $x, y \in T$ and $r \in S$. Then, for some integers $a, b, c, d, e \in \mathbb{Z}$:
$x = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ $y = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ $r = \begin{pmatrix} c & d \\ 0 & e \end{pmatrix}$
giving

$$x+y=\begin{pmatrix} 0 & a+b \\ 0 & 0 \end{pmatrix} \qquad rx=\begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix}$$
$$-x=\begin{pmatrix} 0 & -a \\ 0 & 0 \end{pmatrix} \qquad xr=\begin{pmatrix} 0 & ae \\ 0 & 0 \end{pmatrix}$$

and since these are all in T, it follows that T is an ideal of S.

Remark II.4.1

1. *What is the difference between a subring and an ideal?*
   The answer: subring must be closed under multiplication of elements in the subring.
   An ideal must be closed under multiplication of an element in the ideal by any element in the ring.

2. *If R is commutative, then $rb = br$, so we only need to check that one of $rb, br \in S$.*
   In the commutative case, there is no difference between left ideals, right ideals, and two-sided ideals.

Lemma II.4.1
Let R be a ring. Then R and $\{0\}$ are ideals.

Proof II.4.1
R is a group under addition, and as such we know that R (the whole group) and $\{0\}$ (the set consisting of the identity) are subgroups of R. Thus, they are both closed under addition, contain 0, and are closed under taking additive inverses.
For R, if $x \in R$ and $r \in R$, then, $xr, rx \in R$. (Because R is closed under multiplication). Therefore, R is an ideal.
For $\{0\}$, we take $0 \in \{0\}$, and $r \in R$. Then,

$$r.0 = 0 \in \{0\} \text{ and } 0.r = 0 \in \{0\}.$$

Therefore, $\{0\}$ is an ideal. □

Operations on ideals

Let R be a commutative ring with a unit.
(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 ideals 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 $I + J = \{a + b,\ a \in I, b \in J\}$.
(3) The product of I and J, denoted by I.J is the ideal generated by elements of the type ab where $a \in I$ and $b \in J$. Therefore

$$I.J = a_1b_1 + a_2b_2 + \cdots + a_nb_n,\ a_1, a_2, \cdots, a_n \in I,\ b_1, b_2, \cdots, b_n \in J.$$

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

II.4.1 Quotient ring

Definition II.4.2 *[3]*
Let R be a ring, and let I be a (two sided) ideal. Considering just the operation of addition, R is a group and I is a subgroup. In fact, since R is an abelian group under addition. I is a normal subgroup, and the quotient group R/I is defined. Addition of cosets is defined by adding coset representatives:

$$(a + I) + (b + I) = (a + b) + I.$$

The Zero coset is $0 + I = I$, *and the additive inverse of a coset is given by* $-(a + I) = (-a) + I$. *However, R also comes with a multiplying coset representatives:*

$$(a + I).(b + I) = ab + I.$$

We need to check that this operation is well defined, and that it depends on the fact that I is an ideal. Specifically, it depends on the fact that I is closed under multipliction by elements of R. By the way, we will sometimes write $\frac{R}{I}$ *and sometimes we write* R/I, *they mean the same thing.*

Theorem II.4.1
If I is a two sided ideal in a ring R, then R/I *has the structure of a ring under coset addition and multiplication.*

Proof II.4.2
Supposing that I is a two-sided ideal in R. Let $r, s \in I$ *. Coset addition is well-defined, because R is an abelian group and I a normal subgroup under addition. we proved that coset addition was well-defined when we constructed quotient groups. we need to show that coset multiplication is well-defined:*

$$(r + I)(s + I) = rs + I.$$

As before, supposing that;

$$r + I = r' + I,\ so,\ r = r' + a,\ a \in I.$$
$$s + I = s' + I,\ so,\ s = s' + b,\ b \in I.$$

Then,

$$\begin{aligned}(r+I)(s+I) =& rs+I\\ =&(r'+a)(s'+b)+I\\ =&r's'+r'b+as'+ab+I\\ =&r's'+I\\ =&(r'+I)(s'+I).\end{aligned}$$

The next-to-last equality is derived as follows: $r'b+as'+ab \in I$, because I is an ideal. hence, $r'b+as'+ab+I=I$.
Noting that this uses the multiplication axiom for an ideal; in a sense, it explains why the multiplication axiom requires that an ideal be closed under multiplication by ring elements on the left and right. □

Definition II.4.3 *[3]*
If R is a ring and I is a two-sided ideal, the quotient ring of R mod I is the group of cosets $\frac{R}{I}$ with the operations of coset addition and coset multiplication.

Proposition II.4.1
Let R be a ring, and let I be an ideal:
(a) If R is a commutative ring, so is R/I.
(b)) If R has a multiplicative identity 1. then $1+I$ is a multiplicative identity for R/I. In this case, if $r \in R$ is a unit, then so is $r+I$, and $(r+I)^{-1}=r^{-1}+I$.

Proof II.4.3
(a) Let $r+I, s+I \in R/I$. Since R is commutative.

$$(r+I)(s+I)=rs+I=sr+I=(s+I)(r+I).$$

Therefore, R/I is commutative.
(b) Suppose R has a multiplicative identity 1. Let $r \in R$. Then

$$(r+I)(1+I)=r1+I=r+I \text{ and } (1+I)(r+I)=1r+I=r+I.$$

Therefore, $1+I$ is the identity of R/I.
If $r \in R$ is a unit. Then,

$$(r^{-1}+I)(r+I)=r^{-1}r+I=1+I \text{ and } (r+I)(r^{-1}+I)=r^{-1}+I=1+I.$$

Therefore, $(r+I)^{-1}=r^{-1}+I$.
□

Example II.4.2
The set of even integers $\langle 2\rangle = 2\mathbb{Z}$ is an ideal in $\mathbb{Z}$. Form the quotient ring $\mathbb{Z}/2\mathbb{Z}$.

Theorem II.4.2
Let R and S be rings and let $\phi : R \longrightarrow S$ be an homomorphisme. Then:

1. *The kernel of ϕ is an ideal of R.*
2. *The image of ϕ is a subring of S.*
3. *The application*

$$\begin{aligned} \varphi : R|ker\phi &\longrightarrow Im\phi \subset S \\ r + ker\phi &\longrightarrow \phi(r) \end{aligned}$$

is a well-defined isomorphism.

Proof II.4.4
The image of ϕ is a subring.
Let us prove that ker ϕ is an ideal. We know that $\phi(0) = 0$, so, $0 \in ker\phi$ and hence, the kernel is nonempty. Let $a, b \in ker\phi$ and let $r \in R$. Then since ϕ is a homomorphism we have:

$$\begin{aligned} \phi(a+b) = \phi(a) + \phi(b) = 0 + 0 = 0. \\ \phi(ra) = \phi(r).\phi(a) = \phi(r).0 = 0. \\ \phi(ar) = \phi(a).\phi(r) = 0.\phi(r) = 0. \end{aligned}$$

Thus, $a + b, ra$, and ar are in $ker\phi$ and so $ker\phi$ is an ideal.
Consider the application φ. We first show that it is well-defined. Let $r, r' \in R$ be such that $r - r' \in ker\phi$, i.e, such that $r + ker\phi = r' + ker\phi$. Then,

$$\phi(r) = \phi(r' + (r - r')) = \phi(r') + \phi(r - r') = \phi(r') + 0 = \phi(r').$$

So φ is well defined . Let $r_1 + I \in R/I$. Then since ϕ is an homomorphism we have :

$$\begin{aligned} \varphi(r_1 + I + r_2 + I) &= \varphi(r_1 + r_2 + I) \\ &= \varphi(r_1) + \varphi(r_2) \\ &= \varphi(r_1 + I) + \varphi(r_2 + I). \end{aligned}$$

and we have

$$\begin{aligned} \varphi((r_1 + I)(r_2 + I)) &= \varphi(r_1 r_2 + I) \\ &= \varphi(r_1 r_2) \\ &= \varphi(r_1)\varphi(r_2) \\ &= \varphi(r_1 + I)\varphi(r_2 + I). \end{aligned}$$

we have also $\varphi(1 + I) = \varphi(1) = 1$. Therefore φ is a homomorphism. Let us prove that φ is bijective. If $r + ker\phi \in ker\varphi$, then $\varphi(r + I) = \phi(r) = 0$ and so $r \in ker\phi$ or equivalently $r + ker\phi = ker\phi$. Thus $ker\phi$ is trivial and so ϕ is injective. Let $s \in Im\phi$. Then there exists an $r \in R$ such that $\phi(r) = s$ or equivalently that $\varphi(r + \ker\phi) = s$. Thus $s \in Im\varphi$ and so φ is surjective. Hence φ is an isomorphism as desired. □

Lemma II.4.2
Supposing $f : R_1 \mapsto R_2$ is a ring homomorphism. Then, **ker f** *is a subring of R_1 and* **Im** *is a subring of R_2.*
Moreover, for every $a \in A$ and $x \in$ **ker f**, *we have that ax and xa are in* **ker f**.

Proof II.4.5 *From group theory, we know that* **ker f** *and* **Im f** *are additive subgroups. It is enough to show that they are closed under multiplication. We show a stronger result for* **ker f**, *and we will come back to this property when we define an ideal of a ring.*
For every $a \in$ **ker f** *and every $a' \in R_1$, we have*

$$f(a.a') = f(a).f(a') = 0.f(a') = 0.$$

and so $a, a' \in$ **ker f**. *For every $b, b' \in$* **Im f**, *there are $a, a' \in R_1$ such that $b = f(a)$ and $b' = f(a')$.*
Therefore, $b.b' = f(a).f(a') = f(a.a') \in$ **Im f**. □

Remark II.4.2
1. If $\theta : R \mapsto S$ is a homomorphism with $\ker \theta = I$ then θ maps two elements of R to the same element of $im\theta \subseteq S$ if and only if the two given elements of R differ by an element of I. Since factoring out I amounts to regarding two elements of R as equal if and only if they differ by an element of I, this means that each element of $im\theta$ corresponds to just one element of R/I. So the homomorphism $R \mapsto im\theta$ becomes an isomorphism $R/I \mapsto im\theta$.
2. For any ring R the identity map $\psi : R \mapsto R$ (given by $\psi(x) = x$ for all $x \in R$) is a homomorphism. Clearly $ker\psi = \{0\}$ and $im\psi = R$, and so the Fundamental Homomorphism Theorem says that $R/0 \cong R$. The isomorphism guaranteed by 1. is $\{0\} + a \mapsto \psi(a) = a$.
3. For any rings R and S the zero map $R \mapsto S$, defined by $x \mapsto 0_S$ (for all $x \in R$, is a homomorphism. Its kernel is the whole of R and its image is the zero subring of S. By 1.

$$R/R \cong \{0\}.$$

(We note that R/R has just one element, since $R + x = R$, $\forall x \in R$).

Theorem II.4.3 (**Homomorphism Theorems**).
Let $f : R \mapsto S$ be a surjective ring homomorphism with kernel K.
(1) **The First Homomorphism Theorem** (**TheFundamental Theorem**).
The map

$$\begin{aligned} \bar{f} : R/K &\mapsto S \\ \bar{r} &\mapsto \bar{f}(\bar{r}) = f(r),\ r \in S. \end{aligned}$$

is an isomorphism.
(2) **The Second Homomorphism Theorem**.
There is a 1-1 correspondence between the sets:

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

given by $f^{-1}(J) = J$. 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, $R/f^{-1}(J) \backsimeq S/J$. In particular, if $I \subset K$ are ideals of R, then, $(R/K)/(I/K) \backsimeq R/I$.

Proof II.4.6
(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 the map

$$\begin{aligned} \pi : S &\mapsto S/J \\ s &\mapsto \pi(s) = \bar{s}. \end{aligned}$$

Considering the ring homomorphism $\pi \circ f : R \mapsto S/J$.
Then, $Ker(\pi \circ f) = r \in R$, $\pi(f(r)) = 0 = f^{-1}(J)$.
By the First Homomorphism Theorem, $R/f^{-1}(J) \backsimeq S/J$. 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, $f : R \mapsto R/I$ is the canonical homomorphism $f(r) = \bar{r}$.
Thus, $R/K \backsimeq (R/I)/(K/I)$.

II.4.2 Ideal types

principal Ideal

Definition II.4.4 *[8]*
Let R be a commutive ring with unity and let $a \in R$. then, we denote the **principal ideal** *generated by a, by: $\langle a \rangle = \{ar,\ r \in R\} = aR = Ra$.*

Example II.4.3

$$\langle a \rangle = \{ar + na,\ r \in R,\ n \in \mathbb{Z}\}.$$

is a principle ideal.

Prime Ideal

Definition II.4.5 *[8]*
Let R be a commutative ring and A a proper ideal of R.
A is a **prime ideal** *of R, if: $a, b \in R$ and $ab \in A$ implies $a \in A$ or $b \in A$.*

Examples II.4.1

1. *In $\mathbb{Z}$, an ideal (n) is prime if and only if the integr n is prime or $n = 0$.*
2. *In the ring $\mathbb{Z}$, the zero ideal is prime, but in the ring $\mathbb{Z}/6\mathbb{Z}$, the zero ideal is not prime, since $\overline{2}.\overline{3} = \overline{0}$ but neither $2 = 0$ nor $3 = 0$.*

Maximal Ideal

Definition II.4.6 *[8]*
Let R be a commutative ring and A a proper ideal of R.
A is a **maximal ideal** *of R if any ideal B of R with $A \subseteq B \subseteq R$ has $B = A$ or $B = R$.*

Example II.4.4 *Let be the ring $(12\mathbb{Z}, +, .)$.*
We have $12 = 3(4) = 6(2)$, so the proper ideals are:

1- $I_1 = (\bar{2}) = (\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}, +, .)$

2- $I_2 = (\bar{4}) = (\{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}\}, +, .)$

3- $I_3 = (\bar{4}) = (\{\bar{0}, \bar{4}, \bar{8}\}, +, .)$

4- $I_4 = (\bar{6}) = (\{\bar{0}, \bar{6}\}, +, .)$

I_1 and I_2 are maximal in $12\mathbb{Z}$.

Proposition II.4.2
Any maximal ideal is prime.

Proof II.4.7
Let M be a maximal ideal. To show it is prime, we assume that $a, b \in R$, with $ab \in M$ and $a \notin M$.
We must show that $b \in M$. Since $a \notin M$, the ideal sum $M + (a)$ is strictly larger than M, and since M is maximal, it must be equal to the unit ideal R. So $1 \in M + (a)$, which means we can write $1 = x + ra$ for some $x \in M$ and $r \in R$. Then $b = xb + rab$, and since both x and ab are in M, this shows that $b \in M$. □

III Some special classes of rings

Throughout mathematics there are many examples of rings, starting with the integers. In this section we shall describe some of the most important classes, integral domain and rings of algebraic integers, as well as some of their properties, the Euclidean algorithm and unique factorization.

III.1 Integral domain ring

Definition III.1.1 *[3]*
If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero-divisor if there exists $a, b \in R$, with $b \neq 0$, such that $ab = 0$.

Definition III.1.2 *[3]*
A commutative ring is an integral domain if it has no zero-divisors. The ring of integers, naturally enough, is an example of an integral domain.

Definition III.1.3 *[3]*
A ring is said to be a division ring if its nonzero elements form a group under multiplication.

The unit element under multiplication will be written as 1, and the inverse of an element a under multiplication will be denoted by a^{-1}.
Finally we make the defnition of the ultra-important object known as a field.

Theorem III.1.1
Let P be an ideal of a commutative ring R with identity 1. Then, P is a prime ideal of R if and only if R/P is an integral domain.

Proof III.1.1
Supposing that P is a prime ideal of a commutative ring R, with 1. Then $P \neq R$ implies $1 + P \neq 0 + P$. Hence R/P is a commutative ring R with identity.

Assuming that $(a+P)(b+P) = 0+P$. *Then* $ab+P = 0+P$ *and* $a \in P$. *By the definition of a prime ideal* P *we get* $a \in P$ *or* $b \in P$. *That is,* $a+P = 0+P$ *or* $b+P = 0+P$. *Thus,* R/P *is an integral domain.*
Conversely, if R/P *is an integral domain, then* $1+P \neq 0+P$ *and* R/P *is a commutative ring* R *which has no zero divisors.*
Hence, $P \neq R$. *Assuming* $ab \in P$. *Then* $ab+P = 0+P$ *and* $(a+P)(b+P) = 0+P$. *Since* R/P *is an integral domain, we get* $a+P = 0+P$ *or* $b+P = 0+P$. *So* $a \in P$ *or* $b \in P$. *Thus* P *is a prime ideal.* □

III.2 Field

Definition III.2.1 *[3]*
A **field** *is a nonzero ring in which every nonzero element is a unit.*

Lemma III.2.1
A finite integral domain is a field.

Proof III.2.1
As we may recall, an integral domain is a commutative ring such that $ab = 0$ *if and only if at least one of* a *or* b *is itself* 0. *A field, on the other hand, is a commutative ring with unit element in which every nonzero element has a multiplicative inverse in the ring.*
Let D *be a finite integral domain. In order to prove that* D *is a field we must:*
1. Produce an element $1 \in D$ *such that* $a1 = a$ *for every* $a \in D$.
2. For every element $a \neq 0 \in D$, *produce an element* $b \in D$ *such that* $ab = 1$.
Let $x_1, x_2, ..., x_n$ *be all the elements of* D, *and suppose that* $a \neq 0 \in D$. *Consider the elements* $x_1a, x_2a, ..., x_na$; *they are all in* D. *We claim that they are all distinct! For suppose that* $x_ia = x_ja$ *for* $i \neq j$; *then* $(x_i - x_j)a = 0$.
Since D *is an integral domain and* $a \neq 0$, *this forces* $x_i - x_j = 0$, *and so* $x_i = x_j$, *contradicting* $i \neq j$.
Thus $x_1a, x_2a, ..., x_n$ *a are* n *distinct elements lying in* D, *which has exactly* n *elements. By the pigeonhole principle these must account for all the elements of* D *; stated otherwise, every element* $y \in D$ *can be written as* x_1 *a for some* x_{i_0} *In particular, since* $a \in D$ *,* $a = x_{i_0}$ *a for some* $x_{i_0} \in D$. *Since* D *is commutative,* $a = x_{i_0}a = ax_{i_0}$ *We propose to show that* x_{i_0} *acts as a unit element for every element of* D. *For, if* $y \in D$, *as we have seen,* $y = x_ia$ *for some* $x_i \in D$, *and so* $yx_{i_0} = (x_ia)x_{i_0} = x_i(ax_{i_0}) = x_ia = y$. *Thus* x_{i_0} *is a unit element for* D *and we write it as* 1. *Now* $1 \in D$, *so by our previous argument, it too is realizable as a multiple of* a; *that is, there exists* $a, b \in D$ *such that* $1 = ba$. *The lemma is now completely proved.* □

Theorem III.2.1
Let R *be a commutative ring with unity, and* I *is an ideal of* R. *Then,* R/I *is a field if and only if* I *is maximal.*

Proof III.2.2 *Let I be a maximal ideal. Then, R/I has only two ideals $\{0\}$ and R/I. If $x \notin I$ then, $(\overline{x}) = R/I$. Thus, $\overline{1} = \overline{xy}$, $y \in R$. Thus, R/I is a field.*
The converse is similar. □

Lemma III.2.2 *Every field is an integral domain.*

Proof III.2.3 *If a is an element of the field F and $a \neq 0$, we have a multiplicative inverse a^{-1}. If we have an equation $ab = 0$, we can multiply both sides by a^{-1} :*

$$\begin{aligned} ab = 0 &\Rightarrow a^{-1}ab = a^{-1}0 \\ &\Rightarrow b = 0. \end{aligned}$$

□

Example III.2.1
1. $\mathbb{Z}$ is an integral domain.
2. $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain. It is an integral domain when n is prime.

Remark III.2.1 *We have seen before that if R is a ring then $\{0\}$ and R are ideals.*
For some rings these are the only ideals; for instance, fields have no ideals other than these trivial ones. Let I be an ideal of R, and suppose that $a \in I$. Then I contains every element of the form ra for $r \in R$. In particular, if R has an identity and a has an inverse then I contains $t = (ta^{-1})\, a$ for any $t \in R$. This observation gives us the following theorem:

Theorem III.2.2
(i) An ideal which contains an element with an inverse must be the whole ring.
(ii) If F is a field then the only ideals in F are 0 and F.

Proof III.2.4 *The first part is immediate from the preceding remarks, and the second part follows from the first since all nonzero elements of fields have inverses.* □

III.3 The field of quotient of an integral domain

If every nonzero element in an integral domain D has a multiplicative inverse, then D is a field. It is the purpose of this section to show that every integral domain can be regarded as subring of a field, a field of quotients of the integral domain. This field will be a minimal field containing the integral domain. For example, the integers are contained in the field $\mathbb{Q}$, whose elements can be all expressed as quotients of integers.
We can follow the steps, by the way $\mathbb{Q}$ can be formed from $\mathbb{Z}$.
Let D be an integral domain that we desire to enlarge to a field of quotients F. We take four steps to obtain F as follows:

1. *We define the elements of F.*
2. *We define addition and multiplucation on F.*
3. *We show that F is a field under the operations.*
4. *We show that D can be considered a subring of F.*

Step1. *We consider* $S = \{(a,b)\ ,\ a,b \in D,\ b \neq 0\}$.

Definition III.3.1 *[5]*
Tow elements $(a,b),(c,d) \in S$ are **equivalent**, *denoted by $(a,b) \sim (c,d)$, if $ad = bc$.*

Theorem III.3.1
The relation $\sim$ on S is an equivalence relation.

Proof III.3.1
Reflexive: $(a,b) \sim (a,b)$ since $ab = ba$ (D is an intrgral domain).
Symetric: $(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow (c,d) \sim (a,b)$.
Transitive: If $(a,b) \sim (c,d)$ and $(c,d) \sim (r,s)$, then, $ad = bc$ and $cs = dr$. We have:

$$asd = sad = sbc = bcs = bdr = brd.$$

Now $d \neq 0$, and D is an integral domain, so cancellation is valid.
Hence from $asd = brd$ we obtain $as = br$, so that $(a,b) \sim (r,s)$.
We now know that $\sim$ gives a partitin of S into equivalence classes.
We shall let $\frac{a}{b}$ be the equivalence class of (a,b) in S under the relation $\sim$ .i.e

$$\frac{a}{b} = \{(c,d) \in S,\ (c,d) \sim (r,s),\ r,s \in S\}.$$

Let

$$F = \left\{\frac{a}{b},\ (a,b) \in S\right\}.$$

Step2. *We define addition and multiplication in F. Observing that if $D = \mathbb{Z}$ and $\frac{a}{b}$ is viewed as $a/b \in \mathbb{Q}$, these definitions applied to $\mathbb{Q}$ give the usual operations.*

Theorem III.3.2
For $\frac{a}{b} \in F$, the operations

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}\ ;\ \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

are well-defined on F.

Proof III.3.2
Since $\frac{a}{b}$, $\frac{c}{d} \in F$, then (a,b) and (c,d) are in S and $bd \neq 0$.
So

$$(ad+bc, bd), (ac, bd) \in S$$

Thus

$$\frac{ac}{bd}\ ,\ \frac{ad+bc}{bd} \in F.$$

To see these operations of addition and multiplication are well-defined, we suppose that $\frac{a_1}{b_1} = \frac{a}{b}$ *and* $\frac{c_1}{d_1} = \frac{c}{d}$ *. Then,*

$$a_1 b = b_1 a \quad , \quad c_1 d = d_1 c \tag{III.1}$$

We must show that

$$\frac{a_1 d_1 + b_1 c_1}{b_1 d_1} = \frac{ad+bc}{bd},$$

and,

$$\frac{a_1 c_1}{b_1 d_1} = \frac{ac}{bd}$$

i.e.

$$(a_1 d_1 + b_1 c_1)bd = b_1 d_1 (ad+bc)\ ,\ a_1 c_1 bd = b_1 d_1 ac.$$

These can be verified by using $III.1$*. Now we complete the proof.*
From this theorem we see that:

$$\frac{ab}{ac} = \frac{b}{c},\ \forall a, b, c \in D,\ ac \neq 0.$$

Step3. *We check that F is a field under these operations.* □

Theorem III.3.3
The above defined $(F, +, .)$ *from D is a field.*

Proof III.3.3

1. *Addition in F is commutative: Since* $\frac{a}{b} + \frac{c}{d} = \frac{bc+da}{bd}$ *and* $\frac{c}{d} + \frac{a}{b} = \frac{ad+bc}{bd}$*. So* $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$.
2. *Addition is associative. This is easy to verify.*
3. *The element* $\frac{0}{1}$ *is an identity element for addition in F. This is clear.*
4. *The element* $\frac{-a}{b}$ *is an additive inverse for* $\frac{a}{b}$ *in F. This is clear.*
5. *Multiplication in F is associative. This is easy to verify.*
6. *Multiplication in F is commutative. This is easy to verify.*
7. *The distributive laws hold inF. This is easy to verify.*
8. *The element* $\frac{1}{1}$ *is a multiplicative identity element in F. This is clear.*

9. *If $\frac{a}{b} \in F$ is not the additive identity element, then $a \neq 0$ in D and $\frac{b}{a}$ is a multiplicative inverse for $\frac{a}{b}$: Let $\frac{a}{b} \in F$. If $a = 0$, then, $\frac{0}{b} = \frac{b0}{b1} = \frac{0}{1}$. But $\frac{0}{1}$ is the additive identity element by (3). Thus if $\frac{a}{b} \neq \frac{0}{1}$ in F, we have $a \neq 0$. Now, $\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$. Thus, $\frac{a}{b}\frac{b}{a} = \frac{1}{1}$, and $\frac{1}{1}$ is the multiplicative identity by (8). So $(F, +, .)$ is a field This completes Step 3.*

Step4. *We show that F can be regarded as containing D.* □

Theorem III.3.4
The application

$$\begin{aligned} \phi : D &\mapsto F \\ a &\mapsto \phi(a) = \frac{a}{1} \end{aligned}$$

is an isomorphism of D with a subring of F.

Proof III.3.4
For $a, b \in F$, we have

$$\phi(a) + \phi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a1 + 1b}{1} = \frac{a+b}{1} = \phi(a+b).$$

$$\phi(a)\phi(b) = \frac{a}{1}\frac{b}{1} = \frac{ab}{1} = \phi(ab).$$

It remains for us to show only that ϕ is one to one. If $\phi(a) = \phi(b)$ then $\frac{a}{1} = \frac{b}{1}$, so $(a, 1) \sim (b, 1)$ given $a1 = 1b$; that is, $a = b$. Thus ϕ is an isomorphism of D with $\phi(D)$, of course, as a subdomain of F.
Since $\frac{a}{b} = \frac{a}{1}\frac{1}{b} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \phi(a)\phi(b)^{-1}$ clearly holds in F, we have now proved the following theorem. □

Theorem III.3.5 *Any integral domain D can be enlarged to (or embedde in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is called a field of quotients of D, or field of fractions of D).*

Theorem III.3.6
Let F be a field of quotients of D and let E be any field containing D. Then there exists an application : $\psi : F \longrightarrow E$ that gives an isomorphism of F with a subfield of E such that $\psi(a) = a$ for $a \in D$.

Proof III.3.5
For $a, b \in D$, by a/b we mean the quotient regarded as elements of F, by $a/_E b$ we mean

the quotient regarded as elements of E. Define

$$\psi : F \longrightarrow E$$
$$a/b \longrightarrow \psi(a/b) = a/b,\ a, b \in D, b \neq 0$$

We first show that ψ is well-defined. If $a/b = c/d$ in F, then $ad = bc$ in D : Thus $a/_E b = c/_E d$, in E, so ψ is well-defined. The equations

$$\psi(xy) = \psi(x)\psi(y)$$

and,

$$\psi(x + y) = \psi(x) + \psi(y),\ \forall x, y \in F.$$

Follow easily from the definition of ψ on F and from the fact that ψ is the identity on D If $a/_E b = c/_E d$ we have $ad = bc$ So $a/b = c/d$. Thus ψ is one to one.
By definition, $\psi(a) = a$ for $a \notin D$. □

Theorem III.3.7
Every field E containing an integral domain D contains a field of quotients of D.

Proof III.3.6
Let F be a field of quotients of D. In the above Theorem the subfield $\psi[F]$ of E is a quotient field of D. □

Theorem III.3.8
Any two fields of quotients of an integral domain D are isomorphic.

Proof III.3.7
We remark that, in general, not every unital noncommutative ring without zero divisors can be embedded into a division ring. This leads to Ore theory. The **right Ore condition** *for a multiplicative subset $S = R/\{0\}$ of a ring R is that for any $a \in R$ and any $s \in S$, the intersection $aS \bigcap sR \neq \phi$. A (non-commutative) integral domain for which the set of non-zero elements satisfies the right Ore condition is called a right Ore domain. Only* **right Ore domains** *can be embedded in some division rings.* □

III.4 Principal ideal domain

Definition III.4.1 *[6]*
An integral domain is called a principal ideal domain (PID for short) if every ideal in it is principal (can be generated by a single element).

Example III.4.1
$\mathbb{Z}$ is a principal ideal domain.

Proof III.4.1 *Let n be the smallest positive element of I. Let $a \in I$.*
By the integer division theorem, $a = qn + r$, where $0 \leq r < n$, $r = a - qn \in I$ by absorbtion and commutativity. Since $r \in I, r < n$ and n is the smallest positive element of I, $r = 0$.
Therefore, every element of I is a multiple of n. Also, all multiples of n are in I by the absorbtion property.
Therefore, $I = n\mathbb{Z}$. □

III.5 Euclidean ring

Definition III.5.1 *[3]*
An integral domain R is said to be an Euclidean ring if for every $a \neq 0$ in R there is defined a nonnegative integer $d(a)$ such that:

1. *$\forall a, b \in R$ both non-zero, $d(a) \leqslant d(ab)$.*
2. *$\forall a, b \in R$ both non-zero, $\exists t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.*

Example III.5.1
$\mathbb{Z}$ is an euclidean domain, such that $d(a) = |a|$.

Definition III.5.2 *[3]*
Let R be a commutative ring with a unit element. An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that $ab = 1$.

Remark III.5.1 *The set of all unit element of R is denoted by $U(R)$.*

Theorem III.5.1
Let D be an Euclidean domain with an Euclidean norm d then:

1. *$d(1) \leqslant d(a)$, $\forall a \in R$.*
2. *$u \in D$ is a unit if and only if $d(u) = d(1)$.*

Proof III.5.1
1. For $a \in D \setminus \{0\}$. we have $d(1) \leqslant d(1a) = d(a)$.
2. If $u \in U(D)$, then

$$d(u) \leqslant d(uu^{-1}) = d(1)$$

Thus $d(u) = d(1)$.
Now we suppose $u \in D$ with $d(u) = d(1)$. Then by the division algorithm, there exist $q, r \in D$ such that

$$1 = uq + r.$$

where either $r = 0$ or $d(r) < d(u)$. By (1), we know that $d(r) < d(u)$ is impossible. Then $r = 0$ and $1 = uq$. Hence $u \in U(D)$. □

Theorem III.5.2
Let R be a Euclidean ring and let A be an ideal of R. Then there exists an element $a_0 \in A$ such that A consists exactly of all $a_0 x$ as x ranges over R.

Proof III.5.2
If A just consists of the element 0, put $a_0 = 0$ and the conclusion of the theorem holds. Thus we may assume that $A \neq 0$; hence, there is an $a \neq 0$ in A. Pick an $a_0 \in A$ such that $d(a_0)$ is minimal. (Since d takes on nonnegative integer values this is always possible.)
Supposing that $a \in A$. By the properties of Euclidean rings there exist $t, r \in R$ such that $a = ta_0 + r$ where $r = 0$ or $d(r) < d(a_0)$. Since $a_0 \in A$ and A is an ideal of R, ta_0 is in A. Combined with $a \in A$ this results in $a - ta_0 \in A$; but $r = a - ta_0$, whence $r \in A$. If $r \neq 0$ then $d(r) < d(a_0)$, giving us an element r in A whose d-value is smaller than that of a_0, in contradiction to our choice of a_0 as the element in A of minimal d-value. Consequently $r = 0$ and $a = ta_0$, which proves the theorem.
We introduce the notation $\langle a \rangle = \{xa,\ x \in R\}$ to represent the ideal of all multiples of a. □

Corollary III.5.1
An euclidean ring possesses a unit element.

Proof III.5.3
Let R be an euclidean ring; then R is certainly an ideal of R, so that by previous theorem we may conclude that $R = \langle u_0 \rangle$ for some $u_0 \in R$.
Thus every element in R is a multiple of u_0 Therefore, in particular, $u_0 = u_0 c$ for some $c \in R$. If $a \in R$ then $a = xu_0$ for some $x \in R$, hence $ac = (xu_0)c = x(u_0 c) = xu_0 = a$. Thus c is seen to be the required unit element. □

Definition III.5.3 *[3]*
An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form $A = \langle a \rangle$ for some $a \in R$.
Once we establish that a Euclidean ring has a unit element, in virtue of Theorem III.5.2, we shall know that a Euclidean ring is a principal ideal ring.
The converse, however is false; there are principal ideal rings which are not Euclidean rings.

Definition III.5.4 *[3]*
If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exists $ac \in R$ such that $b = ac$. We shall use the symbol $a|b$ to represent the fact that a divides b and $a \nmid b$ to mean that a does not divide b. The proof of the next remark is so simple and straightforward that we omit it.

Remark III.5.2

1. *If $a \mid b$ and $b \mid c$ then, $a \mid c$.*
2. *If $a \mid b$ and $a \mid c$ then, $a|(b \pm c)$.*
3. *If $a \mid b$ then $a \mid bx$, $forall x \in R$.*

Definition III.5.5 *[3]*
If $a, b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if :

1. *$d \mid a$ and $d \mid b$.*
2. *Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.*

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a and b .

Lemma III.5.1
Let R be an euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof III.5.4
Let A be the set of all elements $ra + sb$ where r, s range over R. We claim that A is an ideal of R. For suppose that $x, y \in A$; therefore $x = r_1 a + s_1 b$, $y = r_2 a + s_2 b$, and so $x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2)b \in A$.
Similarly, for any $u \in R$, $ux = u(r_1 a + s_1 b) = (ur_1)a + (us_1)b \in A$.
Since A is an ideal of R, by Theorem $III.5.2$, there exists an element $d \in A$ such that every element in A is a mutiple of d. By dint of the fact that $d \in A$ and that every element of A is of the form $ra + sb$, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. Now by the corollary to Theorem , R has a unit element 1; thus $a = 1a + 0b \in A$, $b = 0a + 1b \in A$. Being in A, they are both multiples of d, whence $d|a$ and $d|b$.
Suppose, finally, that $c|a$ and $c|b$; then $c|\lambda a$ and $c|\mu b$ so that c certainly divides $\lambda.a + \mu.b = d$. Therefore d has all the requisite conditions for a greatest common divisor and the lemma is proved. □

Lemma III.5.2
Let R be an integral domain with unit element and suppose that for $a, b \in R$ both $a|b$ and $b|a$ are true. Then $a = ub$, where u is a unit in R.

Proof III.5.5 *Since $a|b$, $b = xa$ for some $x \in R$; since $b|a$, $a = yb$ for some $y \in R$. Thus $b = x(yb) = (xy)b$; but these are elements of an integral domain, so that we can cancel the b and obtain $xy = 1$; y is thus a unit in R and $a = yb$, proving the lemma .* □

Lemma III.5.3
Let R be a Euclidean ring and $a, b \in R$. lf $b \neq 0$ is not a unit in R, then $d(a) < d(ab)$.

Proof III.5.6
We consider the ideal $A = \langle a \rangle = xa, x \in R$ of R. By condition 1 for a Euclidean ring, $d(a) \leq d(xa)$ for $x \neq 0$ in R. Thus the d-value of a is the minimum for the d-value of any element in A. Now $ab \in A$; if $d(ab) = d(a)$, by the proof used in establishing Theorem $III.5.1$ since the d-value of ab is minimal in regard to A, every element in A is a multiple of ab. In particular, since $a \in A$, a must be a multiple of ab; whence $a = abx$ for some $x \in R$. Since all this is taking place in an integral domain we obtain $bx = 1$. In this way b is a unit in R, in contradiction to the fact that it was not a unit. The net result of this is that $d(a) < d(ab)$. □

Theorem III.5.3 *(Euclidian algorithm)*
Let D be a Euclidean domain with a Euclidean norm d, and let a and b be nonzero elements of D. 1. There are $q_i, r_i \in D$ such that:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &... \\ r_{s-3} &= r_{s-2}q_{s-1} + r_{s-1} \\ r_{s-2} &= r_{s-1}q_s + r_s. \end{aligned}$$

Where $r_s = 0$.

$$d(r_{s-1}) < d(r_{s-2}) < ... < d(r_2) < d(r_1) < d(b)$$

Furthermore $pgcd(a, b) \sim r_{s-1}$.
2.If $pgcd(a, b) \sim d$ then there exist $\lambda, \mu \in D$ such that $d = \lambda a + \mu b$.

Proof III.5.7 *1. Since $d(r_i) < d(r_{i-1})$ and $d(r_i)$ is a nonnegative integer, it follows that after some finite number of steps we must arrive at some $rs = 0$. Thus, we have all equations in (2.1).*
Suppose $d \sim pgcd(a, b)$. From $d \mid a$ and $d \mid b$, we have $d \mid r_1$. From $d \mid b$ and $d \mid r_1$, we have $d \mid r_2$. In this manner we deduce that $d \mid r_i$ for any i.
In particularly, $d \mid r_{s-1}$.
On the other hand, $r_{s-1} \mid r_{s-2}$. From $(2, 1)$ backward, we deduce that:

$$r_{s-1} \mid r_{s-2}, r_{s-1} \mid r_{s-3}, ..., r_{s-1} \mid b.$$

and

$$r_{s-1}|a.$$

Thus, $r_{s-1}|d$. Therefore, $r_{s-1} \sim d$.
2.We may assume that $d = r_{s-1}$. We shall prove by induction on k that $r_k = \lambda_k a + \mu_k b$ for some $\lambda_k \mu_k \in D$. If $s = 1$, i.e, $r_1 = 0$, then $d = b$, and $d = 0a + 1b$ and we are done. Supposing that $r_j = \lambda_j a + \mu_j b$ for $j = 1, 2, ..., k$. Using $r_{k-1} = r_k q_{k+1} + r_{k+1}$ we deduce that

$$\begin{aligned} r_{k+1} = r_{k-1} - r_k q_{k+1} &= (\lambda_{k-1}a + \mu_{k-1}b) - q_{k+1}(\lambda_k a + \mu_k b. \\ &= \lambda_{k+1}a + \mu_{k+1}b. \end{aligned}$$

Thus

$$d = r_{s-1} = \lambda_{s-1}a + \mu_{s-1}b$$

Where $\lambda_{s-1}\mu_s \in D$. □

Definition III.5.6 *[3]*

In the Euclidean ring R a nonunit π is said to be a prime element of R if whenever $\pi = ab$, where $a, b \in R$, then one of a or b is a unit in R.
A prime element is thus an element in R which cannot be factored in R in a nontrivial way.

Lemma III.5.4
Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Proof III.5.8
The proof is by induction on $d(a)$
If $d(a) = d(1)$ then a is a unit in R , and so in this case, the assertion of the lemma is correct.
We assume that the lemma is true for all elements x in R such that $d(x) < d(a)$. On the basis of this assumption we aim to prove it for a. This would complete the induction and prove the lemma.
If a is a prime element of R there is nothing to prove. So suppose that $a = bc$ where neither b nor c is a unit in R. By Lemma III.5.3, $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Thus by our induction hypothesis b and c can be written as a product of a finite number of prime elements of R;

$$b = \pi_1\pi_2...\pi_n, \quad c = \pi'_1\pi'_2...\pi'_m.$$

Where π' s and π'' s are prime element of R. Consequantly

$$a = bc = \pi_1\pi_2...\pi_n\pi'_1\pi'_2...\pi'_m$$

and in this way a has been factored as a product of a finite number of prime element. □

Definition III.5.7 *[3]*
In the Euclidean ring R, a and b in R are said to be relatively prime if their greatest common divisor is a unit of R.

Definition III.5.8 *[5]*
Let R be a unital commutative ring. Two elements $a, b \in R$ are associates in R if $a = bc$ for some $c \in U(R)$, denoted by $a \sim b$.
It is easy to show that the relation $a \sim b$ is an equivalence relation on R.

Example III.5.2 *We know that $U(\mathbb{Z}) = \{\pm 1\}$. So the only associates of 6 in $\mathbb{Z}$ are ± 6.*

Since any associate of a greatest common divisor is a greatest common divisor, and since 1 is an associate of any unit, if a and b are relatively prime we may assume that $(a, b) = 1$.

Lemma III.5.5 **The Gaussian Theorem**
Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, $a|bc$ but $(a, b) = 1$. Then $a|c$.

Proof III.5.9
As we have seen in Lemma III.5.1, the greatest common divisor of a and b can be realized in the form $\lambda a + \mu b$. Thus by our assumptions, $\lambda a + \mu b = 1$. Multiplying this relation by c we obtain $\lambda ac + \mu bc = c$. Now $a|\lambda ac$, always, and $a|\mu bc$ since $a|bc$ by assumption; therefore $a|(\lambda ac + \mu bc) = c$. This is, of course, the assertion of the lemma. □

Lemma III.5.6
Let R be a Euclidian ring.
If π in R is a prime element and $a \in R$. Then, either $\pi|a$ or $(\pi, a) = 1$.

Proof III.5.10 *In particular, (π, a) is a divisor of π so it must be π or 1(or any unit). If $(\pi, a) = 1$, one-half our assertion is true ; if $(\pi, a) = \pi$, since $(\pi, a) \mid a$ we get $\pi \mid a$, and the other half of our assertion is true.* □

Lemma III.5.7
If π is a prime element in the Euclidean ring R and $\pi \mid ab$ where $a, b \in R$ then π divides at least one of a or b.

Proof III.5.11 *Suppose that π does not divide a; then $(\pi, a) = 1$. By lemma III.5.4 we are led to $\pi \mid b$.* □

Corollary III.5.2
If π is a prime element in the Euclidean ring R and $\pi \mid a_1 a_2 ... a_n$ then π divides at least one $a_1, a_2, ..., a_n$.

Theorem III.5.4 (**Unique factorization theorem**)
Let R be a Euclidean ring and $a \neq 0$ a nonunit in R.
Supposing that $a = \pi_1 \pi_2 ... \pi_n = \pi'_1 \pi'_2 ... \pi'_m$ where the π_i and π'_j are prime elements of R.
Then $n = m$ and each $\pi_i, 1 \leq i \leq n$ is an associate of some $\pi'_j, 1 \leq j \leq m$ and conversely each π'_k is an associate of some π'_q.

Proof III.5.12
Looking at the relation $a = \pi_1 \pi_2 ... \pi_n = \pi'_1 \pi'_2 ... \pi'_m$. But $\pi_1 | \pi_1 \pi_2 ... \pi_n$, hence, $\pi_1 | \pi'_1 \pi'_2 ... \pi'_m$. By lemma III.5.7 , π_1 must divide some π'_i since π_1 and π'_i are both prime elements of R and $\pi_1 | \pi'_i$ they must be associates and $\pi'_i = u_1 \pi_1$, where u_1 is a unit in R. Thus,

$$\pi_1 \pi_2 ... \pi_n = \pi'_1 \pi'_2 ... \pi'_m = u \pi_1 \pi'_1 \pi'_2 ... \pi'_{i-1} \pi'_{i+1} ... \pi'_m;$$

we cancel off π_1 and we are left with

$$\pi_2 ... \pi_n = u_1 \pi'_1 \pi'_2 ... \pi'_{i-1} \pi'_{i+1} ... \pi'_m.$$

We repeat the argument on this relation with π_2.
After n steps, the left side becomes 1, the right side a product of a certain number of π'

(the excess of m over n). This would force $n \leq m$ since the π' are not units. Similarly, $m \leq n$, so that $n = m$. In the process we have also showed that every π_i has some π_i' as an associate and conversely.
We have that every nonzero element in a Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is a unit in R. □

We finish the section by determining all the maximal ideals in a Euclidean ring. In Theorem III.5.2 we proved that any ideal A in the Euclidean ring R is of the form $A = \langle a_0 \rangle$ where $\langle a_0 \rangle = xa_0$, $x \in R$. We now ask : What conditions imposed on a_0 insure that A is a maximal ideal of R? For this question we have a simple precise answer, namely

Lemma III.5.8
The ideal $A = \langle a_0 \rangle$ is a maximal ideal of the Euclidean ring R if and only if a_0 is a prime element of R.

Proof III.5.13
We first prove that if a_0 is not a prime element, then $A = \langle a_0 \rangle$ is not a maximal ideal. For, suppose that $a_0 = bc$ where $b, c \in R$ and neither b nor c is a unit. Let $B = \langle b \rangle$; then certainly $a_0 \in B$ so that $A \subset B$.
We claim that $A \neq B$ and that $B \neq R$. If $B = R$ then $1 \in B$ so that $1 = xb$ for some $x \in R$, forcing b to be a unit in R, which it is not. On the other hand, if $A = B$ then $b \in B = A$ whence $b = xa_0$ for some $x \in R$. Combined with $a_0 = bc$ this results in $a_0 = xca_0$, in consequence of which $xc = 1$. But this forces c to be a unit in R, again contradicting our assumption. Therefore B is neither A nor R and since $A \subset B$, A cannot be a maximal ideal of R.
Conversely, suppose that a_0 is a prime element of R and that U is an ideal of R such that $A = \langle a_0 \rangle \subset U \subset R$. By Theorem III.5.2 , $U = \langle u_0 \rangle$. Since $a_0 \in A \subset U = \langle u_0 \rangle$, $a_0 = xu_0$ for some $x \in R$. But a_0 is a prime element of R, from which it follows that either x or u_0 is a unit in R. If u_0 is a unit in R then $U = R$. If, on the other hand, x is a unit in R,then $x^{-1} \in R$ and the relation $a_0 = xu_0$ becomes $u_0 = x^{-1}a_0 \in A$ since A is an ideal of R. This implies that $U \subset A$; together with $A \subset U$ we conclude that $U = A$. This means that A is a maximal ideal of R. □

III.6 The Gaussian Ring

An abstraction in mathematics gains in substance and importance when, particularized to a specific example, it sheds new light on this example. We are about to particularize the notion of a Euclidean ring to a concrete ring, the ring of Gaussian integers. Applying the general results obtained about Euclidean rings to the Gaussian integers we shall obtain a highly nontrivial theorem about prime numbers due to Fermat.
Let $\mathbb{Z}[i]$ denote the set of all complex numbers of the form $a + bi$ where a and b are integers. Under the usual addition and multiplication of complex numbers b forms an

integral domain called the domain of Gaussian integers.
Our first objective is to exhibit $\mathbb{Z}[i]$ as a Euclidean ring. In order to do this we must first introduce a function $d(x)$ defined for every nonzero element in $\mathbb{Z}[i]$ which satisfies :

1. *$d(x)$ is a nonnegative integer for every $x \neq 0 \in \mathbb{Z}[i]$.*
2. *$d(x) \leq d(xy)$ for every $y \neq 0$ in $\mathbb{Z}[i]$.*
3. *Given $u, v \in \mathbb{Z}[i]$ there exist $t, r \in \mathbb{Z}[i]$ such that $v = tu + r$ where $r = 0$ or $d(r) < d(u)$.*

Our candidate for this function d is the following : if $x = a + bi \in \mathbb{Z}[i]$, then $d(x) = a^2 + b^2$. The $d(x)$ so defined certainly satisfies property 1; in fact, if $x \neq 0 \in j[i]$ then $d(x) \geq 1$.
As is well known, $\forall x, y \in \mathbb{C}$ (not necessarily in $\mathbb{Z}[i]$):

$$d(xy) = d(x)d(y)$$

thus, if x and y are in addition in $\mathbb{Z}[i]$ and $y \neq 0$, then, since

$$d(y) \geq 1,$$

$d(x) = d(x).l \leq d(x)d(y) = d(xy), showingthatcondition\ 2\ issatisfied.$
$Allourefforтnowwillbetoshowthatcondition\ 3\ alsoholdsforthisfunction\ d\ in\ Z[i].$
$Thisisdoneintheproofof$

Theorem III.6.1
$\mathbb{Z}[i]$ is a Euclidean ring.

Proof III.6.1
As was remarked in the discussion above, to prove previous Theorem we merely must show that, given $x, y \in \mathbb{Z}[i]$ there exists $t, r \in \mathbb{Z}[i]$ such that $y = tx + r$ where $r = 0$ or $d(r) < d(x)$.
We first establish this for a very special case, namely, wherey is arbitrary in $\mathbb{Z}[i]$ but where x is an (ordinary) positive integer n. Suppose that $y = a + bi$; by the division algorithm for the ring of integers we can find integers u, v such that $a = u_n + u_1$ and $b = v_n + v_1$ where u_1 and v_1 are integers satisfying $|u_1| \leq \frac{n}{2}$ and $|v_1| \leq \frac{n}{2}$.
Let $t = u + vi$ and $r = u_1 + v_1 i$; then

$$\begin{aligned} y =& a + bi. \\ =& un + u_1 + (vn + v_1)i. \\ =& (u + vi)n + u_1 + v_1 i. \\ =& tn + r,\ t, r \in j[i]. \end{aligned}$$

Since

$$\begin{aligned} d(r) =& d(u_1 + v_1 i). \\ =& u_1^2 + v_1^2. \\ \leq& \frac{n^2}{4} + \frac{n^2}{4}. \\ <& n^2 = d(n). \end{aligned}$$

we see that in this special case we have shown that $y = tn + r$ *with* $r = 0$ *or,* $d(r) < d(n)$.
We now go to the general case; let $x \neq 0$ *and* y *be arbitrary elements in* $\mathbb{Z}[i]$. *Thus* $x\bar{x}$ *is a positive integer* n *where* x *is the complex conjugate of* x. *Applying the result of the paragraph above to the elements* $y\bar{x}$ *and* n *we see that there are elements* $t, r \in \mathbb{Z}[i]$ *such that* $y\bar{x} = tn + r$ *with* $r = 0$ *or* $d(r) < d(n)$. *Putting into this relation* $n = x\bar{x}$ *we obtain*

$$d(y\bar{x} - tx\bar{x}) < d(n) = d(x\bar{x});$$

applying to this the fact that

$$d(y\bar{x} - tx\bar{x}) = d(y - tx)d(\bar{x})$$

and

$$d(x\bar{x}) = d(x)d(\bar{x})$$

we obtain that $d(y - t\bar{x})d(\bar{x}) < d(x)d(\bar{x})$.
Since $x \neq 0$, $d(\bar{x})$ *is a positive integer, so this inequality simplifies to* $d(y - tx) < d(x)$. *We represent* $y = tx + r_0$, *where* $r_0 = y - tx$; *thus,* t *and* r_0 *are in* $\mathbb{Z}[i]$, *and as we saw above,* $r_0 = 0$ *or* $d(r_0) = d(y - tx) < d(x)$. *This proves the theorem.*
Since $\mathbb{Z}[i]$ *has been proved to be a Euclidean ring, we are free to use the results established about this class of rings in the previous section to the Euclidean ring we have at hand,* $\mathbb{Z}[i]$.

Lemma III.6.1
Let p *be a prime integer and suppose that for some integer* c *relatively prime to* p *we can find integers* x *andy such that* $x^2 + y^2 = cp$. *Then* p *can be written as the sum of squares of two integers, that is, there exist integers* a *and* b *such that* $p = a^2 + b^2$.

Proof III.6.2
The ring of integers is a subring of $\mathbb{Z}[i]$. *Suppose that the integer* p *is also a prime element of* $\mathbb{Z}$. *Since* $cp = x^2 + y^2 = (x + yi)(x - yi)$, $p \mid (x + yi)$ *or* $p \mid (x - yi)$ *in* $\mathbb{Z}[i]$. *But if* $p \mid (x + yi)$ *then* $x + yi = p(u + vi)$ *which would say that* $x = pu$ *and* $y = pv$ *so that* p *also would divide* $x' - yi$. *But then* $p^2 | (x + yi)(x - yi) = cp$ *from which we would conclude that* $p \mid c$ *contrary to assumption. Similarly if* $p \mid (x - yi)$. *Thus* p *is not a prime element in* $\mathbb{Z}[i]$ *! In consequence of this,*

$$p = (a + bi)(g + di).$$

where $a + bi$ *and* $g + di$ *are in* $\mathbb{Z}[i]$ *and where neither* $a + bi$ *nor* $g + di$ *is a unit in* $\mathbb{Z}[i]$. *But this means that neither* $a^2 + b^2 = 1$ *nor* $g^2 + d^2 = 1$. *From* $p = (a + bi)(g + di)$

it follows easily that $p = (a - bi)(g - di)$. *Thus,*

$$p = (a + hi)(g + di)$$

where $a + bi$ *and* $g + di$ *are in* $\mathbb{Z}[i]$ *and where neither* $a + bi$ *nor* $g + di$ *is a unit in* $\mathbb{Z}[i]$. *But this means that neither* $a^2 + b^2 = 1$ *nor* $g^2 + d^2 = 1$. *From* $p = (a + bi)(g + di)$ *it follows easily that* $p = (a - bi)(g - di)$. *Thus,*

$$p^2 = (a + bi)(g + di)(a - hi)(g - di) = (a^2 + b^2)(g^2 + d^2).$$

Therefore

$$(a^2 + b^2 | P^2)$$

so $a^2 + b^2 = 1, p$ *or* p^2; $a^2 + b^2 \neq -1$ *since* $a + bi$ *is not a unit, in* $\mathbb{Z}[i]$;
$a^2 + b^2 \neq -p^2$, *otherwise* $g^2 + d^2 = 1$, *contrary to the fact that* $g + di$ *is not a unit in* $\mathbb{Z}[i]$.
Thus the only feasibility left is that $a^2 + b^2 = p$ *and the lemma is thereby established.*
The odd prime numbers divide into two classes, those which have a remainder of 1 *on division by* 4 *and those which have a remainder of* 3 *on division by* 4. *We aim to show that every prime number of the first kind can be written as the sum of two squares, whereas no prime in the second class can be so represented.* □

Lemma III.6.2
If p *is a prime number* r *if the form* $4n + 1$, *then we can solve the congruence*
$x^2 = -1$ *mod* p.

Proof III.6.3
Let $x = 1 \cdot 2 \cdot 3 \cdots (P - 1)|2$. *Since,* $p - 1 = 4n$, *in this product for* x *there are an even number of terms, in consequence of which*

$$X = (-1)(-2)(-3)... \left(- \left(\frac{p-1)}{2} \right) \right.$$

But $p - k = -k$ *mod* p, *so that*

$$\begin{aligned} x^2 \equiv & \left(1.2... \frac{p-1}{2} \right) (-1)(-2)... \left(- \left(\frac{p-1}{2} \right) \right) \\ \equiv & 1.2... \frac{p-1}{2} \frac{p+1}{2} ... (p-1) \\ \equiv & (p-1)! = -1 mod p. \end{aligned}$$

We are using here Wilson's theorem, proved earlier, namely that if p *is a prime number* $(p - 1)! \equiv -l(p)$. *To illustrate this result, if* $p = 13$,

$$x = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720 = 5 mod 13$$

and

$$5^2 = -1 mod 13.$$

□

Theorem III.6.2 (**Fermat**)
If p is a prime number of the form $4n+1$, then $p = a^2 + b^2$ for some integers a, b.

Proof III.6.4
By previous Lemma there exists an x such that $x^2 = -1 \bmod p$. The x can be chosen so that $0 \leq x \leq p-1$ since we only need to use the remainder of x on division by p.
We can restrict the size of x even further, namely to satisfy $|x| \leq \frac{p}{2}$.
For if $x > \frac{p}{2}$, then $y = p - x$ satisfies $y^2 = -1 \bmod p$ but $|Y| \leq \frac{p}{2}$. Thus we may assume that we have an integer x such that $|x| \leq \frac{p}{2}$ and $x^2 + 1$ is a multiple of p, say cp. Now $cp = x^2 + 1 \leq \frac{p^2}{4} + 1 < p^2$, hence $c < p$ and so $p \nmid c$. Invoking the previous lemma we obtain that $p = a^2 + b^2$ for some integers a and b, proving the theorem. □

III.7 Noetherian Ring

We now introduce Noetherian rings, left Noetherian rings, and right Noetherian rings in this section and prove Hilbert basis theorem.

Definition III.7.1 *[5]*
A ring R is Noetherian (or left Noetherian, or right Noetherian, respectively) if any chain of ideals (or left ideals, or right ideals, respectively) of R.

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$$

satisfies ACC, i.e., there is some $n \in \mathbb{N}$ such that $I_n = I_{n+1} = I_{n+2} = ...$

Example III.7.1
1. Every finite ring is Noetherian, left Noetherian and right Noetherian.
2.Every principal ideal domain D is Noetherian. This is because any nonzero and nonunit $a \in D$ has only finitely factors up to associates.

We have the following proposition that makes Noetherian rings much more concrete, and makes it obvious why PIDs are Noetherian.

Definition III.7.2 *(Finitely generated ideal)[5]*
An ideal I of a ring R is finitely generated if there are $r_1 \cdots r_n \in R$ such that, $I = \langle r_1, ..., r_n \rangle$. We can define finitely-generated left ideals and finitely-generated right ideals.

Proposition III.7.1
A ring R is Noetherian (or left Noetherian, or right Noetherian, respectively) if and only if every ideal (or left ideal, or right ideal, respectively) of R is finitely generated.

Proof III.7.1
We suppose that every ideal of R is finitely generated. Given the chain $I_1 \subseteq I_2 \subseteq \cdots$, *we have the ideal*

$$I = I_1 \cup I_2 \cup I_3 \cup \cdots$$

We know I is finitely generated, say $I = \langle r_1, ..., r_n \rangle$ *, with* $r_i \in I_{k_i}$. *Let*

$$n = max\left\{k_i\right\}, \quad i = \overline{1;n}.$$

Then $r_1, \cdots, r_n \in I_k$. *So* $I_n = I$, *and furthermore* $I_n = I_{n+1} = I_{n+2} = \cdots$
Conversely, we suppose there is an ideal $I \lhd R$ *that is not finitely generated.*
We pick $r_1 \in I$. *Since I is not finitely generated, we know* $(\langle r_1 \rangle \neq I)$.
So we can find some $r_2 \in I\ (r_1)$. *Again* $\langle r_1, r_2 \rangle \neq I$. *So we can find* $r_3 \in I\ \langle r_1, r2 \rangle$. *We continue on, and then can find an infinite strictly ascending chain*

$$\langle r_1 \rangle \subseteq \langle r_1, r_2 \rangle \subseteq \langle r_1, r_2, r_3 \rangle \subseteq \cdots$$

So R is not Noetherian.
For left Noetherian, or right Noetherian cases the proof is similar.
If R is Noetherian, not necessarily every subring of R has to be Noetherian. □

Proposition III.7.2
Let R be a Noetherian ring and $I \lhd R$. *Then* R/I *is Noetherian.*

Proof III.7.2
Considering the natural homomorphism:

$$\pi : R \longrightarrow R/I$$

$$x \longmapsto x + I.$$

Let $J \trianglelefteq R/I$. *We want to show that J is finitely generated. We know that* $\pi^{-1}(J) \trianglelefteq R$, *and is hence finitely generated, since R is Noetherian. So* $\pi^{-1}(J) = \langle r_1, \cdots, r_n \rangle$ *for some* $r_1, \cdots, r_n \in R$ *is generated by* $\pi(r_1), \cdots, \pi(r_n)$.
So R/I *is Noetherian by Proposition III.7.1.*

□

III.8 boolean ring

Definition III.8.1 *[4]*
A Boolean ring is a ring of more than one element with the property that :

$$x^2 = x$$

for every element x. It is at once evident that a ring of subclasses of a given class is an example of a Boolean ring. Also the ring I_2 of integers modulo 2 is a Boolean ring of two elements which is, in fact, isomorphic to the ring of all subclasses of a class of one element. Another example of a Boolean ring is the set of four elements $0, 1, a, b$, where 0 is the zero and 1 the unit element, sums and products being otherwise defined by:

$$a + b = b + a = 1$$

$$a + 1 = 1 + a = b, b + 1 = 1 + b = a$$

$$1 + 1 = 0, a + a = 0, b + b = 0$$

$$a^2 = a, b^2 = b$$

We proceed to prove some properties of an arbitrary Boolean ring. Let a be any element of the Boolean ring B. By applying $x^2 = x$ to the element $2a$, we see that $4a^2 = 2a$.
But $a^2 = a$; hence $4a = 2a$, or $2a = 0$ Hence, in particular, $x = -x$ for every x in B. It is now easy to show that a Boolean ring is necessarily commutative. Let a and b be any elements of B, and applying $x^2 = x$ to $a + b$; thus

$$(a + b)^2 = a^2 + ab + ba + b^2 = a + b.$$

Since $a^2 = a, b^2 = b$, it follows that $ab + ba = 0$. That is, $ab = -ba = ba$, and B is commutative.

III.9 Relationship between different types of rings

We now establish some containments between these various types of rings. The results are summarized in the following theorem.

Theorem III.9.1
{ fields } ⊂ { Euclidean domains } ⊂ { principal ideal domains } ⊂ { unique factorization domains } ⊂ { integral domains }

1. Fields are Euclidean domain :
Given any field F, define a norm n on F by setting $n(a) = 0$ for all $a \neq 0$ in F. This satisfies the division algorithm because we can always divide without even needing remainders (it is a field).
2. Euclidean domains are PIDs :
Starting with any Euclidean domain R, and picking an arbitrary ideal I in R (we can assume it is nonzero since the zero ideal is already principal). We need to show it can be generated by one element.
First we have to choose this element. Well, it should be the "smallest". So let f be a nonzero element of I of smallest norm (there may be more than one choice for f, as in using 3 or -3 to generate $\langle 3 \rangle$ in $\mathbb{Z}$). How do we know that there is an element of smallest norm? Well, We look at the set of all norms of all nonzero elements of R. It is a subset of $\mathbb{N} \backslash \{0\}$, so it has a smallest element ($\mathbb{N}$ is "well-ordered").
Now we have got our putative generator, and we have to show that everything else in I can be written as a multiple of f . So picking any other nonzero g in I, and do the division algorithm on g by f. This gives a quotient q and remainder r satisfying $g = qf + r$, where r has smaller norm than f (or else is 0). But since f and g are both in the ideal I, and $r = g - qf$, r must also be in I. Since f has smallest norm in I, we cannot have $n(r) < n(f)$, and therefore $r = 0$, which shows that f divides g, hence g is a multiple of f . Since g was arbitrary in I, this shows that $I = (f)$.
PIDs are UFDs :
We start with a $PIDR$, and we have to show it is a UFD, which breaks into two parts: 1. showing that any element can be factorized into finitely many irreducibles, and 2. showing that this factorization is unique (in the sense of the definition of UFD). Here is a sketch of step 1: Picking an element r of R. If it is zero or a unit, we have no need to factorize. So we assume r is nonzero and not a unit. It is either irreducible, or it is not. If irreducible, we are done. If not, it has two proper non-unit factors. Repeating the process for these factors. Keep repeating this process until we reach irreducible elements. Problem: what if the process does not stop? To see that it stops, supposing for contradiction that a certain element could be factored indefinitely: in this case we would be able to produce a chain of distinct ideals $\langle a_1 \rangle \subset \langle a_2 \rangle \subset ...$ (by taking as generator, one of the new factors in each successive factorization).

Then if we take the union of all these ideals, it is $\langle a \rangle$ still an ideal and $\langle b \rangle$ principal (we are in a PID). Then we would have to check that its generator is equal to one of the a_i (up to a unit). But it would also be equal to a_{i+1}, etc, (up to units), and we supposed the ideals were all distinct -contradiction. This shows that in a PID, the process of breaking off irreducibles stops after finitely many steps. For the uniqueness, one makes an inductive argument on the number of irreducibles in a factorization.

UFDs are integral domains :

This is built into the definition: UFDs, PIDs , and EDs all have a "D" for domain.

III.10 The characteristic of a ring

Definition III.10.1 *[7]*

Let R be a ring. If there is a positive integer n such that $na = 0$ for all $a \in R$ then the least such n is called the characteristic of R and denoted by **Char**. *If there is no such n then R is said to have characteristic* 0

Examples III.10.1

1. Char $(\mathbb{Z}) = 0$, *Char* $(\mathbb{Q}) = 0$, *Char* $(\mathbb{R}) = 0$, *Char* $(\mathbb{C}) = 0$.

2. Char $(n\mathbb{Z}) = n$, *since* $\forall \bar{x} \in n\mathbb{Z}, n\bar{x} = \bar{0}$.

IV Polynomial Rings

IV.1 Polynomial Rings

Polynomial rings are important in various branches of mathematics, including algebra, number theory, and algebraic geometry. They provide a framework for studying polynomial equations, wich are fundamental in many areas of mathematics and application in science and engineering.
Polynomial rings also play a crucial role in fields like coding theory, cryptography, and computer science, where they are used in error-correcting codes, cryptographic algorithms, and polynomial time complexity analysis. Additionally, polynomial rings serve as a bridge between abstract algebraic concepts and concrete polynomial computations, making them essential tools for theorical and computational investigations.

Definition IV.1.1 *[2]*
Let R be a commutative ring which has a nonzero identity element 1. A polynomial in the indeterminate X over R is an expression of the form

$$a_0 + a_1X + \cdots + a_nX^n. \tag{IV.1}$$

where n is a positive integer and $a_0, a_1, a_2, ..., a_n \in R$. We call a_i the i^{th} coefficient of the polynomial. We denote this ring $R[x]$.

Notation IV.1.1
The terms in the expression $IV.1$ above may be written in any order, and if $a_i = 0$ the corresponding term may be omitted. Similarly we may omit unnecessary coefficients equal to 1 (writing 'X' instead of '$1X$', and so on). Thus if

$$P = 2 + X^3 - 5X$$

then the 0^{th} coefficient of P is 2, the 1^{st} coefficient is -5, the 2^{nd} is 0, the 3^{rd} is 1. It is also convenient to say that the 4^{th} , 5^{th}, $\cdots$ coefficients are zero (rather than saying that they do not exist). Thus a polynomial always has an infinite sequence of coefficients, one for each nonnegative integer, but all the coefficients beyond some point must be zero.

Definition IV.1.2 *[2]*
The polynomial all of whose coefficients are zero is called the zero polynomial.

Definition IV.1.3 *[2]*
P is a polynomial the largest i for which the i^{th} coefficient is nonzero is called the degree of P , and this coefficient is called the leading coefficient of P.
So if $P = a_0 + a_1X + \cdots + a_nX^n$ with $a_n \neq 0$ then a_n is the leading coefficient and $deg(P) = n$. Noting that we do not define the degree of the zero polynomial. In some treatments the zero polynomial is said to have degree $-\infty$. It would not be suitable to define the degree of the zero polynomial to be zero.
If P is a polynomial in the indeterminate X we often write '$P(X)$' instead of just 'P' to remind ourselves that P is a polynomial or to remind ourselves that the indeterminate is X.

IV.1.1 Addition and multiplication of polynomials

Definition IV.1.4 *[2]*
Let R be a commutative ring with 1 *and let $a, b \in R[X]$. Let a_i, b_i be the i^{th} coefficients of a, b (for $i = 0, 1, 2, \ldots$). Define $a + b$ to be the polynomial with i^{th} coefficient $a_i + b_i$, and define ab to be the polynomial with i^{th} coefficient $a_ib_0 + a_{i-1}b_1 + \ + a_0b_i$ (for $i =$ $0, 1, 2, \ldots$).*

By definition, if

$$a = a_0 + a_1X + \cdots + a_nX^n$$
$$b = b_0 + b_1X + \cdots + b_mX^m$$

then

$$a + b = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots$$
$$ab = a_0b_0 + (a_1b_0 + a_0b_1)X + (a_2b_0 + a_1b_1 + a_0b_2)X^2 + \cdots$$

Theorem IV.1.1
If R is a commutative ring with 1 *and X is an indeterminate then $R[X]$ is a commutative ring with* 1*.*

Proof IV.1.1
We must check the axioms in ring definition and the commutative law for multiplication, and find an identity element. It will be convenient to use the same notation as in the definition above: if P is a polynomial, then P_i is the i^{th} coefficient of P. Let $a, b, c \in R[X]$. Then for all i :

$$\begin{aligned}((a + b) + c)_i =& (a + b)_i + c_i = (a_i + b_i) + c_i \\ =& a_i + (b_i + c_i) = a_i + (b + c)_i = (a + (b + c))_i\end{aligned}$$

and so $(a+b)+c = a+(b+c)$. The proof that $a+b = b+a$ is similar. The i^{th} coefficient of ab is the sum of all terms $a_r b_s$ with $r+s=i$; that is,

$$(ab)_i = \sum_{r+s=i} a_r b_s.$$

in a convenient notation. We find that:

$$\begin{aligned}((ab)c)_i &= \sum_{r+s=i} (ab)_r c_s \\ &= \sum_{r+s=i} \left(\sum_{u+v=r} a_u b_v \right) c_s \\ &= \sum_{u+v+s=i} (a_u b_v)\, c_s \\ &= \sum_{u+v+s=i} a_u (b_v c_s) \\ &= \sum_{u+t=i} a_u \left(\sum_{v+s=t} b_v c_s \right) \\ &= \sum_{u+t=i} a_u (bc)_t \\ &= (a(bc))_i.\end{aligned}$$

and therefore $(ab)c = a(bc)$. Similarly,

$$\begin{aligned}(a(b+c))_i &= \sum_{r+s=i} a_r (b+c)_s \\ &= \sum_{r+s=i} a_r (b_s + c_s) \\ &= \sum_{r+s=i} a_r b_s + a_r c_s \\ &= \sum_{r+s=i} a_r b_s + \sum_{r+s=i} a_r c_s \\ &= (ab)_i + (ac)_i.\end{aligned}$$

Similar proofs also apply for the other distributive law and the commutativity of multiplication.
If we define z to be the polynomial for which $z_i = 0$ for all i then it is readily checked that $(a+z)_i = a_i = (z+a)_i$ for all $a \in R[X]$, so that z is a zero element for $R[X]$. It is also easily seen that $-a$ defined by $(-a)_i = -(a_i)$ for all i satisfies $a + (-a) = z = (-a) + a$; so each $a \in R[X]$ has a negative.
Finally, define e to be the polynomial for which the 0^{th} coefficient is the identity element of R and all the other coefficients are equal to zero.
That is, $e = 1 + 0X + 0X^2 + \cdots$. Then for all $a \in R[X]$,

$$(ae)_i = a_i e_0 + a_{i-1} e_1 + \cdots + a_0 e_i = a_i.$$

Since $e_0 = 1$ and $e_j = 0$ for $j \neq 0$. Thus $ae = a$, and since also $ea = a$, it follows that,

e is an identity. □

Theorem IV.1.2
Let R be an integral domain and a and b nonzero polynomials over R. Then the leading coefficient of ab is the product of the leading coefficients of a and b, and $deg(ab) = deg(a) + deg(b)$.

Proof IV.1.2 *1. Let n be the degree of a and m the degree of b. If* $r + s > n + m$ *then necessarily either* $r > n$ *or* $s > m$, *and so either* $ar = 0$ *or* $bs = 0$. *Hence if* $i > n + m$ *then*

$$(ab)_i = \sum_{r+s=i} a_r b_s = 0.$$

Similarly

$$(ab)_{n+m} = \sum_{r+s=n+m} a_r b_s = a_n b_m.$$

since all other terms have either $r > n$ *or* $s > m$. *Since* $a_n \neq 0$*and* $b_m \neq 0$ *and R is an integral domain it follows that* $(ab)_{n+m} \neq 0$. *Thus* $n + m$ *is the largest value of i for which* $(ab)_i \neq 0$ *and so*

$$deg(ab) = n + m = deg(a) + deg(b).$$

Moreover, the leading coefficient of ab is $(ab)_{n+m}$, *and, as we have seen, it is equal to* $a_n b_m$, *the product of the leading coefficients of a and b.* □

IV.1.2 Constant polynomials

Let R be a commutative ring with 1 . *For each* $a \in R$ *there is a polynomial for which the* 0^{th} *coefficient is a and all the other coefficients are zero. Using the notation described in* $IV.1$ *this polynomial would be denoted by 'a' ; our notation does not distinguish between elements of R and these so-called constant polynomials. However, for the purposes of the next theorem we need a notation which does distinguish; so, temporarily, we will denote the constant polynomial a by* $c(a)$. *(That is,* $c(a) = a + 0X + 0X^2 + \cdots$).

Theorem IV.1.3
The set $S = \{c(a) | a \in R\}$ *of constant polynomials is a subring of* $R[X]$ *isomorphic to R, and the function* $c : R \longrightarrow S$ *defined by* $a \longmapsto c(a)$ *is an isomorphism.*

Proof IV.1.3
we denote the i^{th} *coefficient of P by* P_i. *Then for all* $a \in R$ *we have* $c(a)_0 = a$ *and* $c(a)_i = 0$ *for all* $i > 0$.
Let $a, b \in R$ *with* $c(a) = c(b)$. *Then* $a = c(a)_0 = c(b)_0 = b$. *Thus c is injective. Since every constant polynomial is of the form* $c(a)$ *for some* $a \in R$, *c is surjective also. Furthermore, c preserves addition and multiplication,since*

$$c(a + b)_0 = a + b = c(a)_0 + c(b)_0 = (c(a) + c(b))_0.$$

$$c(ab)_0 = ab = c(a)_0c(b)_0 = \sum_{r+s=0} c(a)_r c(b)_s = (c(a)c(b))_0.$$

and for $i > 0$

$$c(a+b)_i = 0 = 0+0 = c(a)_i + c(b)_i = (c(a)+c(b))_i.$$

$$c(ab)_i = 0 = \sum_{r+s=i} c(a)_r c(b)_s = (c(a)c(b))_i.$$

(since in each term of the sum either $c(a)r = 0$ *or* $c(b)s = 0$*). It remains to check that* S *is indeed a subring of* $R[X]$*. Now clearly* S *is nonempty, since it contains the zero polynomial. If* x *and* y *are arbitrary elements of* S *then* $x = c(a)$*,* $y = c(b)$ *for some* $a, b \in R$ *, and*

$$x + y = c(a) + c(b) = c(a+b) \in S,$$
$$xy = c(a)c(b) = c(ab) \in S,$$
$$-x = -c(a) = c(-a) \in S.$$

(the last line following from the fact that the negative of a polynomial is obtained by taking the negatives of all the coefficients). Then, S *is a subring.* □

IV.1.3 Polynomial functions

Any polynomial function $P(x) = a_0 + a_1x + \cdots + a_nx^n$ *in* $R[x]$ *determines a function*

$$R \longrightarrow R$$
$$c \longmapsto a_0 + a_1c + \cdots + a_nc^n,\ \forall c \in R.$$

Polynomial functions are no doubt very familiar to the reader, but for us it is important to distinguish between polynomials, sometimes called polynomial forms, and polynomial functions. Note, for instance, that two distinct polynomials can give the same function. For example, if $P(x) = X^2$ *and* $q(X) = X$ *in* $\mathbb{Z}_2[X]$ *then*
$p(\bar{0}) = (\bar{0})^2 = 0 = q(0)$ *and* $p(\bar{1}) = (\bar{1})^2 = 1 = q(1)$*,*
so that $p(c) = q(c)$ *for all* $c \in \mathbb{Z}_2$ *. So the functions* $c \mapsto p(c)$ *and* $c \mapsto q(c)$ *are equal. However the polynomials* p *and* q *themselves are not equal since they have different coefficients.*

IV.1.4 Evaluating homomorphisms

If c *is any element of* R*, there is a function:*

$$e_c : R[X] \mapsto R$$
$$p(X) \mapsto p(c).$$

In other words, $e_c(p(X)) = p(c)$ *for all polynomials* p*.*

Theorem IV.1.4
For each $c \in R$ *the map* $e_c : R[X] \longrightarrow R$ *is a homomorphism.*

Proof IV.1.4 *Let $c \in R$ and let $p, q \in R[X]$. Then, in the notation we have been using for the i^{th} coefficient of a polynomial,*

$$\begin{aligned} e_c(pq) =& (pq)_0 + (pq)_1 c + (pq)_2 c^2 + \cdots \\ =& p_0 q_0 + (p_0 q_1 + p_1 q_0)c + (p_0 q_2 + p_1 q_1 + p_2 q_0)c^2 + \cdots \\ =& (p_0 + p_1 c + p_2 c_2 + \cdots)(q_0 + q_1 c + q_2 c^2 + \cdots) \\ =& e_c(p) e_c(q). \end{aligned}$$

and similarly

$$\begin{aligned} e_c(p+q) =& (p+q)_0 + (p+q)_1 c + (p+q)_2 c^2 + \cdots \\ =& (p_0 + q_0) + (p_1 + q_1)c + (p_2 + q_2)c^2 + \cdots \\ =& (p_0 + p_1 c + p_2 c^2 + \cdots)(q_0 + q_1 c + q_2 c^2 + \cdots) \\ =& e_c(p) + e_c(q). \end{aligned}$$

□

Remarks IV.1.1

1. *The function e_c is called an evaluation homomorphism since it maps $p(X) \in R[X]$ to $p(X)$ evaluated at c (that is, to $p(c)$).*
2. *To say that e_c preserves addition is to say that the result of adding two polynomials and then putting $X = c$ is the same as first putting $X = c$ in each and then adding. A similar statement applies for multiplication. The reason it works is because we have defined addition and multiplication of polynomials to make it work when adding or multiplying polynomials the indeterminate X is treated as though it is an element of R.*
3. *If R is a subring of a ring S then $R[X]$ is a subring of $S[X]$. For instance, the set of all polynomials with rational coefficients is a subring of the set of all polynomials with real coefficients. Hence, if c is any element of S the homomorphism $e_c : S[X] \mapsto S$ may be restricted to $R[X]$ to yield a homomorphism from $R[X]$ to S. Thus, for instance, the map $\phi : \mathbb{Q}[X] \mapsto \mathbb{R}$ given by $\phi(p(X)) = p(2^{\frac{1}{3}})$ is a homomorphism.*

IV.2 Polynomial rings over field

Our chief application of polynomials in this section will be to study field extensions. Roughly speaking, if F is a field we wish to be able to make a larger field by adjoining extra elements to F, in much the way that the complex numbers are obtained from the real numbers by adjoining a square root of -1. We have already seen how $F[X]$ can be regarded as a ring obtained by adjoining the element X to F. However, $F[X]$ is not a field, and to obtain fields extending F we will have to deal with quotient rings of $F[X]-$ rings obtained from $F[X]$ in the same way as $\mathbb{Z}_n$ is obtained from $\mathbb{Z}$. Once we have developed the theory of field extensions we will be able to prove things about the field of constructible numbers, which is an extension field of $\mathbb{Q}$ (rational numbers).

IV.2.1 The division Algorithm for Polynomials Over a Field

We start by investigating properties of divisibility and factorization for polynomials properties analogous to those properties of $\mathbb{Z}$ which were used in our construction of $\mathbb{Z}$.

Theorem IV.2.1 *Let F be a field and $f(X), g(X)$ elements of $F[X]$, with $g(X) \neq 0$. Then there exist unique $q(X)$ and $r(X)$ in $F[X]$ such that both the following hold:*

1. $f(X) = q(X)g(X) + r(X)$.
2. *Either $r(X) = 0$ or $deg(r(X)) < deg(g(X))$.*

Proof IV.2.1 *We first prove the existence of such polynomials $q(X)$ and $r(X)$.*
Let

$$S = \{f(X) - k(X)g(X),\ k(X) \in F[X]\}.$$

If $0 \in S$ then there is a polynomial $k(X) \in F[X]$ with $f(X) = k(X)g(X)$, and we may take $q(X) = k(X)$ and $r(X) = 0$. Assume therefore that $0 \notin S$.
The set of nonnegative integers $K = \{deg(p(X)), \quad p(X) \in S\}$ is nonempty, and therefore has at least element d. Let $r(X) \in S$ be such that $deg(r(X)) = d$, and let $q(X)$ be such that $f(X) - q(X)g(X) = r(X)$ (possible since $r(X) \in S$). It suffices to prove that $d < deg(g(X))$; so supposing that this is not true.
Let $deg(g(X)) = m$ and let the leading coefficients of $r(X)$ and $g(X)$ be a and b respectively. Now $ab^{-1}X^{d-m}g(X)$ has degree $(d-m) + deg(g) = d$ and leading coefficient (ab^{-1}) (leading coefficient of g) $= a$; thus it has the same degree and leading coefficient as $r(X)$. It follows that the d^{th} and all higher coefficients of $s(X) = r(X) - ab^{-1}X^{d-m}g(X)$ are zero. Moreover, $s(X) = f(X) - q(X)g(X) - ab^{-1}X^{d-m}g(X) = f(X) - k(X)g(X) \in S$ where $k(X) = q(X) + ab^{-1}X^{d-m}g(X)$. Thus $s(X)$ is a element of S of smaller degree than $r(X)$, contradicting the choice of $r(X)$. Thus the assumption that $d \geq m$ leads to a contradiction, and $d < m$, as required. We have still to prove the uniqueness of q and r; so assume that q_1 and r_1 satisfy the same two properties; that

is,$f = q_1g + r_1$ and either $r_1 = 0$ or $deg(r_1) < deg(g)$. Then $q_1g + r_1 = qg + r$, and so $r_1 - r = (q - q_1)g$.
Now if $q - q_1 \neq 0$ then by Theorem IV.1.2

$$deg(r_1 - r) = deg(q - q_1) + deg(g) < deg(g)$$

which is impossible since the i^{th} coefficients of both r_1 and r are zero for $i > deg(g)$. Hence $q_1 = q$, and this gives $r_1 = f - q_1g = f - qg = r$ also. □

Theorem IV.2.2 **The Remainder theorem**
Let $c \in F$ and $f(X) \in F[X]$, where F is a field. Then the remainder in the division of $f(X)$ by $X - c$ is $f(c)$.

Proof IV.2.2 *By the previous theorem we have $f(X) = (X - c)q(X) + r$, where either $r = 0$ or $deg(r) < 1$. In either case r must be a constant polynomial; that is, an element of F. Evaluating at c gives*

$$f(c) = e_c(f(X)) = e_c(X - c)e_c(q(X)) + e_c(r) = 0q(c) + r = r.$$

□

Theorem IV.2.3 **The Factor Theorem**
If $f(X) \in F[X]$ then $X - c$ is a factor of $f(X)$ if and only if $f(c) = 0$.

Proof IV.2.3 *Since $(X - c) \mid f(X)$ if and only if the remainder on dividing $f(X)$ by $X - c$ is zero, IV*.2.1 *yields that $(X - c) \mid f(X)$ if and only if $f(c) = 0$.* □

IV.2.2 The Euclidean Algorithm

Let F be a field.

Definition IV.2.1 *[2]*
(i) Two polynomials $f(X)$ and $g(X)$ in $F[X]$ are said to be associates if $f(X) = cg(X)$ for some nonzero $c \in F$.
(ii) A polynomial $f(X) \in F[X]$ is said to be monic if it is nonzero and has leading coefficient 1.

Remark IV.2.1
Obviously for any nonzero polynomial $f(X)$ there is a unique monic polynomial which is an associate of $f(X)$ namely, $a^{-1}f(X)$, where a is the leading coefficient of $f(X)$.

Proposition IV.2.1
Nonzero polynomials $f(X)$ and $g(X)$ in $F[X]$ are associates if and only if $f(X) \mid g(X)$ and $g(X) \mid f(X)$.

Proof IV.2.4
If f and g are associates then for some $c \in F$ we have $f = cg$ and $g = c^{-1}f$, so that $g \mid f$ and $f \mid g$. Conversely, assume that $f \mid g$ and $g \mid f$. Then $f = q_1 g$ and $g = q_2 f$ for some $q_1, q_2 \in F[X]$, both of which are nonzero since f and g are. Thus by Theorem IV.1.2 (i) we have:

$$deg(f) = deg(q_1) + deg(g) \geq deg(g) = deg(q_2) + deg(f).$$

Hence $deg(q_2) = 0$, and therefore q_2 is a nonzero element of F, showing that f and g are associates. □

Theorem IV.2.4
If $a(X)$ and $b(X)$ are polynomials in $F[X]$ which are not both zero then there exists a unique monic polynomial $d(X) \in F[X]$ such that both the following conditions are satisfied:

1. *$d\ (X) \mid a(X)$ and $d(X) \mid b(X)$.*

2. *$c(X) \mid a(X)$ and $c(X) \mid b(X)$ then $c(X) \mid d(X)$.*
   Moreover, there exist $m(X), n(X) \in F[X]$ with $d(X) = m(X)a(X) + n(X)b(X)$.

Proof IV.2.5 *Let $a(X)$ and $b(X)$ be elements of $F[X]$ which are not both zero.*
We first prove the existence of a $d(X)$ with the required properties. Define S to be the set of all nonzero polynomials $p(X)$ in $F[X]$ such that $p(X) = m(X)a(X) + n(X)b(X)$ for some $m(X), n(X) \in F[X]$, and observe that $S \neq \emptyset$; since it must contain either $a(X)$ or $b(X)$. Hence the set of nonnegative integers $K = deg(p(X)) \mid p(X) \in S$ is nonempty, and must therefore contain a least element, k. Let $d(X)$ be an element of S which is monic and has degree k. (By the previous remark we can choose $d(X)$ to be monic, since associates of elements of S are also in S). Since $d(X) \in S$ the definition of S yields the existence $m(X)$ and $n(X)$ with $d(X) = m(X)a(X) + n(X)b(X)$, and from this it follows that if $c(X) \mid a(X)$ and $c(X) \mid b(X)$ then $c(X)(m(X)a(X) + n(X)b(X)) = d(X)$. Thus we have established two of the properties of $d(X)$ and have only to prove that $d(X) \mid a(X)$ and $d(X) \mid b(X)$. Supposing that $d(X) \nmid a(X)$, and let $r(X)$ be the remainder on division of $a(X)$ by $d(X)$. Then $r(X) \neq 0$, and since $r(X) = a(X) - q(X)d(X)$ for some $q(X)$, we obtain

$$\begin{aligned} r(X) =& a(X) - q(X)(m(X)a(X) + n(X)b(X)) \\ =& (1 - q(X)m(X))a(X) - q(X)b(X). \end{aligned}$$

so that $r(X) \in S$. But this contradicts the definition of k, since the degree of $r(X)$ is less than $deg(d(X)) = k$. Thus $d(X) \mid a(X)$ and, by a similar argument, $d(X) \mid b(X)$ also. It remains to prove uniqueness. So, let d_1 and d_2 be monic polynomials such that conditions 1 and 2 are satisfied with d replaced by d_1 and also with d replaced by d_2. By 1 for d_1 and 2 for d_2 it follows that $d_1 \mid d_2$, and by 1 for d_2 and 2 for d_1 it follows that $d_2 \mid d_1$. By the previous proposition we deduce that d_1 and d_2 are associates of each other, and hence, by the previous remark, $d_1 = d_2$. □

Remark IV.2.2
The polynomial $d(X)$ in previous theorem is called the greatest common divisor of $a(X)$ and $b(X)$.
As in the case of integers, the greatest common divisor of two polynomials can be calculated by use of the Euclidean Algorithm (which is almost exactly the same for polynomials as integers):
Given $a, b \in F[X]$ with $a \neq 0$, $b \neq 0$ and $deg(a) \geq deg(b)$ (or $b = 0$, $a \neq 0$), let a be the gcd of in the initial two polinomials.
Alternatively, let a_1, a_2 be the initial polynomials, and define $a_3, a_4, \cdots$ by

$$\begin{aligned} a_1 &= q_3 a_2 + a_3 \quad deg(a_3) < deg(a_2) \\ a_2 &= q_4 a_3 + a_4 \quad deg(a_4) < deg(a_3) \\ &\cdots \\ a_{k-2} &= q_k a_{k1} + a_k \quad deg(a_k) < deg(a_{k1}) \\ a_{k-1} &= q_{k+1} a_k \qquad (a_{k+1} = 0). \end{aligned}$$

The algorithm must terminate eventually since the remainder on dividing a_{i-1} by a_i is either zero or a polynomial of degree strictly less than that of a_i. Since the degree of a nonzero polynomial is always a nonnegative integer, and it is impossible to have an infinite decreasing sequence of nonnegative integers, it must eventually happen that we get a remainder of zero. (For instance, if $deg(a_i) = 0$ then we will certainly find that $a_{i+1} = 0$; a polynomial of degree 0 is always a divisor of any other polynomial.) As for integers, the set of common divisors of a_{i-1} and ai remains unchanged throughout the algorithm, and hence

$$gcd(a_1, a_2) = gcd(a_2, a_3) = \cdots = gcd(a_k, a_{k+1}).$$

But $gcd(a_k, a_{k+1}) = gcd(a_k, 0)$, which is the unique monic associate of a_k. (The greatest common divisor is always monic, by definition; so, for instance,

$$gcd(2X + 3, 0) = X + \frac{3}{2}.$$

Thus we conclude that the gcd of a_1 and a_2 is the unique monic associate of the last nonzero remainder obtained in the Euclidean Algorithm.

IV.2.3 Irreducible Polynomials

Let F be a field and let $p \in F[X]$. Then for any nonzero $c \in F$ the equation
$p(X) = c(c^{-1}p(X))$ shows that c is a divisor of p. Similarly all associates of p are divisors of p. Polynomials which have only these trivial divisors are of considerable theoretical importance.

Definition IV.2.2 *[2]*
A polynomial $p \in F[X]$ is said to be irreducible (or prime) if $deg(p) \geq 1$ and the only divisors of p in $F[X]$ are polynomials of degree 0 and associates of p.

Remark IV.2.3

1. *If p is irreducible and $p(X) = d_1(X)d_2(X)$ then either d_1 is an associate of p, in which case $deg(d_2) = 0$, or $deg(d_1) = 0$, in which case d_2 is an associate of p.*
2. *If p is reducible (that is, not irreducible) and $deg(p) \geq 1$ then p has a divisor d_1 satisfying*

(i) $deg(d_1) \geq 1$.

(ii) *d_1 is not an associate of p. Since d_1 is a divisor of p we have $p(X) = d_1(X)d_2(X)$ for some d_2 , and (ii) above implies that $deg(d_2) \geq 1$. This combined with (i) above and the equation*

$$deg(p) = deg(d_1) + deg(d_2)$$

yields that

$$1 \leq deg(d_i) \leq deg(p) - 1$$

for $i = 1$ and $i = 2$.

3. *If $deg(p) = 1$ then it follows from 2. above that p is irreducible. For if p were reducible we could find d_1 and d_2 with $p(X) = d_1(X)d_2(X)$ and $1 \leq deg(d_i) \leq deg(p) - 1$ (for $i = 1, 2$). But this is impossible since $deg(p) - 1 = 0$. (The point is that if neither d_1 nor d_2 is a constant polynomial then $deg(p) = deg(d_1) + deg(d_2) \geq 1 + 1 = 2$).*
4. *If $deg(p)$ is 2 or 3 and p is reducible then p has a zero in F. For it follows from 2 that $p(X) = d_1(X)d_2(X)$ with*

$$deg(d_1) + deg(d_2) = deg(p) = (2\,or\,3)$$

and

$$deg(d_i) \geq 1,\ for \quad i = 1\,and\,i = 2.$$

Now, if both $deg(d_1) \geq 2$ and $deg(d_2) \geq 2$ then $deg(d_1) + deg(d_2) \geq 4$, contradiction. So either d_1 or d_2 has degree 1. So p has a factor of the form $aX + b$ with $a, b \in F$ and $a \neq 0$. Thus, for some $d \in F[X]$,

$$\begin{aligned} p(X) =& (aX + b)d(X) \\ =& a(X - (-a^{-1}b))d(X). \end{aligned}$$

By the Factor Theorem, $-a^{-1}b$ is a zero of $p(X)$.

Example IV.2.1

1- **Irreducibles in $\mathbb{Z}_3[X]$**
the polynomial $p(X) = X^2 - X - 1$ is irreducible. For by (4.) in previous remark,

if $X^2 - X - 1$ were reducible it would have a zero in $\mathbb{Z}_3$. But

$$\begin{aligned} p(0) &= -1 = 2 \neq 0 \\ p(1) &= -1 = 2 \neq 0 \\ p(2) &= 1 \neq 0, \end{aligned}$$

and since $0, 1, 2$ are the only elements of $\mathbb{Z}_3$ we see that $p(X)$ has no zeros in $\mathbb{Z}_3$.

2- **Irreducibles in $\mathbb{C}[X]$**
The "Fundamental Theorem of Algebra" states that every polynomial p in $\mathbb{C}[X]$ of degree at least one has a zero in $\mathbb{C}$. By the Factor Theorem it follows that $p(X) = (X - c)q(X)$ for some $c \in \mathbb{C}$ and $q(X) \in \mathbb{C}[\mathbb{X}]$. So if p is irreducible the degree of q must be zero, making $X - c$ an associate of p.
It follows that the only irreducible polynomials in $\mathbb{C}[X]$ are the polynomials of degree one.

3- **Irreducibles in $\mathbb{R}[X]$**
Supposing that $p \in \mathbb{R}[X]$, p is irreducible, and $deg(p) > 1$. Since p has no factors of degree 1 in $\mathbb{R}[X]$ it has no zeros in $\mathbb{R}$. But by the Fundamental Theorem of Algebra $p(X)$ has a zero $a + bi$ in $\mathbb{C}$. We must have $b \neq 0$ since this zero is not in $\mathbb{R}$. Observe that $a + bi$ is also a zero of the polynomial
$X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$. By Theorem IV.2.1 :

$$p(X) = q(X)(X^2 - 2aX + a^2 + b^2) + (r_0 + r_1 X)$$

for some $r_0, r_1 \in R$. Substituting $X = a + bi$ gives

$$0 = p(a + bi) = q(a + bi)0 + (r_0 + r_1(a + bi)) = (r_0 + r_1 a) + (r_1 b)i.$$

Equating real and imaginary parts gives $r_1 b = 0$ and $r_0 + r_1 a = 0$. Since $b \neq 0$ this gives $r_1 = 0$, and hence $r_0 = 0$. Thus $X^2 - 2aX + a^2 + b^2$ is a factor of $p(X)$, and since $p(X)$ is irreducible it must be an associate of $X^2 - 2aX + a^2 + b^2$. Hence all irreducibles in $\mathbb{R}[X]$ are of degree 1 or 2.

IV.2.4 Factorization of Polynomials

The proofs of the following facts are very similar to the corresponding proofs for $\mathbb{Z}$, and are omitted.

Theorem IV.2.5 *Let a, b, p be polynomials over the field F, and supposing that p is irreducible and $p \mid ab$. Then $p \mid a$ or $p \mid b$.*

Lemma IV.2.1 *Supposing that $p, q_1, q_2, \cdots, q_s$ are monic irreducible polynomials in $F[X]$ and that for some nonzero $d \in F$ we have*

$$p(X) \mid dq_1(X)q_2(X) \cdots q_s(X).$$

Then $p(X) = q_j(X)$ for some j.

IV.2.5 Unique Factorization Theorem

(i) Supposing that $f(X)$ is a polynomial of degree greater than one with coefficients in the field F, and let c be the leading coefficient of f. Then there exist monic irreducible polynomials $p_1(X), p_2(X), \cdots, p_r(X) \in F[X]$ such that

$$f(X) = cp_1(X)p_2(X)\cdots p_r(X).$$

(ii) If $cp_1(X)p_2(X)\cdots p_r(X) = dq_1(X)q_2(X)\cdots q_s(X)$ where c, d are nonzero elements of F and the p_i, q_j are monic irreducible polynomials, then $c = d, r = s$, and $p_1 = q_{i_1}, p_2 = q_{i_2}, \cdots, p_r = q_{i_r}$ where $i_1, i_2, \cdots, i_r$ are the numbers $1, 2, \cdots, r$ in some order.

Example IV.2.2

1. *Since $\mathbb{Z}_{17}$ is a field (because 17 is prime) the Unique Factorization Theorem holds in $\mathbb{Z}_{17}[X]$. So, for instance, $X^2 - 6X + 5 = (X - 1)(X - 5)$, and this is the unique way of writing $X^2 - 6X + 5$ as a product of irreducibles. On the other hand, $\mathbb{Z}_{16}$ is not a field, and in $\mathbb{Z}_{16}[X]$ we find that*

$$\begin{aligned}(X-1)(X-5) &= X^2 - 6X + 5\\ &= X^2 + 10X + 21\\ &= (X+7)(X+3).\end{aligned}$$

   Unique factorization does not hold in $\mathbb{Z}_{16}[X]$.

2. *In $\mathbb{Z}_2[X]$ there are eight polynomials of degree three. We list them all and express each as a product of irreducibles:*

$$\begin{aligned}X^3 &= XXX\\ X^3 + 1 &= (X+1)(X^2+X+1)\\ X^3 + X &= X(X+1)(X+1)\\ X^3 + X + 1 &\text{ is irreducible}\\ X^3 + X^2 &= XX(X+1)\\ X^3 + X^2 + 1 &\text{ is irreducible}\\ X^3 + X^2 + X &= X(X^2+X+1)\\ X^3 + X^2 + X + 1 &= (X+1)(X+1)(X+1).\end{aligned}$$

IV.2.6 Ideals in Polynomial Rings

From now on we will only be concerned with polynomials over fields.

Theorem IV.2.6 *Let F be a field and let I be an ideal of $F[X]$. Then there exists a polynomial $f(X)$ such that $I = f(X)F[X]$.*

Proof IV.2.6 *We know that $0 \in I$. If 0 is the only element of I then the assertion of the theorem holds with $f(X) = 0$. Thus we may assume that I contains nonzero elements. Of all nonzero elements of I choose $f(X)$ to be one of minimal degree, and let $J = f(X)F[X]$. If $p(X) \in J$ then $p(X) = q(X)f(X)$ for some q, and, since $f(X) \in I$, we obtain $p(X) \in I$. Thus $J \subseteq I$. Conversely, let $p(X) \in I$, and let $r(X)$ be the remainder on dividing $p(X)$ by $f(X)$. Then for some polynomial q we have $r(X) = p(X) - q(X)f(X)$, and since $p(X)$ and $f(X)$ are both in I we deduce that $r(X) \in I$. By the choice of f(X) we know therefore that the degree of r(X) cannot be less than the degree of $f(X)$; hence, by Theorem IV.1.2 it follows that $r(X) = 0$. Thus $p(X) = f(X)q(X) \in f(X)F[X] = J$, and we conclude that $I \supseteq J$. Hence $I = J$, as required.* □

Remark IV.2.4 *This says that all ideals of $F[X]$ are principal. Furthermore, in the above proof we have in fact shown that a nonzero ideal in $F[X]$ is generated by any nonzero element of minimal degree contained in it. As a corollary we obtain the following proposition:*

Proposition IV.2.2 *Let I be an ideal in $F[X]$ with $I \neq F[X]$, and supposing that I contains an irreducible polynomial $p(X)$. Then $I = p(X)F[X]$.*

Proof IV.2.7 *By the previous theorem there exists $f(X) \in F[X]$ with $I = f(X)F[X]$. Since $p(X) \in I$ it follows that $f(X) \mid p(X)$. Since $p(X)$ is irreducible $f(X)$ must be either an associate of $p(X)$ or of degree zero. But if $deg(f) = 0$ then by III.2.2 (i), we obtain $I = F[X]$, contrary to hypothesis. So f and p are associates, and therefore $f(X)F[X] = p(X)F[X]$.* □

IV.2.7 Quotient Rings of Polynomial Rings

Continuing with the notation of the previous theorem let $I = f(X)F[X]$. We wish to investigate the ring $Q = F[X]/I$. For simplicity we will use the bar notation for cosets: $\overline{g(X)} = I + g(X)$ for all $g \in F[X]$.

Theorem IV.2.7 *Supposing that $f(X) = c_0 + c_1X + \cdots + c_nX^n$, where $n \geqslant 1$, $c_i \in F$ for each i, and $c_n \neq 0$. Then we have the following:*

(i) *Each element of $Q = F[X]/I$ is uniquely expressible in the form $\overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}}$ with $a_0, a_1, \cdots, a_{n-1} \in F$.*

(ii) *The set $\overline{F} = \{\overline{a} \ , a \in F\}$ is a subring of $F[X]/I$ isomorphic to F.*

(iii) *The element $\overline{X}$ of Q satisfies the equation $\overline{c_0} + \overline{c_1}\overline{X} + \cdots + \overline{c_n}\overline{X^n} = \overline{0}$.*

Proof IV.2.8

(i) *An arbitrary element of Q is a coset of I, and hence equal to $g(X)$ for some polynomial $g \in F[X]$. By Theorem IV.2.1*

$$g(X) = q(X)f(X) + (a_0 + a_1X + \cdots + a_{n-1}X^{n-1}) \qquad \text{(IV.2)}$$

for uniquely determined $a_0, a_1, \cdots, a_{n-1} \in F$. Since I is the set of all polynomials of the form $q(X)f(X)$ it follows that equation $IV.2$ is equivalent to $g(X) \equiv a_0 + a_1X + \cdots + a_{n-1}X^{n-1}(mod I)$, and hence to

$$g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}. \tag{IV.3}$$

So, $IV.3$ holds for unique a_i, as required.

(ii) Define a mapping

$$\begin{aligned} \theta : F &\longrightarrow F[X]/I \\ a &\longrightarrow \theta(a) = \overline{a}. \end{aligned}$$

Then θ is a homomorphism, since it is the restriction to the subring F of $F[X]$ of the natural homomorphism $F[X] \longrightarrow Q$. If $a \in F$ is in $ker\theta$ then $\overline{a} = \overline{0}$, and since $a \in F$ it follows from (i) that $a = 0$. (Alternatively, $\overline{a} = \overline{0}$ means that $a \in I$, and hence a is divisible by $f(X)$. Since a is a constant and $deg(f) \geqslant 1$ we must have $a = 0$.) Thus $ker\theta = 0$, and since $Im\theta = \{\theta(a) , a \in F\} = F$ The fundamental homomorphism theorem gives

$$\overline{F} \cong F/ker\theta \cong F.$$

(iii) By the definition of addition and multiplication in a quotient ring,

$$\overline{r(X)} + \overline{s(X)} = \overline{r(X) + s(X)}$$

$$\overline{r(X)}.\overline{s(X)} = \overline{r(X)s(X)}$$

for all $r(X), s(X) \in F[X]$. Hence

$$\overline{c_0} + \overline{c_1}\overline{X} + \cdots + \overline{c_n}\overline{X^n} = \overline{c_0 + c_1X + \cdots + c_nX^n} = \overline{f(X)}$$

which is equal to $\overline{0}$ since $f(X) \in I$.

□

Theorem IV.2.8
Let $p(X) = a \in F$, and let $I = p(X)F[X]$.

(i) If $a = 0$ then $I = \{0\}$ and $F[X]/I \cong F[X]$.

(ii) If $a \neq 0$ then $I = F[X]$ and $F[X]/I \cong \{0\}$.

Proof IV.2.9 *Part (i) is remark $II.4.2$ $(2.)$, and, in view of $III.2.2$, Part (ii) is immediate from $II.4.2$ $(3.)$.* □

IV.2.8 Some properties

Theorem IV.2.9 *If D is an integral domain then $D[x]$ is an integral domain.*

Proof IV.2.10 *supposing $f(x), g(x) \in D[x]$ are nonzero polynomials $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ where a_n, b_m are the leading coefficients of $f(x), g(x)$ respective. Observing,*

$$f(x)g(x) = a_n b_m x^{m+n} + \cdots + a_0 b_0$$

Noting $a_n, b_m \neq 0$ in integral domain D hence$a_n b_m \neq 0$ and we find $f(x)g(x) \neq 0$. Therefore, there are no zero divisors in $D[x]$. Furthermore, $D[x]$ is a commutative ring with unity:
$f(x) = 1$. Hence, $D[x]$ is an integral domain. □

Definition IV.2.3 *[8]*
The polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, where the $a_0, a_1, a_2, \cdots, a_n$. are integers is said to be primitive if the greates common divisor of $a_0, a_1, \cdots, a_n$ is 1.

Lemma IV.2.2 *Let D be a UFD and let F be a field of quotients of D. Let $f(x) \in D[x]$ with $deg(f(x)) > 0$, then:*
If $f(x)$ is an irreducible in $D[x]$, then, $f(x)$ is also an irreducible in $F[x]$.

Proof IV.2.11
Supposing that $f(x) = r(x)s(x)$ for $r(x); s(x) \in F[x]$ with $deg(r(x)) < deg(f(x))$ and $deg(s(x)) < deg(f(x))$. Since F is a field of quotients of D, each coefficient in $r(x)$ and $s(x)$ is of the form a/b for some $a, b \in D$. By clearing denominators, we can get

$$df(x) = r_1(x)s_1(x)$$

for $d \in D$; and $r_1(x); s_1(x) \in D[x]$; where:

$$deg(r_1(x)) = deg(r(x))$$

and,

$$deg(s_1(x)) = deg(s(x)).$$

Writing $f(x) = ag(x), r_1(x) = a_1 r_2(x)$, and $s_1(x) = a_2 s_2(x)$ for primitive polynomials $g(x), r_2(x)$, and $s_2(x)$, and $a, a_1, a_2 \in D$. Then $(da)g(x) = a_1 a_2 r_2(x)s_2(x)$, and $r_2(x)s_2(x)$ is primitive. By the uniqueness, $a_1 a_2 = dau$ for some unit $u \in D$. So

$$(da)g(x) = daur_2(x)s_2(x)$$

yielding that

$$f(x) = ag(x) = aur_2(x)s_2(x),$$

This is impossible. Thus $f(x) \in D[x]$ is irreducible in $F[x]$. □

Theorem IV.2.10 *Let D be a UFD. Then $D[x]$ is a UFD.*

Proof IV.2.12 *Let $f(x) \in D[x]$; where $f(x)$ is neither 0 nor a unit.*
If $f(x)$ is of degree 0, we are done, since D is a UFD. Suppose that $degf(x) > 0$. Let

$$f(x) = g_1(x)g_2(x)\cdots g_r(x)$$

be a factorization of $f(x)$ in $D[x]$ having the greatest number r of factors of positive degree. Now writing each $g_i(x) = a_i h_i(x)$ where a_i is a content of $g_i(x)$ and $h_i(x)$ is a primitive polynomial. From the maximality of r, each of the $h_i(x)$ is irreducible. Thus, we now have

$$f(x) = a_1 a_2 \cdots a_r h_1(x) h_2(x) \cdots h_r(x)$$

where the $h_i(x)'$ s are irreducibles in $D[x]$. If we now factor the $a_1 a_2 \cdots a_r$ into irreducibles in D; we obtain a factorization of $f(x)$ into a product of irreducibles in $D[x]$. Now we prove the uniqueness. Let

$$a_1 a_2 \cdots a_r g_1(x) g_2(x) \cdots g_s(x) = b_1 b_2 \cdots b_{r'} h_1(x) h_2(x) h_{s'}(x) \tag{IV.4}$$

where the $a_i, b_i, g_j(x), h_j(x)$ are irreducibles in $D[x]$. Then,

$$a_1 a_2 \cdots a_r \sim b_1 b_2 \cdots b_{r'}$$

since they are content of the above polynomial, and also,

$$g_1(x) g_2(x) \cdots g_s(x) \sim h_1(x) h_2(x) \cdots h_s(x) \in F[x].$$

Then after renumbering b_i 's and the fact that $F[x]$ is a UFD, we have

$$r = r', a_i \sim b_i in D;$$

$$s = s', g_j(x) \sim h_j(x) \, in \, F[x].$$

Note that $g_j(x); h_j(x)$ are irreducibles in $F[x]$. There are $c_j; d_j \in D^*$ such that $g_j(x) = \frac{c_j}{d_j} h_j(x)$. Then $d_j g_j(x) = c_j h_j(x)$ and further $c_j \sim d_j \in D$, hence $g_j(x) \sim h_j(x)$ in $D[x]$. The uniqueness follows.

Theorem IV.2.11 *If F is a field then $F[x]$ is a principal ideal domain.*

Proof IV.2.13 *we know $F[x]$ is an integral domain. Supposing I is an ideal in $F[x]$. If $I = 0$ then $I = \langle 0 \rangle$ is principal. If $I \neq 0$ then the degree of polynomials in I is bounded below hence there must be an polynomial of least degree by the well-ordering-principal. Let $g(x)$ be a polynomial of least degree in I. If $f(x) \in I$ then note the division algorithm provides $q(x)$ with $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $deg(r(x)) < deg(g(x))$. But, $g(x)$ is of minimal degree in I and$r(x) = f(x) - g(x)q(x) \in I$ hence $r(x) = 0$. Thus $f(x) = g(x)q(x)$ and $f(x)\langle g(x) \rangle$ and hence$I \subseteq \langle g(x) \rangle$. Conversely, it is easy to see $\langle g(x) \rangle \subseteq I$ thus $I = \langle g(x) \rangle$ and as I was arbitrary we have shown $F[x]$ is a PID.* □

Remark IV.2.5 *If R is a PID, it does not mean that so is $R[x]$.*

Example IV.2.3 *$\mathbb{Z}[x]$ is not a PID.*

Proof IV.2.14 *We have already prooved that $\mathbb{Z}$ is a PID. We consider the ideal $\langle x, 2 \rangle$. We will show that this ideal is not principal.*
First,we note that $\langle x, 2 \rangle \neq \mathbb{Z}[x]$ because $1 \notin \langle x, 2 \rangle$ because if it were then $1 = xf(x) +$

$2g(x)$ *for* $f(x), g(x) \in \mathbb{Z}[x]$. *But* $1 = xf(x) + 2g(x)$ *has even constant term.*
Now, then we suppose $\langle x, 2\rangle = \langle p(x)\rangle$ *for some* $p(x) \in \mathbb{Z}[x]$. *Then we must have* $x = p(x)f(x)$ *and* $2 = p(x)g(x)$ *for some* $f(x), g(x) \in \mathbb{Z}[x]$. *But the second implies that* $p(x)$ *must be a constant polynomial, specially* $p(x) = -2, -1, 1$ *or* 2. *We can not have* $p(x) = \pm 1$ *because then* $\langle p(x)\rangle = \mathbb{Z}[x]$ *so* $p(x) = \pm 2$. *But then* $x = \pm 2f(x)$, *a contradiction since* $\pm 2f(x)$ *have even coefficients.* □

Theorem IV.2.12 (**Hilbert basis theorem**)
Let R *be a Noetherian ring. Then so is* $R[x]$.

Proof IV.2.15
To the contrary, suppose $a \in R[x]$ *is a non-finitelygenerated ideal.*
Then by recursion there is a sequence $\{f_0, f_1, \cdots\} \subset a$ *such that if* b_n*with* $n \geq 1$ *is the ideal generated by* $\{f_0, \cdots, f_{n-1}\}$, *then* $f_n \in a/b_n$ *is of minimal degree. It is clear that* $\{deg(f_0), deg(f_1), \cdots\}$ *is a non-decreasing sequence of nonnegative integers. Let an be the leading coefficient of* f_n *and let* b *be the ideal of* R *generated by* $a_0, a_1, \cdots$. *Since* R *is Noetherian the chain of ideals*

$$\langle a_0\rangle \subset \langle a_0, a_1\rangle \subset \langle a_0, a_1, a_2\rangle \subset \cdots$$

must terminate. Suppose that $b = \langle a_0, \cdots, a_{n-1}\rangle$ *for some integer* n. *So in particular,*

$$a_n = \sum_{i<n} \sum_{j=1}^{n_i} u_{i,j} a_i v_{i,j},\ u_{i,j} v_{i,j} \in R,$$

where the sum is finite. Now consider

$$g = \sum_{i<n} \sum_{j=1}^{n_i} u_{i,j} x^{deg(f_n)-deg(f_i)} f_i v_{i,j} \in b_n,$$

whose leading term is equal to that of f_n. *Hovewer,* $f_n \notin b_n$, *which means that*

$$f_n - g \in a/b_n$$

has degree less than f_n, *contradicting the minimality.*
Modifying the above proof we can have the following result:
Let R *be a left (or right) Noetherian ring. Then, so is* $R[X]$. □

Theorem IV.2.13 *If* F *is a field, the polynomial ring* $F[x]$ *is a Euclidean domain with norm given by the degree map* $N(p) = deg(p)$.

Proof IV.2.16 *(The proof is just the usual-long divisin algorithm for polynomials)*
We induct on the degree n of $a(x)$.
The base case is trivial, as we may take $q = r = 0$ *if* $a = 0$.
Now supposing the result holds for all polynomials $a(x)$ *of degree* $\leqslant n - 1$.
If $deg(b) > deg(a)$ *then we can simply take* $q = 0$ *and* $r = a$, *so now, also we assume* $deg(b) \leqslant deg(a)$.

Writing $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *and* $b(x) = b_m x^m + \cdots + b_0$ *, where* $b_m \neq 0$ *since* $b(x) \neq 0$.
Observing that $a_1(x) = a(x) - \frac{a_n}{b_m}x^{n-m}b(x)$ *has degree less than* n*, since we have cancelled the leading term of* $a(x)$*. (Here we are using the fact that* F *is a field, so that* $\frac{a_n}{b_m}$ *also lies in* F *.)*
By the induction hypothesis, $a_1(x) = q_1(x)b(x) + r_1(x)$ *for some* $q_1(x)$ *and* $r_1(x)$ *with* $r_1 \neq$ *or* $deg(r_1) < deg(b)$.
Then $a(x) = [q_1(x) + \frac{a_n}{b_m}x^{n-m}]b(x) + r_1(x)$*, so* $q(x) = q_1(x) + \frac{a_n}{b_m}x^{n-m}$
and $r(x) = r_1(x)$ *work as claimed.* □
In this section we shall give some examples of Euclidean domains different from the ring $\mathbb{Z}$ *of integers and the polynomial ring* $F[x]$.

Definition IV.2.4
Let $\mathbb{Z}[i] = \{a + bi : a, b\mathbb{Z}\}$ *which is a subring of* $\mathbb{C}$*. Any number in* $\mathbb{Z}[i]$ *is called a Gaussian integer. The norm of a+bi* $\in \mathbb{Z}[i]$*, where* $a, b \in \mathbb{Z}$*, is defined as*
$N(a + bi) = |a + bi|^2 = a^2 + b^2$*. We can easily extend the function N to* $\mathbb{C}$*, i.e., defined* $N(a + bi) = a^2 + b^2$ *for any* $a + bi \in \mathbb{C}$ *where* $a, b \in \mathbb{R}$ *. Note that the Gaussian integers include all the integers. Recall that the norm or absolute value of* $a + bi \in \mathbb{C}$*, where* $a, b \in \mathbb{R}$*, was defined as* $|a + bi| = \sqrt{a^2 + b^2} = \sqrt{N(a + bi)}$*, So here we have different meaning for the word norm.*

Lemma IV.2.3 *For all* $\alpha, \beta \in \mathbb{C}$ *we have:*

(i). $N(\alpha) \geq 0$.

(ii). $N(\alpha) = 0$ *if and only if* $\alpha = 0$.

(iii). $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof IV.2.17 *These results directly follow from properties of absolute value of complex numbers.* □

Lemma IV.2.4 $\mathbb{Z}[i]$ *is an integral domain.*

Proof IV.2.18 *This follows from the fact that* $\mathbb{Z}[i] \subset \mathbb{C}$ *which is a field.* □

Theorem IV.2.14 *The norm* $N(\alpha)$ *for nonzero* $\alpha \in \mathbb{Z}[i]$ *is a Euclidean norm on* $\mathbb{Z}[i]$*, i.e,* $\mathbb{Z}[i]$ *is a Euclidean domain.*

Proof IV.2.19
Let
$\beta = b_1 + b_2 i \neq 0$ *we know that* $N(b_1 + b_2 i) = b_1^2 + b_2^2$ *So* $N(\beta) \geq 1$*. Then*

$$N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta),$$

$\forall \alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$. *This proves Condition* (ii) *in definition of Euclidean norm.*
Now we prove Condition (i) *in the same definition for* N. *Let* $\alpha = a_1 + a_2 i = b_1 + b_2 i \in \mathbb{Z}[i]$; *where*

$\beta \neq 0$.
We want to find σ *and* $\rho \in \mathbb{Z}[i]$ *such that* $\alpha = \beta\sigma + \rho$, *where either*

$$\rho = 0$$

or $N(\rho) < N(\beta) = b_1^2 + b_2^2$.*Let* $\frac{\alpha}{\beta} = r + si$ *for* $r, s \in \mathbb{Q}$. *Taking* $q_1, q_2 \in [\mathbb{Z}]$ *such that* $|r - q_1| \leq \frac{1}{2}$ *and* $|s - q_2| \leq \frac{1}{2}$.
Let $\sigma = q_1 + q_2 i$ *and* $\rho = \alpha - \beta\sigma$. *If* $\rho = 0$, *we are done. Otherwise, we see that*

$$\begin{aligned} N\left(\frac{\alpha}{\beta} - \sigma\right) =& N\left((r + si) - (q_1 + q_2 i)\right) \\ =& N((r - q_1) + (s - q_2)i) \\ \leq& (\frac{1}{2})^2 + (\frac{1}{2})^2) = \frac{1}{2}. \end{aligned}$$

Thus we obtain

$$\begin{aligned} N(\rho) = N(\alpha - \beta\sigma) =& N\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \sigma\right) \\ \leq& \frac{N(\beta)}{2} < N(\beta). \end{aligned}$$

□

Example IV.2.4
In $\mathbb{Z}[i]$, *we search on* $U(\mathbb{Z}[i])$ *and factor* 5 *into a product of irreducibles.*
In $\mathbb{Z}[i]$, *since* $N(1) = 1$, *the units of* $\mathbb{Z}[i]$ *are exactly the* $\alpha = a_1 + a_2 i$ *with* $N(\alpha) = a_1^2 + a_2^2 = 1$. *Since* $a_1, a_2 \in \mathbb{Z}$, *it follows that* $a_1 = 1$ *with* $a_2 = 0$, *or* $a_1 = 0$ *with*
$a_2 = 1$. *Thus* $U(\mathbb{Z}[i]) = \{1, i\}$.
We know that 5 *is an irreducible in* $\mathbb{Z}$. *But* 5 *is no longer an irreducible in* $\mathbb{Z}[i]$, *since,* $5 = (1 + 2i)(1 - 2i)$, *where neither* $1 + 2i$ *nor* $1 - 2i$ *is a unit.*

Example IV.2.5
Using a Euclidean algorithm in $\mathbb{Z}[i]$ *to find a* $gcd(8 + 6i; 5 - 15i)$.
Since, $\frac{5 - 15i}{8 + 6i} = -\frac{1}{2} - \frac{3}{2}i$, *we have*$5 - 15i = -i(8 + 6i) - (1 + 7i)$. *Since* $\frac{8 + 6i}{1 + 7i} = 1 - i$, *we have* $8 + 6i = (1 + 7i)(1 - i)$. *We put them together*

$$\begin{aligned} 5 - 15i =& -i(8 + 6i) - (1 + 7i); \\ 8 + 6i =& (1 + 7i)(1 - i) + 0. \end{aligned}$$

Thus, $gcd(8 + 6i; 5 - 15i) \sim 1 + 7i$.

V conclusion

Polynomial rings are algebraic structures consisting of polynomials with coefficients from a given field. They provide a framework for studying polynomial equations and their properties in a systematic manner.

One significant application of polynomial rings is in computer algebra systems (CAS). These systems employ algorithms based on polynomial ring operations to perform symbolic computations, such as polynomial factorization, polynomial arithmetic, and solving polynomial equations. CAS are widely used in mathematics, engineering, and scientific research for tasks like symbolic integration, solving differential equations, and optimizing mathematical models.

In cryptography, polynomial rings play a crucial role in constructing cryptographic algorithms and protocols. For example, in public-key cryptography, polynomial rings are utilized in schemes like the RSA algorithm and the ElGamal encryption scheme. The security of these systems relies on the hardness of certain mathematical problems, such as factoring large integers or computing discrete logarithms in polynomial rings modulo a prime.

Furthermore, polynomial rings find applications in error-correcting codes, which are used to detect and correct errors that occur during data transmission or storage. Algebraic codes, such as Reed-Solomon codes and BCH codes, are constructed using polynomial rings and have applications in digital communication systems, storage devices, and satellite communication.

In signal processing, polynomial rings are employed in methods for analyzing and processing signals, such as digital filtering, spectral analysis, and data compression. Techniques like polynomial interpolation and approximation are used to estimate continuous signals from discrete samples, enabling applications in audio processing, image processing, and telecommunications.

Moreover, polynomial rings are fundamental in algebraic geometry, where they are used to study geometric objects defined by polynomial equations. Concepts like affine

varieties, projective varieties, and algebraic curves are described using polynomial rings, providing insights into geometric properties and relationships.

Overall, the applications of polynomial rings are diverse and pervasive, spanning multiple disciplines including mathematics, computer science, cryptography, communications, and engineering. Their versatility and mathematical richness make them indispensable tools for solving complex problems and advancing scientific and technological innovation.

V.0 Bibliography

[1] *Robinson, D. j. (2012). A cours in the Theory of Groups (Vol.80). Springer science & Business Media.*

[2] *Howlett, R. (1994). An Undergraduate Course in Abstract Algebra,p.17-19.*

[3] *Cohn, Paul M, (2001). Introduction to ring theory. Springer Science & Business Media.*

[4] *Neal H. McCoy, (1962). (Carus Mathematical Monographs 8)- Rings and Ideals-Mathematical Assoc.*

[5] *Zhao, K. (2022). Ring and Field Theory.*

[6] *McIvor, J. (2014). Ring Theory (Math 113), Summer 2014. University of California, Berkeley.*

[7] *Amar Bapic. (2021). Exercices and solutions in Rings and Fields. Notebook for Algabra IV - Algebraic structures. University of Primorska.*

[8] *James, S. Cook. (2016). Lecture Notes for Abstract Algebra I. Liberty university.*