

Lecture notes on basic and computational algebra

AIMS Skills Course: 12 – 29 October 2009

By

Barry Green

Summary: The aim of this basic algebra course is to introduce and study various axiomatic algebraic structures and concepts. These structures provide the natural setting used to describe and study many of the most important classical and modern results in number theory, algebraic geometry, computational algebra as well as those from other mathematical areas. They are also applied in many other disciplines such as cryptography, coding theory, physics and chemistry. Topics we investigate include groups, rings, polynomial rings and fields. We include selected geometric and computational applications, making use of the computational package SINGULAR where appropriate. This course will serve as useful background to the review course on COMPUTER ALGEBRA AND APPLICATIONS to be offered later.

Contents

1. **The structures we study: Binary relations and operations, groups, rings and fields**
2. **Introductory facts from group theory**
3. **Introductory facts from ring and field theory**
4. **Polynomial algebra**
5. **Applications**
6. **References**

1. The structures we study:

Binary relations and operations, groups, rings and fields

1.1. What is algebra

- Algebra is the study of systems of equations and their solutions which belong to particular sets.

Example: $X^n + Y^n = Z^n$, with $n = 1, 2, 3, \dots$ and $X, Y, Z \in \mathbb{Z}$, or in \mathbb{Q} .

- This study leads to the study of sets which are equipped with additional structure.

Examples: Sets and operations

- i) $(\mathbb{Z}, +, \cdot)$ (a very special ring)
- ii) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ (very special fields)
- iii) $(M_n(\mathbb{R}), +, \cdot)$ ($n \times n$ matrices with entries in \mathbb{R})

In modern algebra this more general view is adopted. Nevertheless we shouldn't forget the underlying motivation which led to this view - the classical view still remains a source of inspiration and many of the most significant new developments have their origin in the investigation and study of a classical problem (such the the proof of Fermat's Last Theorem).

We shall now begin by defining the sets and structures we will be studying:

1.2. Binary relations and operations

Definition. A binary relation on a set A is defined to be a subset of $A \times A$.

Notation: Let $R \subseteq A \times A$ be a binary relation on the set A . Then if $(x, y) \in R$ we write xRy .

Examples: Classwork.

We next list a number of important properties that binary relations may have:

Properties. Let $R \subseteq A \times A$ be a binary relation defined on the set A . Then

- i) R is reflexive if xRx for each $x \in A$.

- ii) R is symmetric if for each $x, y \in A$, $xRy \Rightarrow yRx$.
- iii) R is transitive if for each $x, y, z \in A$, if xRy and yRz then xRz .
- iv) R is anti-symmetric if for each $x, y \in A$, if xRy and yRx then $x = y$.

We next distinguish two very important types of relations:

1. A binary relation R is called an equivalence relation if it is reflexive, symmetric and transitive.
2. A binary relation R is called a partial order if it is reflexive, anti-symmetric and transitive. If in addition for each $x, y \in A$ we have xRy or yRx then the relation is called a total or linear order.

Examples. Classwork.

1.3. Equivalence relations and partitions.

Definition: Let A be a non-empty set. A set P of subsets of A is called a partition of A if

- i) A is the union of the subsets in P
- ii) The intersection of any two distinct subsets in P is empty.

Examples. Classwork

1.4 Theorem. Let A be a non-empty set and P be a partition of A . We define a relation R on A associated with P by defining xRy if x and y lie in the same subset in P . Then R is an equivalence relation on A .

Proof. Classwork.

The converse of this result holds too:

1.5 Theorem. Let R be an equivalence relation defined on A and for each element $a \in A$ we define the set $\bar{a} := \{x \in A : xRa\}$. Then $P = \{\bar{a} : a \in A\}$ is a partition of A .

Proof. Classwork

Remarks. 1. The sets \bar{a} are called the equivalence classes of R .

2. If aRb then $\bar{a} = \bar{b}$.

In order to introduce the algebraic structures we will be studying we need one more definition:

1.6 Definition. A binary operation defined on a set A is defined to be a function $\circ : A \times A \rightarrow A$.

Examples. Classwork.

We now define the basic structures we will be working with and in subsequent chapters study each of them in more detail.

1.7 Definition. Let G be a non empty set and $\circ : G \times G \rightarrow G$ be a binary operation defined on it. Then (G, \circ) is called a group if

- i) for each $a, b, c \in G$ we have $a \circ (b \circ c) = (a \circ b) \circ c$. That is the binary operation \circ is associative.
- ii) there exists an element e such that for all $a \in G$ we have $e \circ a = a \circ e = a$. The element e is called the neutral element or identity.
- iii) For each $a \in G$ there exists an element $b \in G$ such that $a \circ b = b \circ a = e$. The element b is called the inverse of a and is also written $b = a^{-1}$.

If in addition to the properties above for each $a, b \in G$ we have $a \circ b = b \circ a$, so that the operation is commutative, we call (G, \circ) an abelian group, named after the Norwegian mathematician Neils Hendrik Abel.

Examples. Classwork: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(M_n(\mathbb{R}), +)$, $(GL_n(\mathbb{R}), \cdot)$, $(SL_n(\mathbb{Z}), \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p^\times, \cdot)$ where p is a prime number.

Internet work. Read about Neils Abel and what he did, just for interest - and remember our comment about classical problems.

We remark that when the group is abelian we often use $+$ to represent the binary operation. We now introduce the next structure we will be studying:

1.8 Definition. Let $(R, +, \cdot)$ be a non-empty set equipped with two binary operations. Then $(R, +, \cdot)$ is called a ring with identity if

i) $(R, +)$ is an abelian group with identity, which we denote by 0 . The element 0 is called the additive identity.

ii) for each $a, b, c \in R$

a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

b) $a \cdot (b + c) = a \cdot b + a \cdot c$

c) $(b + c) \cdot a = b \cdot a + c \cdot a$

iii) there exists an element $1 \in R$ such that for each $a \in R$ $1 \cdot a = a \cdot 1 = a$. The element is called the identity with respect to the operation \cdot , that is the multiplicative identity. We assume $1 \neq 0$.

Examples. Classwork: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot)$ and $(\mathbb{Z}_n, +, \cdot)$.

Note that if the ring $(R, +, \cdot)$ satisfies the additional property that for each $a, b \in R$ we have $a \cdot b = b \cdot a$, then $(R, +, \cdot)$ is said to be a commutative ring. Most of the rings we will be working with will be commutative rings.

The final structure we introduce is a special case of the above, i.e. a commutative ring with an important additional property.

1.9 Definition. A commutative ring with identity $(F, +, \cdot)$ is called a field if each $a \in F$, $a \neq 0$, has an inverse a^{-1} , i.e. (F^\times, \cdot) is an abelian group.

Examples. Classwork: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}(X), +, \cdot)$, $(\mathbb{Z}_2, +, \cdot)$, $(\mathbb{Z}_3, +, \cdot)$.

2. Introductory facts from group theory

In this chapter we introduce and discuss a number of elementary results from the theory of groups. The investigation of groups can be traced back to the work of Lagrange in his description of the general formula for the roots of a polynomial of degrees 3 and 4 in 1770. Of course at that time the formal structure had not been defined as we did in the previous chapter.

Nowadays the algebraic theory of groups plays an important role in many areas of pure and applied mathematics as well as in physics and chemistry. This is true particularly of areas where symmetry plays an important role, for example coding theory, quantum mechanics, the structure of molecules, complex analysis and Lie groups, and certainly in many areas of algebra too.

For convenience we recall the definition:

Definition (1.7) Let G be a non empty set and $\circ: G \times G \rightarrow G$ be a binary operation defined on it. The (G, \circ) is called a group if

- i) for each $a, b, c \in G$ we have $a \circ (b \circ c) = (a \circ b) \circ c$. That is the binary operation \circ is associative.
- ii) there exists an element e such that for all $a \in G$ we have $e \circ a = a \circ e = a$. The element e is called the neutral element or identity.
- iii) For each $a \in G$ there exists an element $b \in G$ such that $a \circ b = b \circ a = e$. The element b is called the inverse of a and is also written $b = a^{-1}$.

The cardinality of the set G is called the order of the group and is denoted by $o(G)$ or $|G|$. If $o(G)$ is finite, then G is called a finite group. We shall see that the order is an important invariant of the group, which gives us information about its structure.

2.1 Elementary properties. Let (G, \circ) be a group. Then

- i) for each $a, b, c \in G$ if $a \circ b = a \circ c$, then $b = c$ and if $a \circ b = c \circ b$, then $a = c$.
- ii) for any elements $a, b \in G$ the equation $a \circ X = b$ (and $X \circ a = b$) has a unique solution for X in G .

Proof. Classwork.

2.2 Subgroups. In algebra strong emphasis is placed studying the structure of an object by investigating its subsets or sub objects. Hence we would like to say precisely when a subset of a given group G is also a group with respect to the same operation.

2.3 Definition. Let (G, \circ) be a group and H be a subset of G . Then (H, \circ) is called a subgroup of G if it is a group with respect to \circ .

2.4 Theorem. H is a subgroup of (G, \circ) if and only if

i) $H \neq \emptyset$.

ii) If $a, b \in H$ then $a \circ b \in H$

iii) If $a \in H$ then $a^{-1} \in H$.

Proof. Classwork

Exercises

1) Show that ii) and iii) can be replaced by : If $a, b \in H$ then $a \circ b^{-1} \in H$.

2) Show that if (H_1, \circ) and (H_2, \circ) are subgroups of (G, \circ) then $(H_1 \cap H_2, \circ)$ is also a subgroup.

Let a is an element of a group (G, \circ) . We are interested in the "smallest" subgroup of G containing a . Suppose (H, \circ) is a subgroup containing a , then since H is a group, for all $i \in \mathbb{Z}$ it follows that $a^i \in H$, where by definition $a^0 = a^1 \circ a^{-1} = e$. We shall use the notation

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

and note that by the exercise above $(\langle a \rangle, \circ)$ is a subgroup of (G, \circ) , the minimal subgroup containing a .

2.5 Definition. The subgroup $(\langle a \rangle, \circ)$ is called the cyclic subgroup of (G, \circ) generated by a . In general a group is called cyclic if it is generated by one element.

Examples. Decide which of the following are cyclic groups.

i) $(\mathbb{Z}, +)$, $(2\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,

ii) (S, \cdot) , where $S := \{z \in \mathbb{C} : |z| = 1\}$.

iii) (C_5, \cdot) , where $C_5 := \{z \in \mathbb{C} : z^5 = 1\}$.

We now investigate the relationship between a given subgroup and a group more closely. This leads to one of the first results on the structure of groups.

2.6 Cosets. Let (H, \circ) be a subgroup of (G, \circ) . Given an element $a \in G$, the left coset of H with respect to a in G is defined to be $a \circ H = \{a \circ h : h \in H\}$. (We remark that right cosets are defined similarly.)

Examples. Make a list of

1) the left cosets of $(3\mathbb{Z}, +)$ in $(\mathbb{Z}, +)$.

2) The left cosets of (C_3, \cdot) in (C_6, \cdot) .

We remark that if the group is abelian then left and right cosets are the same.

2.7 Theorem. Let (H, \circ) be a subgroup of (G, \circ) . Then the set of left cosets of H in G form a partition. More precisely

- i) if $h \in H$ then $h \circ H = H$.
- ii) if $a \circ H \cap b \circ H \neq \emptyset$ then $a \circ H = b \circ H$
- iii) for each $a \in G$ we have $a \in a \circ H$.

Proof. Classwork

2.8 Proposition. Any two left cosets of a subgroup (H, \circ) of (G, \circ) have the same cardinality.

Proof. Classwork: Show that the function $f : H \rightarrow a \circ H$, defined by $f(h) = a \circ h$ is a bijection.

Remark. If H is finite then each coset has precisely $o(H)$ elements. Note also that the same results hold for right cosets of H in G .

Finite Groups. In this section we prove a number of elementary results on finite groups. These are most useful for helping to describe the group in many cases.

2.9 Lagrange's Theorem. Suppose that (H, \circ) is a subgroup of a finite group (G, \circ) . Then $o(H)$ is a divisor of $o(G)$.

Proof. Classwork.

Returning to our general discussion subgroups.

2.10 Proposition. Let (G, \circ) be a finite group. Then a non-empty subset H is a subgroup of G if for all $a, b \in H$ it follows $a \circ b \in H$.

Proof. By our earlier results it suffices to show that if $a \in H$ then $a^{-1} \in H$. We examine the set $L = \{a, a^2, a^3, \dots\} \subset H$, noting that as this set is finite, for some $l, k \in \mathbb{N}$ with $k < l$ we have $a^k = a^l$. It follows that $a^{l-k} = e$ and so $a^{-1} = a^{l-k-1} \in L$. Hence $a^{-1} \in H$ as required.

We remark the L is a subgroup of G and in fact $L = \langle a \rangle$. We also notice that for a finite group G if $a \in G$ then for some $k \in \mathbb{N}$ it follows $a^k = e$. This leads to the following definition.

2.11 Definition. Let (G, \circ) be a group and $a \in G$. Then if $a^k \neq e$ for all $k \in \mathbb{N}$ we say a has infinite order. If $a^k = e$ for some $k \in \mathbb{N}$ then the smallest such k is called the order of the element a , and is written $o(a)$.

2.12 Corollary. *If $a \in G$ and G is finite then*

- i) $o(a) = |(a)| = o((a))$ and is a divisor of the order of G .
- ii) $a^{o(G)} = e$

As an application we can give a short easy proof of Fermat's Little Theorem

2.13 Fermat's Little Theorem. *Let p be a prime number and suppose $m \in \mathbb{Z}$ then $m^p \equiv m \pmod{p}$.*

Proof. Classwork.

We now study cyclic groups in more detail, and shall see that they are perfectly understood.

2.14 Proposition. *Each cyclic group is abelian.*

Proof. Classwork.

2.15 Proposition. *If the order of finite group is a prime number then it is a cyclic group.*

Proof. Classwork.

In the next section we will characterize cyclic groups, but we can prove the following now:

2.16 Theorem. *Each subgroup of a cyclic group is a cyclic group.*

Proof. Classwork.

2.17 Homomorphisms and Isomorphisms. One way of studying a given type of algebraic object is to develop methods of being able to identify it with other objects having a similar structure. One of the most common and successful ways of doing this (not only in algebra but in many mathematical fields) is to study the functions between objects, noting that it is important to take the algebraic operations into account. Such functions are called homomorphisms and for groups they are defined as follows.

2.18 Definition. Let $(G_1, *)$ and (G_2, \circ) be groups. Then a homomorphism from $(G_1, *)$ to (G_2, \circ) is a function $f: G_1 \rightarrow G_2$ such that $f(a * b) = f(a) \circ f(b)$ for all $a, b \in G_1$.

Terminology. If a homomorphism is injective (1-1) it is called a monomorphism, if it is surjective (onto) it is called an epimorphism and if it is bijective it is called an isomorphism.

- Examples.** 1) $f: (\mathbb{Z}, +) \longrightarrow (C_n, \cdot)$, defined by $f(k) = e^{2\pi k/n}$.
 2) $f: (\mathbb{Z}_3, +) \longrightarrow (\mathbb{Z}_6, +)$, defined by $f(\bar{k}) = \overline{2k}$. Is $f(\bar{k}) = \overline{k}$ a homomorphism?
 3) $f: (\mathbb{C}^\times, \cdot) \longrightarrow (GL_2(\mathbb{R}), \cdot)$, defined by $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
 4) $f: (GL_n(\mathbb{R}), \cdot) \longrightarrow (\mathbb{R}^\times, \cdot)$, defined by $f(A) = \det(A)$.

2.19 Proposition. Let $f: (G_1, *) \longrightarrow (G_2, \circ)$ be a homomorphism of groups. Then

- i) $f(e_1) = e_2$, where e_1, e_2 are the identities of G_1 and G_2 respectively.
- ii) $f(a^{-1}) = (f(a))^{-1}$ for each $a \in G_1$.
- iii) If $(H_1, *)$ is a subgroup of $(G_1, *)$ then $(f(H_1), \circ)$ is a subgroup of (G_2, \circ) .
- iv) If (H_2, \circ) is a subgroup of (G_2, \circ) then $(f^{-1}(H_2), *)$ is a subgroup of $(G_1, *)$.
- v) If $\text{Ker}(f) = \{x \in G_1 : f(x) = e_2\}$, which will be called the kernel of f , then $(\text{Ker}(f), *)$ is a subgroup of $(G_1, *)$ and for each $a \in G_1$ we have

$$a * \text{Ker}(f) a^{-1} = \text{Ker}(f) \quad \text{and} \quad a * \text{Ker}(f) = \text{Ker}(f) * a.$$
- vi) $\text{Ker}(f) = \{e_1\}$ if and only if f is a monomorphism.

Proof. Classwork.

Examples. Determine $\text{Ker}(f)$ in each of the examples above.

When studying groups in general we single out a special class of subgroups which have a particular property which allows us to build new groups in a special way. This construction is very important and has many applications. As we shall see later it is used to construct finite fields of increasing prime power order. These fields play a very important role coding theory, cryptography and in the computational arithmetic.

2.20 Definition. A subgroup $(N, *)$ of a group $(G, *)$ is called a normal subgroup if $a * N = N * a$ for all $a \in G$.

Observation. 1) If the group G is abelian then all subgroups are normal.

2) Given a homomorphism $f: (G_1, *) \longrightarrow (G_2, \circ)$, the subgroup $\text{Ker}(f)$ is normal.

2.21 Exercise. Show that a subgroup $(N, *)$ of a group $(G, *)$ is a normal subgroup if and only if $a * N * a^{-1} \subseteq N$ for all $a \in G$.

2.22 Factor Groups. Let $(G, *)$ be a group and suppose $(N, *)$ is a normal subgroup. We are going to discuss a very important construction which enables us

to build a new group using the group G and its subgroup N . This construction is applied in many areas of algebra (and in other areas of mathematics too). We begin by defining a special set:

$$G/N := \{a * N : a \in G\} = \{N * a : a \in G\}.$$

Our aim is to show that G/N can be endowed with a structure which makes it into a group. Indeed, using the binary operation $*$ on G we define a new binary operation on G/N as follows

$$*: G/N \times G/N \longrightarrow G/N \quad \text{defined by} \quad (a * N) * (b * N) = (a * b) * N.$$

Note that this operation is well defined as if $a * N = c * N$ and $b * N = d * N$ then

$$\begin{aligned} (a * N) * (b * N) &= (a * b) * N \\ &= \{(a * b) * n : n \in N\} \\ &= \{(c * n_1) * (d * n_2) * n : n \in N\} \\ &= \{c * d * n_3 * n_2 * n : n \in N\} \quad \text{as } N * d = N * d \\ &= \{c * d * m : m \in N\} \quad \text{as } N \text{ is a group} \\ &= (c * d) * N = (c * N) * (d * N). \end{aligned}$$

2.23 Theorem. *In the situation above $(G/N, *)$ is a group.*

Proof. Classwork.

Exercises. 1) Consider the homomorphism $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$, defined by $f(k) = \bar{k} = k + n\mathbb{Z}$. Describe the kernel and image of f .

2) Let $f: (\mathbb{R}, +) \rightarrow (\mathbb{C}^\times, \cdot)$ be defined by $f(x) = e^{ix}$. Show that f is a homomorphism and determine its kernel and image.

3) Let $||: (\mathbb{C}^\times, \cdot) \rightarrow ((\mathbb{R}^\times, \cdot))$ be the function which maps each complex number z onto its modulus. Show that $||$ is a homomorphism and determine its kernel, say S , and its image. Describe \mathbb{C}^\times/S .

2.24 Proposition. *Let $(N, *)$ be a normal subgroup of a group $(G, *)$. Then the function $f: G \rightarrow G/N$, defined by $f(a) = a * N$ is an epimorphism of groups with $\text{Ker}(f) = N$.*

Proof. Classwork.

2.25 The First Isomorphism Theorem. *Let $f: G_1 \rightarrow G_2$ be an epimorphism of the group $(G_1, *)$ onto the group (G_2, \cdot) . Then $(G_1/\text{Ker}(f), *)$ is isomorphic to (G_2, \cdot) .*

Proof. Classwork.

3. Introductory facts from ring and field theory

In this chapter we introduce and discuss a number of basic concepts involving rings and fields. When studying rings the first question one studies has to do with division and factorization, when this is possible and when this is unique. This leads to the study of a number of very special rings, those in which we can define and use a division algorithm, just as we do when working in $(\mathbb{Z}, +, \cdot)$. These rings are called Euclidean rings. Another way of studying the properties of rings generally is by studying its subrings and other important subsets of the ring called ideals.

We begin by recalling the definition and discussing the ideas related to factorization.

Definition 1.8. Let $(R, +, \cdot)$ be a non-empty set equipped with two binary operations. Then $(R, +, \cdot)$ is called a ring with identity if

i) $(R, +)$ is an abelian group with identity, which we denote by 0 . The element 0 is called the additive identity.

ii) for each $a, b, c \in R$

a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

b) $a \cdot (b + c) = a \cdot b + a \cdot c$

c) $(b + c) \cdot a = b \cdot a + c \cdot a$

iii) there exists an element $1 \in R$ such that for each $a \in R$, $1 \cdot a = a \cdot 1 = a$. The element is called the identity with respect to the operation \cdot , that is the multiplicative identity. We assume $1 \neq 0$.

Examples. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(M_n(\mathbb{R}), +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$, $(\mathbb{Z}[X], +, \cdot)$, $(\mathbb{Z}_p[X], +, \cdot)$, $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ (here $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$), $(\mathbb{Z}[\sqrt{-1}], +, \cdot)$.

If $a \cdot b = b \cdot a$ for all $a, b \in R$ then the ring R is said to be **commutative**. Further if in addition, whenever $a \cdot b = 0$ either $a = 0$ or $b = 0$, then R is said to be an **integral domain**.

Observe that $(\mathbb{Z}, +, \cdot)$ is an integral domain. Is this the case for $(M_2(\mathbb{R}), +, \cdot)$?

3.1 Divisibility in rings. Let $(R, +, \cdot)$ be a commutative ring with identity. Then

i) if $a, b \in R$ we say a is a divisor of b if there exists $c \in R$ such that $b = c \cdot a$.

- ii) we say $d \in R$ is a greatest common divisor of $a, b \in R$ if $d|a$ and $d|b$ and for each $d'|a, b$ it follows $d'|d$. Notation: $d = \gcd(a, b) = (a, b)$.
- iii) $u \in R$ is called a unit if there exists $v \in R$ such that $uv = vu = 1$.
- iv) $a, b \in R$ are called associates if there exists a unit $u \in R$ such that $a = ub$.
- v) $\pi \in R$ is called irreducible if $\pi \neq 0$, π is not a unit and whenever $\pi = \alpha \cdot \beta$ then α or β is a unit.
- vi) $\pi \in R$ is called prime if $\pi \neq 0$, π is not a unit and whenever $\pi|\alpha \cdot \beta$ then $\pi|\alpha$ or $\pi|\beta$.
- vii) $a, b \in R$ are called relatively prime if $\gcd(a, b) = 1$.

3.2 Examples. Write down the units in each of the following rings.

- i) $(\mathbb{Z}, +, \cdot)$,
- ii) $(\mathbb{Z}[\sqrt{-1}], +, \cdot)$,
- iii) $(\mathbb{Z}[\sqrt{-3}], +, \cdot)$,
- iv) $(\mathbb{Q}[X], +, \cdot)$,

The following example shows that the definitions of irreducibility and primeness don't always agree and that for many rings we cannot factorize uniquely. We illustrate this by analyzing factorization in $(\mathbb{Z}[\sqrt{-3}], +, \cdot)$. Consider the product:

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2 \cdot 2$$

We show that the elements $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ and 2 are irreducible in $\mathbb{Z}[\sqrt{-3}]$, but not prime.

Showing $1 + \sqrt{-3}$ is irreducible: Suppose $1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$, with $a, b, c, d \in \mathbb{Z}$. Then

$$4 = |1 + \sqrt{-3}|^2 = |a + b\sqrt{-3}|^2 |c + d\sqrt{-3}|^2 = (a^2 + 3b^2)(c^2 + 3d^2)$$

Since $a^2 + 3b^2 = 2$ doesn't have a solution with $a, b \in \mathbb{Z}$, we must have $a^2 + 3b^2 = 1$ or 4.

If $a^2 + 3b^2 = 1$, then $a = \pm 1$ and $b = 0$ so that $a + b\sqrt{-3} = \pm 1$ which is a unit in $\mathbb{Z}[\sqrt{-3}]$.

If $a^2 + 3b^2 = 4$, then $c^2 + 3d^2 = 1$ and we deduce $c + d\sqrt{-3} = \pm 1$ which is a unit in $\mathbb{Z}[\sqrt{-3}]$.

Hence $1 + \sqrt{-3}$ is irreducible.

Similarly one shows that $1 - \sqrt{-3}$ and 2 are irreducible.

Finally it is easy to see that although the elements $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ and 2 are irreducible in $\mathbb{Z}[\sqrt{-3}]$, they are not prime. Indeed, $1 + \sqrt{-3} | (1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2 \cdot 2$ in $\mathbb{Z}[\sqrt{-3}]$, but $1 + \sqrt{-3}$ does not divide 2. Therefore $1 + \sqrt{-3}$ isn't prime. Similarly $1 - \sqrt{-3}$ and 2 aren't prime in $\mathbb{Z}[\sqrt{-3}]$ either.

The example above illustrates two points:

1. We don't always have unique factorization into a product of irreducible elements which is unique.
2. Irreducible elements aren't always prime.

In order to address this problem Dedekind (1831 – 1916) introduced special sets, which play the role of integers and prime numbers in \mathbb{Z} with respect to factorization, called ideals and prime ideals. We shall define ideals later in this section and see that using properties developed for the study of groups, we can prove many useful results. First we study a special family of rings which do have good properties with respect to factorization, namely **Euclidean Domains**. These are integral domains (commutative rings with identity and no non-zero divisors) which satisfy a **Euclidean Algorithm**.

3.3 Definition. Let R be an integral domain. Then R will be called a Euclidean Domain if there is a function

$$N: R \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

such that

- 1) for every $a, b \in R \setminus \{0\}$, $N(a) \leq N(ab)$,
- 2) for every $a, b \in R \setminus \{0\}$, there exists $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $r \neq 0$ and $N(r) < N(b)$.

Remarks. The function N will be called the Euclidean Norm Function. We will use the abbreviation ED in place of writing 'Euclidean Domain'.

3.4 Examples. 1) \mathbb{Z} with $N(a) = |a|$ for every $a \in \mathbb{Z} \setminus \{0\}$ is a ED.

2) Let $(F, +, \cdot)$ be a field. Then the polynomial ring $F[X]$ with $N(f(X)) = \deg(f(X))$ for every $f(X) \in F[X] \setminus \{0\}$ is a ED.

3) Each field can be made into a ED by defining $N(a) = 1$ for all $a \in F \setminus \{0\}$.

3.5 Proposition. The ring $\mathbb{Z}[\sqrt{-1}]$ with $N(a + b\sqrt{-1}) = |a^2 + b^2|$ is a ED.

Proof. Classwork.

Observation. In exercise sheet 1 we investigated greatest common divisors of non-zero positive integers and showed that given $m, n \in \mathbb{Z}^+$, using the Euclidean Division Algorithm there exist $k, l \in \mathbb{Z}$ such that $km + ln = d = \gcd(m, n)$. The only property we used in the proof of that result was the Euclidean Algorithm and so this result is true more generally in any ED. Precisely, let $a, b \in R \setminus \{0\}$, then a and b possess a greatest common d and there exist $s, t \in R$ such that $d = sa + tb$. Moreover d is an element of smallest norm with this property.

Examples. Find the greatest common divisor of each the following:

- i) $f(X) = X^6 - 3X^5 + X^3 - 3X^2 + 2X - 6$ and $g(X) = X^2 - 4X + 3$ in $\mathbb{Q}[X]$.
- ii) $3 + 7i$ and $1 + 3i$ in $\mathbb{Z}[i]$, where $i = \sqrt{-1}$.

3.6 Relationship between prime and irreducible elements. We have seen when considering elements of $\mathbb{Z}[\sqrt{-3}]$ that irreducible elements need not be prime.

Generally we can say the following: Suppose R is an integral domain.

1) Then each prime element π is irreducible.

Indeed, suppose $\pi \in R$ is prime and that $\pi = \alpha\beta$. Then by assumption $\pi|\alpha$ or $\pi|\beta$, say $\pi|\alpha$. It follows $\alpha = \pi\gamma$, for some $\gamma \in R$. We obtain $\pi = \pi\gamma\beta$ and so $\pi(1 - \gamma\beta) = 0$. Since R is an integral domain and $\pi \neq 0$ it follows $1 - \gamma\beta = 0$, from which it follows $\gamma\beta = 1$ so that β is a unit. Therefore π is irreducible.

2) If R is a ED then an element π is prime if and only if it is irreducible.

We need to show that if π is irreducible, then it is prime. Suppose $b, c \in R$ and that $\pi|bc$ and that $\pi \nmid b$. Note that as π is irreducible the only element of R that divide it are the units $u \in R$ and the associates $u\pi$.

We investigate which divisors of π are also divisors of b . If $u\pi|b$ then $b = u\pi d$ for some $d \in R$ and it follows $\pi|b$, a contradiction. Therefore the only divisors of π which divide b are the units $u \in R$.

Hence by our discussion 1 is a greatest common divisor of b and π . It follows we find $s, t \in R$ such that $s\pi + tb = 1$. It follows that $s\pi c + tbc = c$. As $\pi|s\pi c$ and $\pi|tbc$ we deduce that $\pi|c$ as required.

Remark. Notice from our earlier discussion $2 \in \mathbb{Z}[\sqrt{-3}]$ isn't prime, although irreducible. Therefore $\mathbb{Z}[\sqrt{-3}]$ isn't a ED.

The following theorems show that in a ED we can factorize elements uniquely into products of irreducible elements.

3.7 Theorem. Let R be a ED and $a \in R$ with $a \neq 0$ and not a unit in R . Then a can be expressed as a product of irreducible elements and this representation is unique up to order and multiplication by associates.

Remark. We shall assume this result without proof.

3.8 Definition. An integral domain R will be called a **unique factorization domain (UFD)** if each $a \in R$ with $a \neq 0$ and not a unit in R can be uniquely expressed as a product of irreducible elements. As before this representation is unique only up to order and multiplication by associates.

Observation. Each ED is a UFD.

Examples. 1) \mathbb{Z} , $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $F[X]$ where F is any field
2) The ring $\mathbb{Z}[\sqrt{-3}]$ isn't a UFD.

Exercise. Describe the prime (=irreducible) elements in $\mathbb{R}[X]$ and $\mathbb{C}[X]$.

Challenge. Describe the prime elements in $\mathbb{Z}[\sqrt{-1}]$.

A very useful way of studying rings is by studying their subsets, which are endowed with structure that is determined by the ring we are working with.

3.9 Definition. Let R be a commutative ring with identity and suppose $I \subseteq R$ is a non-empty subset. Then I will be called an ideal in R if

- i) $(I, +)$ is an abelian group
- ii) for every $a \in I$ and $r \in R$ we have $ra \in I$.

Example. For each integer n , $n\mathbb{Z}$ is an ideal in \mathbb{Z} .

Remarks. 1) If I is an ideal in R and $1 \in I$, then $I = R$.

2) If I is an ideal in a field F , then $I = \{0\}$ or $I = F$.

3) An ideal I is said to be a principal ideal if it is generated by one element. In other words there exists $x \in I$ such that $I = \{xr : r \in R\} = xR = Rx = \langle x \rangle$.

4) An ideal I is said to be finitely generated if there exist finitely many elements $x_1, x_2, \dots, x_m \in I$ such that

$$I = \{x_1r_1 + x_2r_2 + \dots + x_mr_m : r_1, r_2, \dots, r_m \in R\} = \sum_{i=1}^m x_iR = \langle x_1, x_2, \dots, x_m \rangle.$$

Exercises. Let $I = \{P(X) : 2|P(0)\} \subset \mathbb{Z}[X]$. Show that

- i) I is an ideal in $\mathbb{Z}[X]$,
- ii) $I = \langle 2, X \rangle$,
- iii) I isn't a principal ideal.

It is helpful to know when all ideals in a given ring or integral domain are principal. When this happens the ideals behave very similarly to the elements, but the ideal structure allows us to deduce more, as we shall see.

3.10 Definition. An integral domain is said to be a principal ideal domain (**PID**), if each ideal is principal.

The following theorem shows that there is a large family of rings having this property.

3.11 Theorem. *Each ED is a PID.*

Proof. Let R be a ED and suppose $I \subseteq R$ is any ideal. If $I = \{0\}$ or $I = R$, then $I = \langle 0 \rangle$ or $I = \langle 1 \rangle$, respectively. Suppose $I \neq \langle 0 \rangle$ and choose $a \in I$ with $N(a)$ as small as possible. We show that $I = \langle a \rangle$.

Clearly $\langle a \rangle \subseteq I$, so suppose $b \in I$. Then as R is a ED there exist $q, r \in R$ such that $b = qa + r$ with $r = 0$ or $N(r) < N(a)$. Note that $r = b - qa \in I$ and as $N(a)$ is minimal for elements in I , by assumption, we must have $r = 0$. Hence $b = qa \in \langle a \rangle$ and it follows $I \subseteq \langle a \rangle$, completing the proof.

Remark. With slightly more work we can show that each PID is a UFD. Hence we have the following implications for families of integral domains:

$$\mathbf{ED} \quad \Rightarrow \quad \mathbf{PID} \quad \Rightarrow \quad \mathbf{UFD}.$$

Elementary properties of rings and ideals.

3.12 Definition. Let R be a commutative ring with identity. An ideal P of R , ($P \neq R$), is said to be a prime ideal if for each $a, b \in R$, if $ab \in P$ then $a \in P$ or $b \in P$.

Example. 1) In \mathbb{Z} the prime ideals are $\langle 0 \rangle$ and $\langle p \rangle$, for p any prime number.

2) In $\mathbb{Q}[X]$ the prime ideals are $\langle 0 \rangle$ and $\langle f(X) \rangle$, for $f(X)$ any irreducible polynomial over \mathbb{Q} .

3) In any integral domain R the ideal $\langle 0 \rangle$ is a prime ideal.

More generally we show:

3.13 Proposition. *Let R be an integral domain and I be a non-zero principal ideal. Then*

i) *if I is a prime ideal it can be written as $I = xR$ for some irreducible element $x \in R$.*

ii) *if R is a UFD and $I = xR$ for some irreducible element $x \in R$ then I is a prime ideal.*

Proof. i) Suppose $I = xR$ is a prime ideal and suppose $x = ab$. Then as I is prime it follows $a \in I$ or $b \in I$. Let us suppose $a \in I$, then $a = xr$ for some $r \in R$. It follows $x = xrb$ and so $rb = 1$, ie b is a unit and so x is irreducible.

ii) Suppose R is a UFD and $I = xR$ for some irreducible element $x \in R$. We show that xR is a prime ideal. Let $ab \in xR$ and suppose $a \notin xR$. As $ab \in xR$ it

follows $ab = xr$ for some $r \in R$. As $a \notin xR$ it follows x is not in the irreducible decomposition of a . Therefore as R is a UFD, $ab = xr$ and as x is irreducible it follows it must be in the irreducible decomposition of b , i.e. $b = xr'$ for some $r' \in R$. We obtain $b \in xR$ as required, proving that $I = xR$ is a prime ideal.

3.14 Definition. Let R be a commutative ring with identity. An ideal M will be called maximal if $M \neq R$ and if $M \subset I$, for any ideal I with $M \neq I$, then $I = R$.

3.15 Theorem 3.15. Let R be a commutative ring with identity. Then each maximal ideal is a prime ideal.

Proof. Let M be a maximal ideal and suppose $ab \in M$ with $b \notin M$. We show that $a \in M$. Since M is maximal it follows that

$$M + bR = R.$$

Therefore there exist $m \in M$ and $r \in R$ such that $m + br = 1$. It follows that $a = am + abr \in M$, as $am \in M$ and $abr \in M$. Consequently M is a prime ideal as asserted.

3.16 Factor rings. In chapter 2 we defined the factor group G/N for a given group G and subgroup N , provided it was normal. Here we show how to define the factor ring R/I of a given commutative ring R with respect an ideal I . Note that as an ideal $(I, +)$ is an abelian group it is clearly normal.

Precisely: Let $(R, +, \cdot)$ be a commutative ring with identity and let I be an ideal in R . We define the set of cosets of I in R by

$$R/I := \{r + I : r \in R\}.$$

This set naturally inherits a ring structure from that of R by defining

- i) $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$ for each $r_1, r_2 \in R$.
- ii) $(r_1 + I) \cdot (r_2 + I) = (r_1 \cdot r_2) + I$ for each $r_1, r_2 \in R$.

Note that these operations are well defined and determine a ring structure on $(R/I, +, \cdot)$, which we call the factor ring of R with respect to the ideal I . The additive identity of R/I is $0 + I = I$ and the multiplicative identity is $1 + I$. It is also easy to see that as R is assumed to be commutative, so is R/I .

3.17 Lemma. Let R be a commutative ring with identity and suppose P is an ideal in R . Then R/P is an integral domain if and only if P is a prime ideal.

Proof. We have observed above that R/I is a commutative ring with identity.

Suppose P is a prime ideal and that $(a + P)(b + P) = ab + P = 0 + P = P$. We need to show that $a + P = P$ or $b + P = P$. Now as P is prime and $ab \in P$,

it follows that $a \in P$ or $b \in P$, say $a \in P$. We obtain $a + P = P = 0 + P$ as required. Hence R/P is an integral domain.

Now suppose R/P is an integral domain: we leave the proof that P is a prime ideal to be done as an exercise.

3.18 Lemma. *Let R be a commutative ring with identity and suppose M is an ideal in R . Then R/M is a field if and only if M is a maximal ideal.*

Proof. Suppose that M is a maximal ideal and consider the factor ring R/M . Since M is maximal it is prime and so by Lemma 3.17 R/M is an integral domain. Therefore to prove R/M is a field it suffices to show that each non-zero element $r + M \in R/M$ is invertible.

As $r + M \neq 0 + M = M$ it follows $r \notin M$. As M is maximal it follows $M + rR = R$, and there exist $m \in M$ and $s \in R$ such that $m + rs = 1$. We deduce that

$$(r + M)(s + M) = rs + M = (1 - m) + M = 1 + M.$$

Therefore $s + M = (r + M)^{-1}$, proving that R/M is a field.

Conversely suppose R/M is a field: we leave the proof that M is a maximal ideal in R as an exercise.

Examples. Decide which of the following factor rings are fields and give a description of the cosets in "simplest form". Determine the number of elements in the factor ring where finite.

- 1) $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$
- 2) $\mathbb{R}[X]/\langle X^2 - 2 \rangle$
- 3) $\mathbb{Z}_3[X]/\langle X^3 - X^2 + 1 \rangle$
- 4) $\mathbb{Z}_5[X]/\langle X^4 - X^2 - 2 \rangle$

3.19 Exercise. Suppose x is an irreducible element in a PID R . Then the ideal xR is maximal.

3.20 Homomorphisms and Isomorphisms. Just as when working with groups, the homomorphisms between rings and fields play a very important role in describing their structure. For rings they are defined as follows.

3.21 Definition. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings. Then a homomorphism from $(R, +, \cdot)$ to $(S, +, \cdot)$ is a function $h : R \rightarrow S$ such that

- i) $h(a + b) = h(a) + h(b)$ for all $a, b \in R$.

ii) $h(a \cdot b) = h(a) \cdot h(b)$ for all $a, b \in R$.

Terminology. As before if a homomorphism is injective (1-1) it is called a monomorphism, if it is surjective (onto) it is called an epimorphism and if it is bijective it is called an isomorphism.

3.22 Proposition. Let $h : (R, +, \cdot) \longrightarrow (S, +, \cdot)$ be a homomorphism of rings. Then

i) $h(0) = 0$,

ii) $h(-a) = -h(a)$ for each $a \in R$.

iii) $h(1) = 1$, if there exists $a \in R$ such that $h(a)$ is a unit in S .

v) $\text{Ker}(h) := \{x \in R : h(x) = 0\}$ is an ideal of R and $\text{Ker}(h) = \{0\}$ if and only if h is a monomorphism.

Proof. Classwork.

Examples. 1) If $h : \mathbb{Q}[X] \rightarrow \mathbb{Q}[\sqrt{2}]$ is defined by $h(P(X)) = P(\sqrt{2})$, show that h is a homomorphism of rings and determine $\text{Ker}(h)$. Is $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ a field?

2) If $h : \mathbb{Q}[X] \rightarrow \mathbb{R}$ is defined by $h(P(X)) = P(e)$, where $e := \sum_{n=0}^{\infty} \frac{1}{n!} \in \mathbb{R}$, then h is a homomorphism of rings and $\text{Ker}(h) = \{0\}$.

This result follows as there is no polynomial with coefficients in \mathbb{Q} which has e as a root. Elements of \mathbb{R} or \mathbb{C} which are roots of polynomials with coefficients in \mathbb{Q} (such as $\sqrt{2}$ with polynomial $f(X) = X^2 - 2$, or $\sqrt{-1}$ with polynomial $f(X) = X^2 + 1$) are called algebraic elements over \mathbb{Q} . A deep theorem, which was proved at the end of the 19th century, confirms that e isn't an algebraic element over \mathbb{Q} , i.e. $P(e) \neq 0$ for each non-zero polynomial $P(X) \in \mathbb{Q}[X]$. Such elements are called transcendental over \mathbb{Q} .

3.23 Field homomorphisms. Let E and F be fields and suppose $\phi : F \rightarrow E$ is a homomorphism of rings (recall that since F and E are fields they are rings too). Then ϕ is said to be a homomorphism of fields if $\phi(1) = 1$.

Observation. Observe that every field homomorphism is a **monomorphism**.

Proof. Classwork.

3.24 Theorem (Kronecker). Let F be a field and $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in F[X]$ be a polynomial without a root in F . Then there exists a field E containing F as a subfield so that $P(X)$ has a root in E .

Proof. As the polynomial ring $F[X]$ is a UFD we can factorize $P(X)$ uniquely as a product of irreducible polynomials:

$$P(X) = Q_1(X)Q_2(X) \cdots Q_r(X).$$

Choose $Q(X) := Q_i(X)$ for some i , $1 \leq i \leq r$. Then the ideal $\langle Q(X) \rangle = Q(X)F[X]$ is a maximal ideal and so $E = F[X]/\langle Q(X) \rangle$ is a field. We have

$$F \xrightarrow{\phi} F[X] \xrightarrow{\psi} F[X]/\langle Q(X) \rangle = E$$

with $\phi(a) = a$ and $\psi(h(X)) = h(X) + \langle Q(X) \rangle$. Note that $\psi \circ \phi: F \rightarrow E$ is a homomorphism of fields and so a monomorphism.

We now show that the polynomial P has a root in E . Let $\bar{X} = X + \langle Q(X) \rangle$, then after some manipulation one obtains

$$\begin{aligned} P(\bar{X}) &= Q_1(\bar{X}) \cdots Q_i(\bar{X}) \cdots Q_r(\bar{X}) \\ &= Q_1(X) \cdots Q_i(X) \cdots Q_r(X) + \langle Q(X) \rangle \\ &= \langle Q(X) \rangle \end{aligned}$$

showing that \bar{X} is a root of the polynomial P in E .

Terminology. We remark that the field E is called an extension field of F .

Examples. Find a field containing a root of the given polynomial in each of the following cases:

- 1) $P(X) = X^4 - X^3 - X - 1$ over $F = \mathbb{F}_3 := \mathbb{Z}_3$
- 2) $P(X) = X^4 - X^2 - 2$ over $F = \mathbb{R}$
- 3) $P(X) = X^4 - X^2 - 2$ over $F = \mathbb{Q}$.

Just as in the case of groups we have a very useful isomorphism structure theorem, which we state below. We will use this result to prove the central result describing extensions of fields.

3.25 The first isomorphism theorem for rings. Let $\phi: R \rightarrow S$ be an epimorphism of commutative rings and suppose $I = \text{Ker}(\phi)$. Then there exists an isomorphism between the factor ring R/I and S .

Proof. Classwork.

Returning to field extensions: Let E and F be fields with $F \subseteq E$. An element $\alpha \in E$ is called algebraic over F if it is the root of a monic polynomial in $F[X]$.

(A polynomial is called monic if the coefficient of the term of highest degree is 1). The smallest field in E containing F and α will be denoted by $F(\alpha)$. Our main theorem describes this field precisely.

3.26 Theorem. *Let E , F , α and $F(\alpha)$ be as defined above and suppose $M_\alpha(X) \in F[X]$ is a monic polynomial of smallest degree having α as a root. Then $M_\alpha(X)$ is unique and irreducible in $F[X]$. If $\deg(M_\alpha(X)) = n$ then each element of $F(\alpha)$ can be uniquely written in the form $f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{n-1}\alpha^{n-1}$ for suitable $f_i \in F$. Furthermore $F(\alpha) \cong F[X]/\langle M_\alpha(X) \rangle$.*

Proof. i) *Uniqueness of M_α* : Let M_α and N_α be two distinct monic polynomials having α as a root and suppose $\deg(M_\alpha) = \deg(N_\alpha) = n$. Then α is a root of the polynomial $M_\alpha - N_\alpha \neq 0$ with $\deg(M_\alpha - N_\alpha) \leq n - 1$. Therefore we find a monic polynomial whose degree is strictly smaller than n having α as a root, a contradiction. Hence M_α is unique.

ii) *Irreducibility of M_α* : Suppose $M_\alpha = R_\alpha S_\alpha$ with $R_\alpha, S_\alpha \in F[X]$ and $\deg(R_\alpha), \deg(S_\alpha) < n$. Then $M_\alpha(\alpha) = R_\alpha(\alpha)S_\alpha(\alpha) = 0$. As $R_\alpha(\alpha), S_\alpha(\alpha) \in E$, a field, at least one of them is zero. It follows once more that there is a monic polynomial of lower degree having α as a root, a contradiction. Hence M_α is irreducible.

iii) $F(\alpha) \cong F[X]/\langle M_\alpha(X) \rangle$: Consider the homomorphism $\psi: F[X] \rightarrow E$ defined by $\psi(P(X)) = P(\alpha)$ and let L be the image of ψ in E , i.e. $\psi: F[X] \rightarrow L \subset E$. We investigate the structure of L . Let $h(X) \in \text{Ker}(\psi) \subseteq F[X]$, then since $F[X]$ is a ED we find polynomials $q(X)$ and $r(X)$, so that $h(X) = q(X)M_\alpha(X) + r(X)$ with $r(X) = 0$, or $r(X) \neq 0$ and $\deg(r(X)) < \deg(M_\alpha(X)) = n$.

It follows that $0 = \psi(h(X)) = h(\alpha) = q(\alpha)M_\alpha(\alpha) + r(\alpha) = r(\alpha)$. We see that α is a root of $r(X)$, which must be identically 0 for otherwise $\deg(r(X)) < \deg(M_\alpha(X))$ contradicts the assumption on $M_\alpha(X)$.

Therefore $\text{Ker}(\psi) = \langle M_\alpha(X) \rangle$. Hence by the First isomorphism Theorem we deduce $F[X]/\langle M_\alpha(X) \rangle \cong L$, and note that this is a field as $M_\alpha(X)$ is irreducible in $F[X]$, which is a ED and so a UFD.

Clearly L contains F and α and so $F(\alpha) \subseteq L$ (as L is a field and $F(\alpha)$ is the smallest field containing both F and α). On the other hand L being the image of ψ is precisely the set of polynomials in α with coefficients from F , so we have $L \subseteq F(\alpha)$, proving equality.

iv) *Description of the elements*: To complete the proof of the theorem we describe the elements of $F(\alpha)$ precisely. Let $h(\alpha) = a_0 + a_1\alpha + \cdots + a_m\alpha^m \in F(\alpha)$,

$a_i \in F$, $1 \leq i \leq m$. Using the Euclidean Algorithm we find polynomials $q(X)$ and $r(X)$, so that $h(X) = q(X)M_\alpha(X) + r(X)$ with $r(X) = 0$, or $r(X) \neq 0$ and $\deg(r(X)) < \deg(M_\alpha(X)) = n$. Therefore

$$h(\alpha) = q(\alpha)M_\alpha(\alpha) + r(\alpha) = r(\alpha)$$

Since $r(X) \neq 0$ and $\deg(r(X)) < n$ we find $f_0, f_1, \dots, f_{n-1} \in F$ so that

$$r(X) = f_0 + f_1X + f_2X^2 + \dots + f_{n-1}X^{n-1}$$

and so

$$h(\alpha) = f_0 + f_1\alpha + f_2\alpha^2 + \dots + f_{n-1}\alpha^{n-1} \quad (*)$$

Hence we see that each element of $F(\alpha)$ can be written in the form (*).

We now show that this is a unique expression for the given element of $F(\alpha)$ with degree in α less than or equal to $n-1$. Suppose that $a \in F(\alpha)$ and that

$$a = f_0 + f_1\alpha + f_2\alpha^2 + \dots + f_{n-1}\alpha^{n-1} = g_0 + g_1\alpha + g_2\alpha^2 + \dots + g_{n-1}\alpha^{n-1}$$

with the $f_i, g_i \in F$ for each i and $g_i \neq f_i$ for some i . Then

$$0 = (f_0 - g_0) + (f_1 - g_1)\alpha + (f_2 - g_2)\alpha^2 + \dots + (f_{n-1} - g_{n-1})\alpha^{n-1}.$$

We define $S(X) = (f_0 - g_0) + (f_1 - g_1)X + (f_2 - g_2)X^2 + \dots + (f_{n-1} - g_{n-1})X^{n-1}$ and note that although $S(X) \neq 0$ and $\deg(S(X)) < n$ we have $S(\alpha) = 0$, contradicting the minimality of the degree of $M_\alpha(X)$. Therefore $f_i = g_i$ for each i and the writing is unique.

3.26 Observation. We note that the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly dependent over F , and consequently $F(\alpha)$ is a vector space over F of dimension n , the degree of the irreducible polynomial of α over F . The set $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F . The integer n is called the degree of the extension $F(\alpha)$ of F and we write $n = [F(\alpha) : F]$. We say that the extension is finite.

Examples. Determine M_α , $F(\alpha)$, a basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ and $[F(\alpha) : F]$ for each of the following fields F and α :

a) $F = \mathbb{Q}$ and $\alpha = \sqrt[3]{2}$

b) $F = \mathbb{Q}(i)$ and $\alpha = \sqrt[2]{7}$

3.27 Proposition. Let $F \subseteq E \subseteq K$ be finite field extensions. Then

$$[K : F] = [K : E][E : F].$$

Proof. Exercise.

Example. $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[2]{3}) : \mathbb{Q}(\sqrt[2]{3})] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[2]{3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt[2]{3})]$.

3.28 An Application: Compass and straightedge constructions. We consider a finite set of points in the plane, say $\{P_1, P_2, \dots, P_r\}$, and consider which points can be constructed from these, as points of intersection, using only a straightedge and compass. Suppose $P_i = (a_i, b_i)$ and set $F = \mathbb{Q}(a_1, b_1, \dots, a_r, b_r)$, the smallest subfield of \mathbb{R} containing \mathbb{Q} and all the coordinates of the given points. We observe that if K is any field extension of F obtained by adjoining the coordinates of finitely many points constructed from those given, using a straightedge and compass, then $[K : F] = 2^l$ for suitable l . (Classroom discussion).

Examples. 1. Show that given $P_1 = (0, 0)$, $P_2 = (1, 0)$ and a arbitrary angle with vertex P_1 it isn't possible to trisect this angle using only a straightedge and compass.

2. Using a straightedge and compass show how to construct a regular pentagon given $P_1 = (0, 0)$, $P_2 = (1, 0)$.

3. By applying the same method, show that it isn't possible to construct a regular heptagon.

4. Polynomial Algebra

In this chapter we introduce and discuss monomial orderings on polynomial rings, the multivariate division algorithm, Gröbner Bases and Buchberger's Algorithm for computing a Gröbner basis of an ideal with respect to a given monomial order.

Handwritten notes provided for the lectures.

5. Applications

Elementary applications of Gröbner Bases presented. Problems discussed using the computational package "singular" within the SAGE interface.

Handwritten notes and exercises.

6. References

- [1] R. Allenby, *Rings, Fields and Groups*, Butterworth Heineman, 1991.
- [2] M. Artin, *Algebra*, Prentice Hall, 1991
- [3] D. Cox, J. Little, D. O'Shea, *Ideals Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Undergraduate Texts in Mathematics, 1992.
- [4] B. Green, *Classnotes on undergraduate algebra*, University of Stellenbosch, 2009.