University of Wisconsin - La Crosse

MTH 495: Special Topics in Math

Galois Theory

Notebook

[Work in Progress]

Author:
Nathaniel K. Green

Faculty Mentor:
Dr. Tushar Das

December 19, 2024

Évariste Galois, 1811–1832.

Contents

0 Introduction

What follows is a compilation of notes taken on the topic of galois theory over the fall semester of 2024. The primary text that guided these notes is John M. Howie's *Fields and Galois Theory* [3]. It goes without saying that this book is the primary contributor to the following pages. Other books and resources may be referenced throughout these notes, but will be cited appropriately. Much of the design of these notes has been taken from a similar document from Kean Fallon[1].

We will begin with a review of rings, fields, and groups which are the contents of a usual first course in abstract algebra. Sections following the review will dive into topics beyond an introductory abstract algebra course such as field extensions, splitting fields, and galois groups.

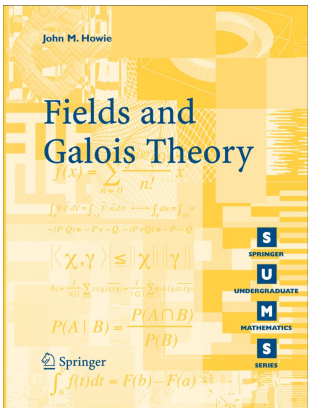


Figure 0.1: Howie's *Fields and Galois Theory*

0.1 Organization of notes; Color-coding

This course has the requirement of weekly LaTeX note submissions, and in order to meet these requirements notes may initially be typed up precisely as found in the book. Definitions and theorems may lack examples and proof, but the author will make an effort to fill in the gaps over time. These notes may differ from the founding texts by omitting excerpts that do not advance the chapter's narrative and by including additional definitions, theorems, proofs, and examples. Finally, the ending of each chapter will be reserved for exercises.

- Standard galois theory material will be in the standard black color. This includes material taken from Howie, in addition to any self generated proofs or examples.
- Throughout the text there will be sections that serve to build intuition, rather than provide strict definitions or results. These are meant to be notes to the reader which give intuitive ideas about concepts. Notes of this type will be written in this color.
- It will often be useful to connect concepts in this text to linear algebra. Connections to linear algebra will be written in this color. The primary text referenced for linear algebra connections is Sheldon Axler's *Linear Algebra Done Right* [1], but additional resources will be cited appropriately.

[1]Link to Kean Fallon's website: `https://www.keanfallon.com/`.

There may arise another suitable category for inserted content, in this event, we will introduce the color along with its description similarly.

0.2 Definitions

Definitions in these notes are all very close, if not the same, as those founds in Howie's *Fields and Galois Theory*. If a definition comes from elsewhere, it will be cited as such. An effort will be made to ensure definitions have examples and non-examples (where applicable). All definitions will be contained in a gray box, containing the definition itself and a bracket denoting parts of speech, e.g. for the definition of a *function*:

Definition 0.1. ⟨ *noun, set* ⟩
Let A and B be sets. Then a **function** from A to B is a set f of ordered pairs in $A \times B$ such that for each $a \in A$, there exists a unique $b \in B$ with $(a, b) \in f$.

Example. Consider the sets $\mathbb{Z}$ and $\mathbb{R}$. Then $f : \mathbb{Z} \to \mathbb{R}$ defined by $f(x) = x^2$ is a function. The ordered pairs $(1, 1), (2, 4)$, and $(-3, 9)$ are all elements of f.

Example. Consider equation for a circle $r^2 = (x - h)^2 + (y - k)^2$ centered at (h, k), with radius r. The equation is not a function.

The part of speech box has the following format depending on what part of speech applies to some definition of a "thing" X.

- ⟨ *noun, what X is* ⟩
- ⟨ *verb, what X acts on (direct object)* ⟩
- ⟨ *adj., what noun X describes* ⟩
- ⟨ *adverb, what verb X describes* ⟩

Definitions used for connections to linear algebra will be done will follow a similar convention, but with slight modifications to help with differentiation. An example is below.

Definition 0.2. ⟨ *noun, vector space* ⟩
A subset U of a vector space V is called a **subspace** of V if U is also a vector space (using the same addition and scalar multiplication as on V).

0.3 Theorems

As with definitions, most theorems in this text will be nearly identical to Howie's *Fields and Galois Theory*. It is beneficial to have examples and proofs of theorems so an effort will be made to do so. Theorems will be contained in a blue box and will describe the statement of the theorem and any title it may have. We illustrate a notable number theory result thusly:

Theorem 0.3. The square root of a prime number is irrational:
Let p be a prime number. There does not exist a rational number r such that $r^2 = p$.

Proof. Assume by way of contradiction, there exists a rational number $k/q \in \mathbb{Q}$ where k and q share no common factors, and $(k/q)^2 = p$. Note, $(k/q)^2 = k^2/q^2 = p \implies k^2 = pq^2$ which means k^2 is a multiple of p. Thus k is a multiple of p, so $k = pn$ for some $n \in \mathbb{N}$. Since k and q share no common factors, q is not a multiple of p. Note, $k^2 = (pn)^2 = p^2n^2 = pq^2 \implies pn = q^2$ which means q^2 is a multiple of p, thus q is multiple of p, which is a contradiction. Therefore, there does not exists a rational number r such that $r^2 = p$ when p is prime. □

Example. Note, by Theorem 0.3 $\sqrt{2}$ is irrational.

Corollaries will follow a similar convention as theorems. Below lies an example.

Corollary 0.4.
There does not exist a rational number r such that $r^2 = 13$.

As with definitions, theorems used for connections to linear algebra will follow a similar convention but with a slight modification as shown below.

Theorem 0.5. Fundamental Theorem of Linear Maps:
Suppose V is finite-dimensional and $T \in \mathcal{L}(V, W)$. Then $\mathsf{range}(T)$ is finite-dimensional and

$$\mathsf{dim}(V) = \mathsf{dim}(\mathsf{null}(T)) + \mathsf{dim}(\mathsf{range}(T)).$$

1 Rings and Fields

1.1 Definitions and Basic Properties

We will begin with some discussion on rings, integral domains, fields, and groups.

Definition 1.1. ⟨ *noun, set together with two operations* ⟩
A **ring** is a non-empty set R, with two binary operations[a] called addition and multiplication, denoted $+$ and $\cdot$ respectively, satisfying the following:

R1. *associativity of addition,* for all $a, b, c \in R$,

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

R2. *commutativity of addition,* for all $a, b \in R$,

$$a + b = b + a$$

R3. *existence of 0,* there exists a $0 \in R$ such that for all $a \in R$,

$$a + 0 = a$$

R4. *existence of negatives,* for all $a \in R$ there exists $-a \in R$ such that,

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

R5. *associativity of multiplication,* for all $a, b, c \in R$,

$$(ab)c = a(bc)$$

R6. *distributive laws,* for all $a, b, c \in R$,

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc.$$

[a] See Gallian (pg. 42) [2]

Rings are a large area of study within abstract algebra. Below are a few examples and nonexamples of rings.

- The set $\mathbb{R}$ is a ring under the usual operations of addition and multiplication.
- The set $\mathbb{Z}$ is a ring under the usual operations of addition and multiplication.
- The set of 2×2 matrices with entries from a field[2] F denoted

$$M_2(F) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in F \right\}$$

  is an example of a ring under the usual matrix operations of addition and multiplication.
- The set $\mathbb{N}$ is **not** a ring (it doesn't have a zero element).
- The set $\mathbb{P} \cup \{0\}$ is **not** a ring (there are no additive inverses).
- The set of 2×2 symmetric matrices with entries from a field F denoted

$$S_2(F) \coloneqq \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \middle| a, b, c \in F \right\}$$

  is **not** an example of a ring under the usual matrix operations of addition and multiplication (the product of two symmetric matrices need not be symmetric).

Notice the definition of a ring does not require multiplication to be commutative. Rings may possess commutative multiplication, below lies the complete definition.

Definition 1.2. ⟨ *adjective, describing a ring* ⟩
A **commutative** ring is a non-empty set R with two binary operations called addition and multiplication, denoted $+$ and $\cdot$ respectively, that satisfy properties R1-R6 of a ring with the addition of the following seventh property:

R7. *commutativity of multiplication,* for all $a, b \in R$,

$$ab = ba.$$

According to Howie the textbook will be primarily focused on commutative rings. Below are a few examples and nonexamples of commutative rings.

- The ring $\mathbb{R}$ under the usual operations of addition and multiplication is commutative.
- The ring $\mathbb{Z}$ under the usual operations of addition and multiplication is commutative.

[2]Refer to definition 1.6.

- The ring of 2×2 matrices with entries from a field F denoted

$$M_2(F) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in F \right\}$$

under the usual matrix operations of addition and multiplication is **not** an example of a commutative ring.

- The quaternions $\mathbb{H} \coloneqq \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$ form a ring under the usual operations of addition and multiplication but are **not** commutative.

Definition 1.3. $\langle$ *noun, ring with identity* $\rangle$
A **ring with unity** is a non-empty set R with two binary operations called addition and multiplication, denoted $+$ and $\cdot$ respectively, that satisfy properties R1-R6 of a ring with the addition of the following eighth property:

R8. *existence of 1,* there exists $1 \in R$ such that for all $a, b \in R$,

$$a1 = 1a = a.$$

The element 1 is called the **unity element**.

Below are a few examples and nonexamples of rings with unity.

- The ring $\mathbb{R}$ under the usual operations of addition and multiplication has 1.
- The ring $\mathbb{Z}$ under the usual operations of addition and multiplication has 1.
- The ring of 2×2 matrices with entries from a field F denoted

$$M_2(F) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in F \right\}$$

under the usual matrix operations of addition and multiplication is an example of a ring with unity. The unity element is the 2×2 identity matrix I_2.

- The ring of even integers $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ under the usual operations of addition and multiplication does **not** have a unity element.

Definition 1.4. ⟨ *noun, commutative ring with unity and cancellation* ⟩
An **integral domain** is a non-empty set D with two binary operations called addition and multiplication, denoted $+$ and $\cdot$ respectively, that satisfy properties R1-R8, of a commutative ring with the addition of the following ninth property:

R9. *cancellation,* for all $a, b, c \in D$ with $c \neq 0$,

$$ca = cb \implies a = b.$$

Property R9 is equivalent to:

R9′. *no divisors of zero*[a], for all $a, b \in D$,

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

[a]See Gallian (pg. 237) [2]

Integral domains are the generalization of integers. Below are a few examples and nonexamples of integral domains.

- The ring $\mathbb{R}$ under the usual operations of addition and multiplication is an integral domain.
- The ring $\mathbb{Z}$ under the usual operations of addition and multiplication is an integral domain.
- The ring $\mathbb{Z}_6$ under addition modulo 6 and multiplication modulo 6 is **not** an integral domain.
- The ring of 2×2 matrices with entries from a field F denoted

$$M_2(F) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in F \right\}$$

  under the usual matrix operations of addition and multiplication is **not** an integral domain because it contains zero divisors.

As stated in the definition of integral domains, a commutative ring R with unity has cancellation if and only if R has no divisors of zero. This statement was proved in exercise 1.4 but will also be proved below.

Theorem 1.5. Equivalence of R9 and R9′:
Let R be a commutative ring with unity. For all $a, b, c \in R$ with $c \neq 0$,

$$ca = cb \implies a = b$$

if and only if for all $a, b \in R$,

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Proof. Let R be a commutative ring with unity. Suppose for all $a, b, c \in R$ with $c \neq 0$, $ca = cb \implies a = b$. Let $a, b \in R$ with $ab = 0$. Note, $ab = 0 = a0$ implies $b = 0$, or $ba = ab = 0 = b0$ implies $a = 0$. Therefore, cancellation implies no zero divisors. Now suppose for all $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$. Let $a, b, c \in R$ with $c \neq 0$ and $ca = cb$. Note, $c(a + (-b)) = ca + c(-b) = cb + c(-b) = 0$ so $a + (-b) = 0$ and therefore $a = b$. Hence no zero divisors implies cancellation, and the theorem is proved.

□

Definition 1.6. ⟨ *noun, commutative ring with unity and multiplicative inverses* ⟩
A **field** is a non-empty set R with two binary operations called addition and multiplication, denoted $+$ and $\cdot$ respectively, that satisfy properties R1-R8 of a ring with the addition of the following tenth property:

R10. *existence of multiplicative inverses,* for all $a \in R$ with $a \neq 0$, there exists an $a^{-1} \in R$ such that

$$aa^{-1} = 1.$$

A field is a generalization of the rational numbers. Below are a few examples and nonexamples of fields.

- The ring $\mathbb{Q}$ under the usual operations of addition and multiplication is a field.
- The ring $\mathbb{R}$ under the usual operations of addition and multiplication is a field.
- The ring $\mathbb{C}$ under the usual operations of addition and multiplication is a field.
- The set $\{0, 1\}$ is a field under addition modulo 2 and multiplication (shown in exercise 1.3).
- The integral domain $\mathbb{Z}$ under addition and multiplication is **not** a field.

- The set of polynomials with integer coefficients $\mathbb{Z}[x]$ is an integral domain but **not** a field.

Property R10 implies R9 but the converse in general is not true. Below is a restatement of this fact.

Theorem 1.7. All fields are integral domains:
If F is a field then F is also an integral domain.

Proof. Let F be a field. We will show that F is also an integral domain. Let $a, b, c \in F$ with $c \neq 0$. Suppose $ca = cb$, then we can see $a = (c^{-1}c)a = c^{-1}(ca) = c^{-1}(cb) = (c^{-1}c)b = b$. Therefore F has cancellation, hence F is an integral domain. □

Example. Consider the field $\mathbb{R}$. Let $a, b, c \in \mathbb{R}$ with $c \neq 0$. It is well known that $ca = cb \implies a = b$. A specific example follows, $15 = 15 \implies 3 \cdot 5 = 3 \cdot 5 \implies 5 = 5$.

Definition 1.8. ⟨ *noun, set with one binary operation* ⟩
A **group** is a non-empty set G with a binary operation called multiplication, denoted $\cdot$, that satisfies the following:

G1. *associativity,* for all $a, b, c \in G$,

$$(ab)c = a(bc)$$

G2. *existence of an identity element,* there exists an $\exists e \in G$ such that for all $a \in G$,

$$ea = a$$

G3. *existence of inverses*, for all $a \in G$ there exists an $a^{-1} \in G$ such that,

$$a^{-1}a = e.$$

Group theory is, in essence, the study of symmetry. Groups are a major topic in abstract algebra. Below are a few examples and nonexamples of groups.

- The set $\mathbb{Z}$ under addition is a group.
- The set $\mathbb{Z}_n \coloneqq \{0, 1, \cdots, n-1\}$ under addition modulo n is a group.

- The set S_n of all permutation of n items is a group.
- The set of all 2×2 matrices with real entries and nonzero determinants, denoted

$$GL(2,R) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\}$$

  under matrix multiplication is a group.
- The set $\mathbb{Z}$ under multiplication is **not** a group.
- The set $\mathbb{R}$ under multiplication is **not** a group.
- The set $\mathbb{Q}\backslash\{0\}$ under addition is **not** a group.

Definition 1.9. ⟨ *adjective, group* ⟩
An **abelian** group is a non-empty set G with a binary operation called multiplication, denoted $\cdot$, that satisfy properties G1-G3 of a group with the addition of the following fourth property:

G4. *commutativity,* for all $a, b \in G$,

$$ab = ba.$$

Groups need not be abelian. Below are a few examples of abelian and nonabelian groups

- The group Z_n of integers under addition modulo n is an abelian group.
- The group R_n under addition is an abelian group.
- The group S_n of permutations is **not** an abelian group.
- The group of 2×2 matrices with real entries and nonzero determinants $GL(2,R)$ under matrix multiplication, is **not** an abelian group.

Definition 1.10. ⟨ *noun, group of elements of a ring* ⟩
The **group of units** of a commutative ring with unity R is defined by,

$$U \coloneqq \{u \in R : \exists v \in R \text{ such that } uv = 1\}.$$

Example. Consider the commutative ring with unity $\mathbb{Q}$. Note, for all nonzero elements of $p/q \in \mathbb{Q}$, there exists an element $q/p \in \mathbb{Q}$ such that $(p/q)(q/p) = 1$, thus the group of units of $\mathbb{Q}$ is the set $\mathbb{Q}\backslash\{0\}$.

Example. Consider the commutative ring with unity $\mathbb{Z}_6 \coloneqq \{0, 1, 2, 3, 4, 5\}$. Note, the group of units of $\mathbb{Z}_6$ is the set $U = \{1, 5\}$. Note, the group of units for this set is not the set of all nonzero elements of $\mathbb{Z}_6$.

It is curious that $\mathbb{Z}_6$ was chosen instead of the more general $\mathbb{Z}_n$. The choice of $\mathbb{Z}_6$ was made to illustrate there are rings whose group of units is a proper subset of the nonzero elements of the ring. We conjecture a statement below.

Claim: The group of units of the ring $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$ if and only if n is prime.

Proof. Consider the ring $\mathbb{Z}_n$ under addition modulo n and multiplication modulo n.

We will show if n is prime then the group of units is $U = \mathbb{Z}_n\backslash\{0\}$. Suppose n is prime and let $a \in \mathbb{Z}_n\backslash\{0\}$. Note, a and n share no common factors. Thus, for all $a, b \in \mathbb{Z}_n\backslash\{0\}$, $ab \neq 0$ meaning $\mathbb{Z}_n$ is an integral domain. Hence, for all a^k with $k \in \mathbb{N}$, $a^k \neq 0$. Since $\mathbb{Z}_n$ is a finite ring, there must be $i, j \in \mathbb{N}$ with $i < j$ such that $a^i = a^j$. By cancellation we have $1 = a^{j-i}$ and thus $a(a^{j-i-1}) = 1$. Therefore a is a unit. Since $0a = 0$ for all $a \in \mathbb{Z}_n$, 0 is not a unit. Therefore the group of units of $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$.

We will now show if the group of units of $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$, then n is prime. Assume the group of units of $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$. So, for all nonzero elements $a \in \mathbb{Z}_n$, there exists $a^{-1} \in \mathbb{Z}_n$ such that $aa^{-1} = 1$. Therefore $\mathbb{Z}_n$ is a field. By Theorem 1.7, fields are integral domains, so for all $a, b \in \mathbb{Z}_n$ $ab = 0$ implies $a = 0$ or $b = 0$. Therefore there are no nonzero elements of $\mathbb{Z}_n$ whose product is 0, hence n is relatively prime to each element in $\mathbb{Z}\backslash\{0\}$, and n is prime.

Therefore, the group of units of the ring $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$ if and only if n is prime. □

Our claim can now be stated as a theorem.

Theorem 1.11. Group of Units of a $\mathbb{Z}_n$:
The group of units of the ring $\mathbb{Z}_n$ is $U = \mathbb{Z}_n\backslash\{0\}$ if and only if n is prime.

Below are a few examples of this theorem. Most can be easily verified.

- The group of units of the ring $\mathbb{Z}_2$ is the set $U = \{1\}$.
- The group of units of the ring $\mathbb{Z}_3$ is the set $U = \{1, 2\}$.
- The group of units of the ring $\mathbb{Z}_4$ is the set $U = \{1, 3\}$.

- The group of units of the ring $\mathbb{Z}_{2^{82589933}-1}$ is the set $U = \{k \in \mathbb{N} : k < 2^{82589933} - 1\}$[3].
- The group of units of the ring $\mathbb{Z}_{16}$ is the set $U = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

The proof of Theorem 1.11 is very similar to the proof in exercise 1.5. We will state the theorem and a proof below.

Theorem 1.12. Finite integral Domains are Field:
A finite integral domain D is a field.

Proof. Let D be a finite integral domain and let $a \in D\backslash\{0\}$. If $a = 1$ then $aa = 1(1) = 1$ and we are done. If $a \neq 1$ then consider the elements $a, a^2, a^3, \ldots$. Since D is finite there must be two elements in this list that are equal, say a^i and a^j. Without loss of generality say $i > j$. Note, $a^i = a^j \implies a^j a^{i-j} = a^j 1 = \implies a^{i-j} = 1$. Therefore, the inverse of a is a^{i-j-1} because $aa^{i-j-1} = a^{i-j} = 1$. Thus, all nonzero elements of D have inverses, so D is a field. □

Definition 1.13. ⟨ *noun, relationship between ring elements* ⟩
If a and b are elements of a ring R and $a = ub$ for some $u \in U$, we say a and b are **associates** and write $a \sim b$.

Example. Consider the ring $\mathbb{Z}$. Note, the group of units of $\mathbb{Z}$ is $U = \{1, -1\}$. For all $a \in \mathbb{Z}$, $a = 1(a)$ and $a = -1(-a)$. Therefore, for all $a \in \mathbb{Z}$, $a \sim a$ and $a \sim -a$.

Theorem 1.14. Group of Units of a Field:
A group of units of a field K is the group K^* of all non-zero elements of K.

Proof. Let K be a field and let $K^* \coloneqq \{a \in K : a \neq 0\}$ and let $k \in K^*$. Note, $k \neq 0$, so by the definition of a field there exists $k^{-1} \in K$ such that $kk^{-1} = 1$, thus k is a unit. Additionally, 0 cannot be a unit. Therefore, the set K^* is the group of units. □

Example. Consider the field $\mathbb{Q}$. The set $\mathbb{Q}^* \coloneqq \{p/q : p, q \in \mathbb{Z}\backslash\{0\}\}$. Let $p/q \in \mathbb{Q}^*$. Note, $(p/q)(q/p) = 1/1 = 1$ so therefore p/q is a unit.

[3]As of October 6th, 2024, the number $2^{82589933} - 1$ is the largest known prime.

Definition 1.15. ⟨ *verb, performed by one element of a ring on another* ⟩
In an integral domain D, if an element $a \in D\backslash\{0\}$ and element $b \in D$ we say a **divides** b, or that a is a **divisor** of b, or that a is a **factor** of b if there exists a $z \in D$ such that $az = b$. We write $a|b$, and sometimes write $a \nmid b$ if a does not divide b.

We say a is a **proper divisor** or a **proper factor** of b, or that a **properly divides** b if z is not a unit. Equivalently, a is a proper divisor of b if and only if $a|b$ and $b \nmid a$.

Example. Consider the integral domain $\mathbb{Z}$. Note, $6 \cdot 4 = 24$, so $6 \mid 24$.

1.2 Subrings, Ideals, and Homomorphisms

Much of the material in this section can be adapted with alteration to fit rings in general. Throughout the section our rings are assumed, without explicit mention, to be commutative. Additionally, standard algebraic notaion will be used, e.g. $a - b$ will be written instead of $a + (-b)$.

Definition 1.16. ⟨ *noun, ring contained in another ring* ⟩
A **subring** U of a ring R is a non-empty subset of R with the property that for all $a, b \in R$,

1. if $a, b \in U$ then $a - b, ab \in U$.

Equivalently, for all $a, b \in R$,

1. if $a, b \in U$ then $a + b, ab \in U$,
2. if $a \in U$ then $-a \in U$.

Below are a few examples and nonexamples of subrings.

- The set of even integers $2\mathbb{Z} \coloneqq \{2k : k \in \mathbb{Z}\}$ is a subring of the ring $\mathbb{Z}$.
- The set $\mathbb{Z}$ is a subring of the ring $\mathbb{Q}$.
- The set $\mathbb{Q}$ is a subring of the ring $\mathbb{R}$.
- The set of odd integers $\{2k + 1 : k \in \mathbb{Z}\}$ does **not** form subring of $\mathbb{Z}$.
- The set of positive rational numbers $\mathbb{Q}^+$ does **not** form a subring of $\mathbb{Q}$.

Definition 1.17. ⟨ *noun, field contained in another field* ⟩
A **subfield** E is a subset of a field K, containing at least two elements, such that for all $a, b \in K$,

1. if $a, b \in E$ then $a - b \in E$,
2. if $a \in E, b \in E \backslash \{0\}$ then $ab^{-1} \in E$.

Equivalently, for all $a, b \in K$,

1. if $a, b \in E$ then $a - b \in E$,
2. if $a, b \in E$ then $ab \in E$,
3. if $a \in E \backslash \{0\}$ then $a^{-1} \in E$.

If $E \subset K$ we say E is a **proper** subfield of K.

Below are a few examples and nonexamples of subfields.

- The set $\mathbb{Q}$ is a subfield of the field $\mathbb{R}$ ($\mathbb{Q}$ is also a proper subfield).
- The set $\mathbb{R}$ is a subfield of the field $\mathbb{C}$ ($\mathbb{R}$ is also a proper subfield).
- The set $\mathbb{C}$ is a subfield of the field $\mathbb{C}$.
- The set $\mathbb{Z}$ is **not** a subfield of the field $\mathbb{R}$ ($\mathbb{Z}$ is not a field).

Definition 1.18. ⟨ *noun, subring with additional property* ⟩
An **ideal** I of a ring R is a non-empty subset of R with the properties,

1. if $a, b \in I$ then $a - b \in I$,
2. if $a \in I$ and $r \in R$ then $ra \in I$.

The ideal I is said to be **proper** if $\{0\} \subset I \subset R$.

Example. Consider the ring $\mathbb{Z}$. The subset $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Additionally, $2\mathbb{Z}$ is a proper ideal. Below lies a proof.

Proof. Let $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Note, $2 \cdot 0 = 0 \in 2\mathbb{Z}$ so $2\mathbb{Z}$ is nonempty. Let $a, b \in 2\mathbb{Z}$. For some $k, j \in \mathbb{Z}$, $a = 2k$ and $b - 2j$. Note, $a - b = 2k - 2j = 2(k - j) \in 2\mathbb{Z}$. Thus the

first condition of an ideal is met. Now let $a \in 2\mathbb{Z}$ and $r \in \mathbb{Z}$. For some $k \in \mathbb{Z}$, $a = 2k$. Note, $ra = r2k = 2(rk) \in 2\mathbb{Z}$, and the second condition is met. Therefore $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Additionally, $1 \in \mathbb{Z}$ but $1 \notin 2\mathbb{Z}$ so $2\mathbb{Z}$ proper subset of $\mathbb{Z}$, and since $\{0\} \subset 2\mathbb{Z}$ we can say $2\mathbb{Z}$ is a proper ideal. □

It should be noted that the definition of an ideal looks very similar to the definition of a subring. It happens that ideals are also subrings. We will state this as a theorem and provide a proof below.

Theorem 1.19. Ideals are Subrings:
Let I be an ideal of a ring R. Then, I is a subring of R.

Proof. Let I be an ideal of a ring R. Let $a, b \in I$. Note, by the definition of an ideal $a - b \in I$. Therefore I is closed under subtraction. Note $a \in R$, thus $ab \in I$ and I is closed under multiplication. Therefore I is a subring. □

Theorem 1.20. Smallest ideal containing A:
Let $A \coloneqq \{a_1, a_2, \ldots, a_n\}$ be a finite set of elements of a commutative ring R with unity. Then, the set[a]

$$Ra_1 + Ra_2 + \cdots + Ra_n \coloneqq \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in R\}$$

is the smallest[b] ideal of R containing A.

[a] The set described is referred to as the **ideal generated** by $a_1, a_2, \ldots, a_n$.
[b] Smallest here refers to inclusion.

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ be a finite subset of a commutative ring R. We claim

$$\mathcal{R}_A \coloneqq Ra_1 + Ra_2 + \cdots + Ra_n = \{x_1a_1 + x_2a_2 + \cdots + x_na_n : x_1, x_2, \ldots, x_n \in R\}$$

is the smallest ideal of R containing A. First we will show $\mathcal{R}_A$ contains A. Note, for a_j with $j \leq n$, $1a_j + \sum_{i=1, j\neq j}^{n} 0a_i = a_j \in \mathcal{R}_A$. Thus $A \subseteq \mathcal{R}_A$.

Next we will show $\mathcal{R}_A$ is an ideal. Let $x, y \in \mathcal{R}_A$. Note, $x = x_1a_1 + x_2a_2 + \cdots + x_na_n$ for some $x_1, x_2, \ldots, x_n \in R$ and $y = y_1a_1 + y_2a_2 + \cdots + y_na_n$ for some $y_1, y_2, \ldots, y_n \in R$. We

will show $x - y$ is in $\mathcal{R}_A$ below,

$$\begin{aligned} x - y &= x_1a_1 + x_2a_2 + \cdots + x_na_n - (y_1a_1 + y_2a_2 + \cdots + y_na_n) \\ &= x_1a_1 + x_2a_2 + \cdots + x_na_n - y_1a_1 - y_2a_2 - \cdots - y_na_n \\ &= x_1a_1 - y_1a_1 + x_2a_2 - y_2a_2 + \cdots + x_na_n - y_na_n \\ &= (x_1 - y_1)a_1 + (x_2 - y_2)a_2 + \cdots + (x_n - y_n)a_n \in \mathcal{R}_A. \end{aligned}$$

Now let $x \in \mathcal{R}_A$ with $x = x_1a_1 + x_2a_2 + \cdots + x_na_n$ for some $x_1, x_2, \ldots, x_n \in R$ and let $r \in R$. We will show $rx \in \mathcal{R}_A$ below,

$$\begin{aligned} rx &= r(x_1a_1 + x_2a_2 + \cdots + x_na_n) \\ &= rx_1a_1 + rx_2a_2 + \cdots + rx_na_n \\ &= (rx_1)a_1 + (rx_2)a_2 + \cdots + (rx_n)a_n \in \mathcal{R}_A. \end{aligned}$$

Therefore, $\mathcal{R}_A$ is an ideal.

Now we will show $\mathcal{R}_A$ is the smallest ideal of R containing A. Let I be an ideal of R with $A \subseteq I$. Let $x \in \mathcal{R}_A$ with $x = x_1a_1 + x_2a_2 + \cdots + x_na_n$ for some $x_1, x_2, \ldots, x_n \in R$. Note, each $x_ja_j \in I$ by the definition of an ideal. Since an ideal is a subring and therefore closed under addition, $x = x_1a_1 + x_2a_2 + \cdots + x_na_n \in I$. Thus $\mathcal{R}_A \subseteq I$.

Therefore $\mathcal{R}_A$ is the smallest ideal of R containing A. □

Example. Consider the commutative ring $\mathbb{Z}_6$ under addition modulo 6 and multiplication modulo 6. Consider the set $A = \{2, 3\}$. Then the set

$$\mathbb{Z}_62 + \mathbb{Z}_63 = \{x_12 + x_23 : x_1, x_2 \in \mathbb{Z}_6\} = \{0, 2, 4, 3\}$$

contains A, and is the smallest idea of $\mathbb{Z}_6$ containing A.

Definition 1.21. ⟨ *noun, ideal generated by a single element* ⟩
A **principal ideal** is an ideal of a ring R if it is generated by a single element $a \in R$, denoted $Ra = \langle a \rangle$.

Example. An example of a principal ideal of the ring $\mathbb{Z}$ is the ideal generated by 6, namely $\langle 6 \rangle = 6\mathbb{Z} = \{6k : k \in \mathbb{Z}\}$.

Theorem 1.22. Properties of ideals of integral domains:
Let D be an integral domain with group of units U, and let $a, b \in D\backslash\{0\}$. Then,

1. $\langle a\rangle \subseteq \langle b\rangle$ if and only if $b \mid a$,
2. $\langle a\rangle = \langle b\rangle$ if and only if $a \sim b$,
3. $\langle a\rangle = D$ if and only if $a \in U$.

Proof. Let D be an integral domain with group of units U and let $a, b \in D\backslash\{0\}$.

1. We will show $\langle a\rangle \subseteq \langle b\rangle$ if and only if $b \mid a$.

   Suppose $\langle a\rangle \subseteq \langle b\rangle$. Note, $a \in \langle a\rangle$ so $a \in \langle b\rangle$, thus there exists $z \in D$ such that $bz = a$, so $b \mid a$.

   Suppose $b \mid a$. Let $c \in \langle a\rangle$. Note, there exists $z \in D$ such that $bz = a$. So for some $k \in D$, $c = ka$, thus $c = ka = k(bz) = (kz)b$. Since $kz \in D$, $c \in \langle b\rangle$ and $\langle a\rangle \subseteq \langle b\rangle$.

   Therefore, $\langle a\rangle \subseteq \langle b\rangle$ if and only if $b \mid a$.

2. We will show $\langle a\rangle = \langle b\rangle$ if and only if $a \sim b$.

   Suppose $a \sim b$. Then $au = b$ and $bv = a$ for $u, v \in U$, so $a \mid b$ and $b \mid a$. By part 1, we know $\langle a\rangle \subseteq \langle b\rangle$ and $\langle b\rangle \subseteq \langle a\rangle$, so $\langle a\rangle = \langle b\rangle$.

   Now suppose $\langle a\rangle = \langle b\rangle$. By part 1, we know $a \mid b$ and $b \mid a$ so for some $u, v \in D$, $au = b$ and $bv = a$. Therefore, $(au)(bv) = (ab)(uv) = (ab)1$ and by cancellation we get $uv = 1$, so $u, v \in U$ and $a \sim b$.

   Therefore $\langle a\rangle = \langle b\rangle$ if and only if $a \sim b$.

3. We will show $\langle a\rangle = D$ if and only if $a \in U$.

   Suppose $a \in U$. Note, $\langle a\rangle \subseteq D$ by definition. Let $b \in D$. Note, for some $c \in U$, $ac = 1$. Also note, $bc \in D$, and $(bc)a = b(ac) = b1 = b \in \langle a\rangle$, so $D \subseteq \langle a\rangle$. Therefore $\langle a\rangle = D$.

   Suppose $\langle a\rangle = D$. Since $1 \in \langle a\rangle$, there must be some $c \in D$ such that $ac = 1$, therefore $a \in U$.

   Therefore, $\langle a\rangle = D$ if and only if $a \in U$.

□

Example. We will show a few examples using each part of the theorem below.

1. Consider the integral domain $\mathbb{Z}$ with group of units $U = \{1, -1\}$. Consider $2\mathbb{Z} = \langle 2 \rangle$ and $6\mathbb{Z} = \langle 6 \rangle$. Note, $\langle 6 \rangle \subseteq \langle 2 \rangle$ because $6k = 2(3k) \in \langle 2 \rangle$. It is also clear $2 \mid 6$.

2. Consider the integral domain $\mathbb{Z}$ with group of units $U = \{1, -1\}$. Note $7\mathbb{Z} = \langle 7 \rangle = \langle -7 \rangle = -7\mathbb{Z}$ and $7 = (-1)7$, so $7 \sim -7$.

3. Consider the integral domain $\mathbb{Z}$ with group of units $U = \{1, -1\}$. Note, $-1\mathbb{Z} = \langle -1 \rangle = \mathbb{Z}$.

Definition 1.23. $\langle$ *noun, function* $\rangle$
A **homomorphism** from a ring R to a ring S is a mapping $\varphi : R \to S$ with the following properties,

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$,

2. $\varphi(ab) = \varphi(a)\varphi(b)$.

Example. Consider the function $\varphi : \mathbb{Z} \to S$ where

$$S \coloneqq \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R} \right\}$$

defined by

$$\varphi(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}.$$

We will show φ is a homomorphism.

Proof. Let $\varphi : \mathbb{Z} \to S$ be a function. Let $a, b \in \mathbb{Z}$. First we will show φ preserves addition. Note,

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

Next we will show φ preserves multiplication. Note,

$$\begin{aligned}\varphi(a)\varphi(b) &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \\ &= \begin{pmatrix} ab+0\cdot 0 & a0+0b \\ 0b+a0 & 0\cdot 0+ab \end{pmatrix} \\ &= \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \\ &= \varphi(ab).\end{aligned}$$

Since φ preserves addition and multiplication, φ is a homomorphism. □

Theorem 1.24. Properties of Homomorphisms:
Let R and S be rings with zero elements 0_R and 0_S. Let $\varphi : R \to S$ be a homomorphism. Then,

1. $\varphi(0_R) = 0_S$,
2. for all $r \in R$, $\varphi(-r) = -\varphi(r)$,
3. $\varphi(R)$ is a subring of S.

Proof. Let R and S be rings with zero elements 0_R and 0_S. Let $\varphi : R \to S$ be a homomorphism. Then,

1. We will show $\varphi(0_R) = 0_S$. Let $a \in R$. Note $\varphi(a) = \varphi(a + 0_R) = \varphi(a) + \varphi(0_R)$ so by the definition of 0, $\varphi(0_R) = 0_S$.
2. We will show for all $r \in R$, $\varphi(-r) = -\varphi(r)$. Let $r \in R$. Note $0_S = \varphi(0_R) = \varphi(r + (-r)) = \varphi(r) + \varphi(-r)$ which implies $\varphi(-r) = -\varphi(r)$.
3. We will show $\varphi(R)$ is a subring of S. Let $\varphi(a), \varphi(b) \in R$. Note $\varphi(a) - \varphi(b) = \varphi(a-b) \in \varphi(R)$. Also note, $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(R)$. By the definition of a subring, $\varphi(R)$ is a subring of S.

□

Example. Let $\varphi : \mathbb{Z} \to S$ be the homomorphism defined above. Below we will show an example using each part of the theorem.

1. The zero elements of S is
$$0_S = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
So it is easy to see $\varphi(0) = 0_S$.

2. Let $k \in \mathbb{Z}$. Note,
$$\varphi(k) = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$$
and
$$\varphi(-k) = \begin{pmatrix} -k & 0 \\ 0 & -k \end{pmatrix}.$$
Thus,
$$\begin{aligned} \varphi(k) + \varphi(-k) &= \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} + \begin{pmatrix} -k & 0 \\ 0 & -k \end{pmatrix} \\ &= \begin{pmatrix} k-k & 0 \\ 0 & k-k \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ &= 0_S. \end{aligned}$$

3. Let $\varphi(a), \varphi(b) \in S$. Note,
$$\varphi(a) - \varphi(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & a-b \end{pmatrix} \in \varphi(\mathbb{Z}).$$
Additionally,
$$\varphi(a)\varphi(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} \in \varphi(\mathbb{Z}).$$
Thus $\varphi(\mathbb{Z})$ is a subring of S.

Corollary 1.25.
If R and S are rings and $\varphi : R \to S$ is a homomorphism and $a, b \in R$, then $\varphi(a-b) = \varphi(a) - \varphi(b)$.

Proof. Let R and S be rings and let $\varphi : R \to S$ be a homomorphism. Let $a, b \in R$. By the definition of a homomorphism, and Theorem 1.24 we have $\varphi(a-b) = \varphi(a) + \varphi(-b) =$

$\varphi(a) - \varphi(b)$. □

Definition 1.26. ⟨ *noun, homomorphism* ⟩
A **monomorphism** from a ring R to a ring S is a homomorphism $\varphi : R \to S$ that is injective. A monomorphism may also be referred to as an **embedding**.

Definition 1.27. ⟨ *noun, homomorphism* ⟩
A **isomorphism** from a ring R to a ring S is a homomorphism $\varphi : R \to S$ that is bijective. We say rings R and S are **isomorphic** and write $R \simeq S$.

Definition 1.28. ⟨ *noun, isomorphism* ⟩
An **automorphism** is an isomorphism from a ring R onto itself.

Definition 1.29. ⟨ *noun, set* ⟩
Let $\varphi : R \to S$ be a homomorphism between rings R and S with zero elements 0_R and 0_S, respectively. The set

$$K = \varphi^{-1}(0_S) \coloneqq \{a \in R : \varphi(a) = 0_S\}$$

is called the **kernel** of the homomorphism φ, denoted $\mathsf{ker}\varphi$.

kernel is a subring.

In the world of rings and homomorphisms, the kernel of a homomorphism is the set of all elements that map to 0 in the codomain. There is an analogous concept in linear algebra relating to linear transformations.

Definition 1.30. ⟨ *noun, subset* ⟩
For $T \in \mathcal{L}(V, W)$, the **null space** of T, denoted $\mathsf{null}(T)$, is the subset of V consisting of those vectors that T maps to 0:

$$\mathsf{null}(T) \coloneqq \{v \in V : T(v) = 0\}.$$

As defined here, the set of all elements of that map to 0 in a linear transformation is called the null space of the linear transformation. It is also sometimes referred to the kernel of the linear transformation. Both concepts represent the same idea of the set of elements in the domain of a function that map to 0. It turns, out the null space is a subspace of the

domain. There is a similar result for the kernel of a homomorphism.

Definition 1.31. ⟨ *noun, ideal plus an element* ⟩
Let I be an ideal of a ring R and let $a \in R$. The set

$$a + I \coloneqq \{a + x : x \in I\}$$

is called the **residue class of** a **modulo** I.

Theorem 1.32. Properties of residue classes:
Let I be an ideal of a ring R and let $a, b \in R$. Then,

1. $a + I = b + I$ if and only if $a - b \in I$,
2. $(a + I) + (b + I) = (a + b) + I$,
3. $(a + I)(b + I) \subseteq ab + I$.

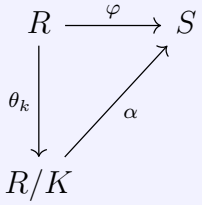
Definition 1.33. ⟨ *noun, ring* ⟩
The set R/I of all residue classes modulo I forms a ring with respect to the operations

1. $(a + I) + (b + I) = (a + b) + I$,
2. $(a + I)(b + I) = (ab) + I$,

called the **residue class ring** modulo I.

Theorem 1.34.
Let n be a positive integer. The residue class ring $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ is a field if and only if n is prime.

Theorem 1.35.
Let R be a commutative ring, and let φ be a homomorphism from R onto a commutative ring S, with kernel K. Then there is an isomorphism $\alpha : R/K \to S$ such that the diagram



commutes.

1.3 The Field of Fractions of an Integral Domain

In this section we will describe how to construct a field out of an arbitrary integral domain. Let D be an integral domain and let

$$P(D) \coloneqq D \times D \backslash \{0\} = \{(a, b) : a, b \in D, b \neq 0\}.$$

Define the relation $\equiv$ on the set $P(D)$ by the rule that

$$(a, b) \equiv (a', b') \text{ if and only if } ab' = a'b.$$

Theorem 1.36.
The relation $\equiv$ is an equivalence relation.

Definition 1.37. ⟨ *noun, field* ⟩
The quotient set $Q(D) = P(D)/\equiv$ is called the **fields of fractions** of the integral domain D. The elements of $Q(D)$ are equivalence classes $[a, b] \coloneqq \{(x, y) \in P(D) : (x, y) \equiv (a, b)\}$, and will be denoted a/b. Two elements a/b and c/d are said to be equal if $ad = bc$.
Addition is defined by

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

and multiplication is defined by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Definition 1.37 describes a mapping from sets in $P(D)$ to elements in $Q(D)$ which can be thought of like fractions. A picture describing the idea of this definition lies below.

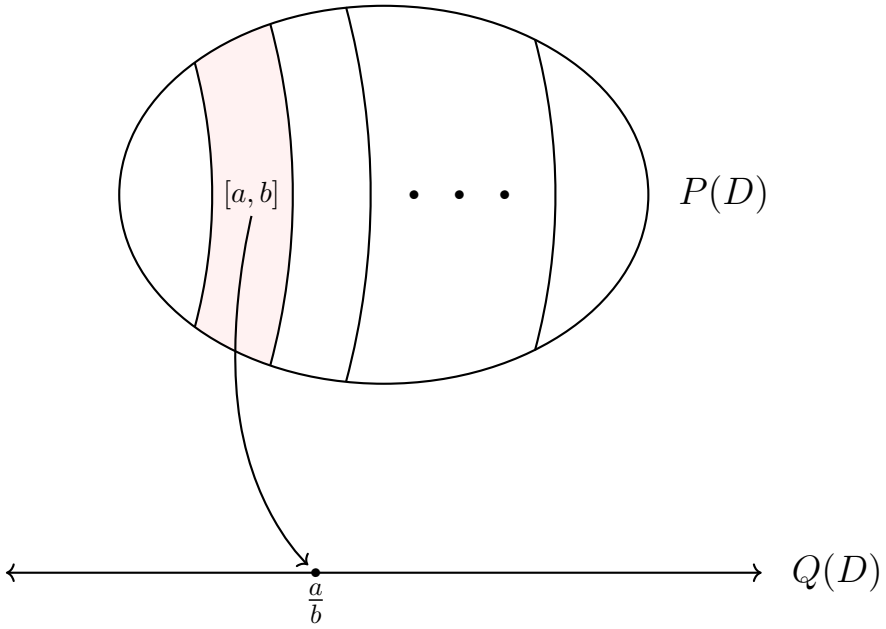


Figure 1.1: equivalence classes to field of fractions

It is important to note in this definition, we are mapping **subsets** of $P(D)$, to **elements** of $Q(D)$. In $P(D)$ we may refer to a set $[a, b]$ which is an equivalence class, but in $Q(D)$, $[a, b]$ is an element.

Theorem 1.38.
The addition and multiplication defined in Definition 1.37 are well-defined.

Theorem 1.39. Field of Fractions is a Field:
The field of fractions $Q(D)$ is a field.

Theorem 1.40.
The mapping $\varphi : D \to Q(D)$ given by

$$\varphi(a) = \frac{a}{1}$$

is a monomorphism.

Proof. Let $\varphi : D \to Q(D)$ be defined by $\varphi(a) = \frac{a}{1}$. Let $a, b \in D$. We will first show φ is a

homomorphism. Note,

$$\varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(b),$$

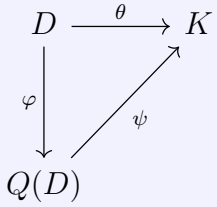
thus φ preserves addition. Note,

$$\varphi(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = \varphi(a)\varphi(b),$$

thus φ preserves multiplication and φ is a homomorphism. Suppose $a \neq b$. Note, $1a = a \neq b = 1b$ so $\varphi(a) = \frac{a}{1} \neq \frac{b}{1} = \varphi(b)$. Therefore, φ is a monomorphism. □

Theorem 1.41.
The field $Q(D)$ is the smallest field containing D.

Theorem 1.42.
Let D be an integral domain, let φ be the monomorphism form D into $Q(D)$ give by Theorem 1.40 and let K be a field with the property that there is a monomorphism θ from D into K. Then there exists a monomorphism $\psi : Q(D) \to K$ such that the diagram



commutes.

1.4 The Characteristic of a Field

In a ring R we can denote $a + a$ as $2a$, and more generally, $na = a + a + \cdots + a$ (n times) for $n \in \mathbb{N}$. If we define $0a = 0_R$ and $(-n)a = n(-a)$, then we can give meaning to na for all $n \in \mathbb{Z}$. We will provide a formal definition below.

Definition 1.43. ⟨ *noun, sum* ⟩
Let R be a ring and $a \in R$. For $n \in \mathbb{N}$, we define $na = \sum_{i=1}^{n} a$, $0a = 0_R$, and $(-n)a = n(-a)$.

Definition 1.44. ⟨ *noun, integer* ⟩
Let R be a commutative ring with unity. If $m1_R$ for $m \in \mathbb{N}$ are all distinct, then we say R has **characteristic** zero, and write $\mathsf{char}R = 0$.
If there exists $m, n \in \mathbb{N}$ such that $m1_R = (m+n)1_R$, in other words, $n1_R = 0_R$ and n is the least positive integer for which this occurs, we say R has characteristic n, and write $\mathsf{char}R = n$.

Theorem 1.45.
Let R be a commutative ring with unity with characteristic n. For all $a \in R$, $na = 0_R$.

Proof. Let R be a commutative ring with unity and characteristic n. Let $a \in R$. Note, $na = (n1_R)a = 0a = 0$. Thus, for all $a \in R$, $na = 0_R$. □

Theorem 1.46. Characteristic of a Field:
The characteristic of a field is either 0 or a prime number p.

The proof in Howie of this theorem doesn't seem to require that the set be a field, only that it is an integral domain.

Definition 1.47. ⟨ *noun, subfield* ⟩
Let K be a field. If K has characteristic zero, then we define the **prime subfield** of K to be the set

$$P(K) \coloneqq \left\{ \frac{m1_K}{n1_K} : m, n \in \mathbb{Z},\ n \neq 0 \right\}.$$

If K has prime characteristic p then the prime subfield of K is

$$P(K) \coloneqq \{0_K, 1_K, 2(1_K), \ldots, (p-1)1_K\}.$$

Theorem 1.48.
Let K be a field. Then K contains a prime subfield $P(K)$ contained in every subfield. If $\mathsf{char}K = 0$, then $P(K)$ is isomorphic to $\mathbb{Q}$. If $\mathsf{char}K = p$, a prime number, then $P(K)$ is isomorphic to $\mathbb{Z}_p$.

Remark 1.49.
Given an element a of a field K, we sometimes wish to denote $a/(n1)$ by a/n. If $\mathsf{char}K = 0$ this is no problem, but if $\mathsf{char}K = p$ then we cannot assign meaning to a/n when n is a multiple of p.

Theorem 1.50.
Let K be a field of characteristic p. Then for all $x, y \in K$,

$$(x+y)^p = x^p + y^p.$$

Theorem 1.51. Binomial Theorem:
Let R be a commutative ring with unity and let $n \in \mathbb{N}$. Then for all $a, b \in R$,

$$(a+b)^n = \sum_{r=0}^{n} a^{n-r} b^r.$$

Remark 1.52.
The fields $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ for a prime p are important building blocks in field theory. We usually find it convenient to write $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ with addition and multiplication carried out modulo p. The multiplication table for $\mathbb{Z}_5$ is

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

When it comes to $\mathbb{Z}_3$ we sometimes wish to write $\mathbb{Z}_3 = \{0, 1, -1\}$.

1.5 A Reminder of Some Group Theory

We will begin this section with several concrete examples of groups. We have had a very brief discussion of groups thus far. A few examples we have already seen are

- The set $\mathbb{Z}$ under addition is a group,
- The set $\mathbb{Z}_n \coloneqq \{0, 1, \ldots, n-1\}$ under addition modulo n is a group.

Below is a more interesting example of groups.

Example. Consider the square below.

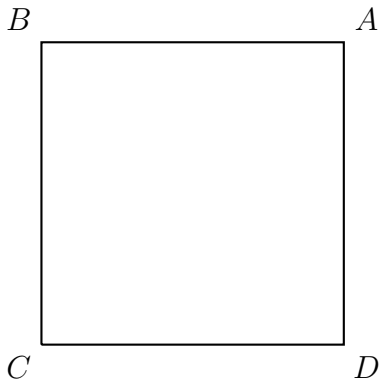


Figure 1.2: Square

The square has labels A, B, C and D on each of the corners. Notice that there are actions we could take on this square that leave it looking the same as before (except for the location of the letters). We could, for example, rotate the square 90 degrees and it would look the same as before. We are both able to rotate and flip the square, and leave it looking the same. The set of all rotations and flips of the square will be denoted $D_4 \coloneqq \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$, where R_θ represents a rotation of θ degrees, H represents a flip across the horizontal axis, V represents a flip across the vertical axis, and D and D' represent flips across diagonals. Below lies a summary of these actions.

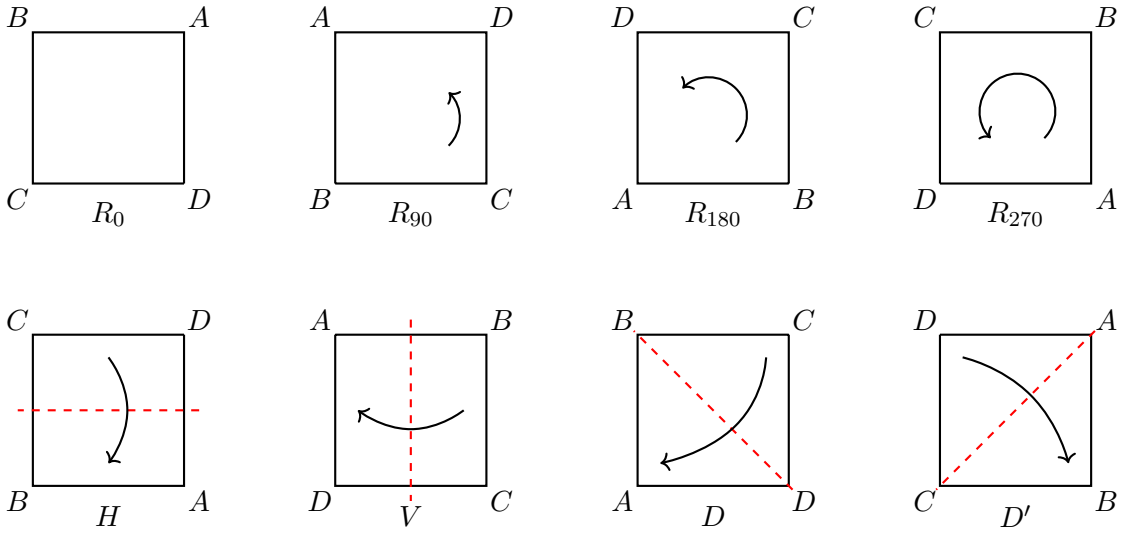


Figure 1.3: Elements of D_4

This set is called the Dihedral group of order 8. It is in fact a group. The identity element is R_0, as performing this action has no effect on the permutation of corners. We will draw a multiplication table[4] below. It should be noted, ab denotes the entry at the intersection of row a and column b. When performing the actions ab by hand on the square 1.2, action b should be performed, followed by action a (like function composition).

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Figure 1.4: Cayley Table of D_4

Since this set is small enough each condition of a group can be verified by hand. From looking at the cayley table we can see the element R_0 acts as the identity element. Each element has an inverse, and associativity can be verified. Additionally, the product of any two elements, is an element in the set. Therefore, D_4 is a group.

Theorem 1.53. Socks and Shoes Theorem:
Let G be a group and let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. Let G be a group and let $a, b \in G$. We will show $(ab)^{-1} = b^{-1}a^{-1}$. Note, $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Thus $(ab)^{-1} = b^{-1}a^{-1}$. □

Example. Let D_4 be the group as defined above with the multiplication table described in Figure 1.4. Consider the element (VR_{90}). Note, $V^{-1} = V$ and $R_{90}^{-1} = R_{270}$. We can see $(VR_{90})(R_{270}V) = VR_{90}R_{270}V = VR_0V = VV = R_0$. Thus $(VR_{90})^{-1} = (R_{270}V)$. As additional verification, note $(VR_{90}) = D'$ and $(R_{270}V) = D'$, since $D'^{-1} = D'$ we can see $(VR_{90})(R_{270}V) = D'D' = R_0$.

[4] Also referred to as a cayley table.

Definition 1.54. ⟨ *noun, group* ⟩
Let G be a group. If the set G is finite then G is called a **finite group**. The cardinality $|G|$ is called the **order** of the group.

We will describe a few examples of the order of finite groups below.

- Consider D_4 as described previously. This group has 8 elements, thus the order of D_4 is 8, written $|D_4| = 8$.
- Consider the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6. It is clear to see $\mathbb{Z}_6$ has 6 elements, thus $|\mathbb{Z}_6| = 6$.
- Let S_n be the group of all permutation of n items. There are $n!$ elements in S_n, therefore $|S_n| = n!$.

As seen in section 1.4, it is often tedious to write $aa \cdots a$ (n times), so it is far more convenient to write a^n. We will define this convention below.

Definition 1.55. ⟨ *noun, product* ⟩
Let G be a group and let $a \in G$. For $n \in \mathbb{N}$, define $a^n \coloneqq \prod_{i=1}^{n} a$, $a^0 \coloneqq e$, and $a^{-n} \coloneqq (a^{-1})^n = (a^n)^{-1}$.

Example. Consider the group D_4 as defined above. Note, $(R_{90})^3 = R_{90}R_{90}R_{90} = R_{270}$.

It should be noted this convention can be confusing in certain situations. Consider the group $\mathbb{Z}_6$. The element $3^3 = 3 + 3 + 3 = 9 \mod 6 = 3$. This should **not** be confused with the operation from previous courses, $3^3 = 3 \cdot 3 \cdot 3 = 27$.

Definition 1.56. ⟨ *adjective, group* ⟩
A group G is **cyclic**[a] if there exists an $a \in G$ such that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. If the powers a^n are all distinct then G is the **infinite cyclic group**. If $|G| = m$, then G is the **cyclic group of order** m.

[a] All cyclic groups are abelian.

Below is list of examples and nonexamples of cyclic groups.

- Consider the group $\mathbb{Z}$ under addition. Note,

$$\begin{aligned}\mathbb{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3\ldots\} \\ &= \{\ldots, 1^{-3}, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, 1^3\ldots\} \\ &= \langle 1 \rangle.\end{aligned}$$

  Thus $\mathbb{Z}$ is cyclic group. Additionally, each power of 1 is distinct so $\mathbb{Z}$ is an infinite cyclic group.

- Consider the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4. Note $\mathbb{Z}_4 = \{0, 1, 2, 3\} = \{1^0, 1^1, 1^2, 1^3\}$. Note not all powers or 1 are unique ($1^5 = 1^1$). The order of $\mathbb{Z}_4$ is 4, so $\mathbb{Z}_4$ is a finite cyclic group.

- Consider the group D_4 as described above. The group D_4 is **not** a cyclic group. There is no element whose powers generate[5] D_4.

Similar to how rings can have subrings, groups can have subgroups. We will provide a formal definition below.

Definition 1.57. ⟨ *adjective, group* ⟩
A nonempty subset U of a group G is called a **subgroup** of G if, for all $a, b \in G$

1. $a, b \in U \implies ab^{-1} \in U$.

Equivalently,

1. $a, b \in U \implies ab \in U$,
2. $a \in U \implies a^{-1} \in U$.

Example. Consider the group D_4 as defined above, and let $U \coloneqq \{ R_0, R_{90}, R_{180}, R_{270}\}$. We will list the inverse of each element, $R_0^{-1} = R_0$, $R_{90}^{-1} = R_{270}$, $R_{180}^{-1} = R_{180}$, and $R_{270}^{-1} = R_{90}$. It can be seen from Figure 1.4 that this subset is closed. Thus U is a subgroup of G.

It should be noted associativity, and the property of the identity element are inherited from the larger group G. While we haven't yet proved each subgroup contains the identity element, this result is easy to obtain. We will state this below.

[5] Definition 1.59.

Theorem 1.58. All Subgroups Contain the Identity Element:
Let U be a subgroup of a group G. Then the identity element e from G is an element of U.

Proof. Let U be a subgroup of a group G, and let $a \in U$. By the definition of a subgroup $aa^{-1} = e \in U$. Thus all subgroups contain the identity element.

□

Definition 1.59. ⟨ *noun, group* ⟩
For each a in a group G, the set $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, is a subgroup called the **cyclic subgroup generated by** a.

We will list a few examples of cyclic subgroups below.

- Consider the group $\mathbb{Z}$. Note, the subgroup $\langle 5 \rangle = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$ is a subgroup of $\mathbb{Z}$. It is called the cyclic subgroup generated by 5.
- Consider the group D_4 and the subgroup $U \coloneqq \{ R_0, R_{90}, R_{180}, R_{270}\}$. We can see that $U = \langle R_{90} \rangle$. Thus $\langle R_{90} \rangle$ is the cyclic subgroup generated by R_{90}.
- Consider the group D_4. A smaller subgroup of D_4 is the subgroup $\langle V \rangle = \{R_0, V\}$. Then $\langle V \rangle$ is the cyclic subgroup generated by V.

Definition 1.60. ⟨ *noun, integer* ⟩
Let G be a group and let $a \in G$. The order of the cyclic subgroup generated by a is called the **order of the element** a. It is the smallest positive integer n such that $a^n = e$, and is denoted $o(a)$.

Example. Consider the group D_4. Note, using the work from above we know $|\langle R_{90} \rangle| = 4$, thus the order of R_{90} is $o(R_{90}) = 4$. The order of V is $o(V) = 2$.

Definition 1.61. ⟨ *noun, integer* ⟩
Let U be a subgroup of a group G and let $a \in G$. The subset $Ua \coloneqq \{ua : u \in U\}$ is called the **left coset** of U. Symmetrically, the subset $aU \coloneqq \{au : u \in U\}$ is called the **right coset** of U.

Example. Consider the group D_4 with subgroup $U \coloneqq \{R_0, R_{90}, R_{180}, R_{270}\}$. The left coset $UR_{90} = \{(R_0R_{90}), (R_{90}R_{90}), (R_{180}R_{90}), (R_{270}R_{90})\} = \{R_{90}, R_{180}, R_{270}, R_0\}$. The left coset

$UD = \{(R_0D), (R_{90}D), (R_{180}D), (R_{270}D)\} = \{D, H, D', V\}$. It should be noted that left (and right) cosest need not be groups. We have already shown that $U = UR_{90}$ is a group, but it is clear UD is not a group, as it has no identity element.

Theorem 1.62. Equality of Cosets:[a]
Let U be a subgroup of a group G and let $a \in G$. Then $Ua = U$ if and only if $a \in U$.

[a]Theorem from [2].

Proof. Let U be a subgroup of a group G and let $a \in G$. We will show $Ua = U$ if and only if $a \in U$. First suppose $Ua = U$. Note, $e \in U$, thus $ea = a \in Ua$, and since $Ua = U$, $a \in U$. Now suppose $a \in U$. The inclusion $Ua \subseteq U$ is a direct result of the closure of U. Let $b \in U$. Note $(ba^{-1}) \in U$, therefore $(ba^{-1})a = b(a^{-1}a) = be = b \in Ua$. So, $U \subseteq Ua$, and thus $Ua = U$. Therefore, $Ua = U$ if and only if $a \in U$. □

Example. We have already seen $UR_{90} = U$ and $UD \neq U$. We will provide a few more examples of this within D_4. Note, $UR_{180} = \{R_{180}, R_{270}, R_0, R_{90}\} = U$, but $UH = \{H, D', V, D\} \neq U$. Now consider the subgroup $S \coloneqq \{R_0, V\}$. Note, the left coset $SV = \{V, 0\} = S$, but $SR_{270} = \{R_{270}, D\} \neq S$.

Theorem 1.63. Equality of Cosets:
Let U be a subgroup of a group G and let $a, b \in G$. Then $Ua = Ub$ if and only if $ab^{-}1 \in U$.

Proof. Let U be a subgroup of a group G and let $a, b \in G$. We will show $Ua = Ub$ if and only if $ab^{-}1 \in U$. Suppose $Ua = Ub$. Note, $a \in Ua$ so $a \in Ub$ and there exists $u \in U$ such that $a = ub$. Therefore $u = ab^{-1} \in U$. Now suppose $ab^{-1} \in U$. Since U is a group $(ab^{-1})^{-1} = ba^{-1} \in U$. Let $ua \in Ua$. Note, $ua = u(ab^{-1})(ba^{-1})a = (uab^{-1})b \in Ub$ since $u(ab^{-1}) \in U$. Thus $Ua \subseteq Ub$. Symmetrically, for $vb \in Ub$, $vb = v(ba^{-1})(ab^{-1})b = (vba^{-1})a \in Ua$. Thus $Ub \subseteq Ua$ and $Ua = Ub$. Therefore, $Ua = Ub$ if and only if $ab^{-1} \in U$. □

Example. Consider the set D_4 with subgroup $U \coloneqq \{R_0, R_{180}, H, V\}$. Now consider the left cosets UD and UD'. Note, $D'^{-1} = D'$ and $DD' = R_{180} \in U$. We can see $UD = \{R_0D, R_{180}D, HD, VD\} = \{D, D', R_{90}, R_{270}\} = \{R_{180}D', R_0D', VD', HD'\} = UD'$.

Definition 1.64. ⟨ *noun, division of a set* ⟩
Let S be a nonempty set. A set of distinct disjoints subsets $S_1, S_2, \ldots, S_n$ of S are a **partition** of S if for each $s \in S$, s belongs to exactly one of $S_1, S_2, \ldots, S_n$.

Example. Consider the set $\mathbb{Z}$, and the subsets $S_1 \coloneqq \{2k+1 : k \in \mathbb{Z}\}$ and $S_2 \coloneqq \{2k : k \in \mathbb{Z}\}$. The two sets form are disjoint, and each element of $\mathbb{Z}$ is in one of S_1 and S_2. Therefore, S_1 and S_2 form a partition of $\mathbb{Z}$.

Theorem 1.65.
Let U be a subgroup of a group G. The distinct left cosets of U form a partition of G.

Proof. Let U be a subgroup of a group G. We will show the distinct left cosets of U form a partition of G. First we will show each element of G is contained in a left coset of U. Let $g \in G$. Note, $eg = g \in Ug$, thus each element of G is contained in a left coset. Now we will show each element of G is in only one left coset. Let $g \in G$ and suppose $g \in Ua$ and $g \in Ub$ for some $a, b \in G$. Note, for some $u, v \in U$, $g = ua = vb$ which implies $uab^{-1} = v$ so $uab^{-1} \in U$. Since $u \in U$ we know $u^{-1} \in U$, therefore $u^{-1}uab^{-1} = eab^{-1} = ab^{-1} \in U$. Thus, by Theorem 1.63, $Ua = Ub$. Therefore each element of G is contained in exactly one left coset of U, hence the distinct left cosets of U form a partition of G. □

Example. Consider the group $\mathbb{Z}_6$ with subgroup $U \coloneqq \{0, 2, 4\}$. Note, the distinct left cosets of U are $U = U0 = U2 = U4 = \{2, 4, 0\}$ and $U1 = U3 = U5 = \{1, 3, 5\}$.

Theorem 1.66. Lagrange's Theorem:
Let U be a subgroup of a finite group G. Then $|U|$ divides $|G|$.

Proof. Let U be a subgroup of a finite group G. We will show $|U| = n$ divides the order of G. We will show for all $a \in G$, $|U| = |Ua|$. Let $a \in G$. Note, $Ua = \{ua : u \in U\}$ so $|Ua| \leq |U|$ by definition. Now suppose by way of contradiction $|Ua| < |U|$. So, there exists $u, v \in U$ with $u \neq v$ such that $ua = va$. But this implies $u = v$, which is a contradiction (could also say if $ua = va$ then $u = v$ so each ua is unique). Thus $|Ua| \geq |U|$, and therefore $|Ua| = |U|$ for all $a \in G$. Since the distinct left cosets of U form a partition of G there can only be finitely many of them, say m. So, each left coset has n elements and there are m cosets, thus G has nm elements, so $|U|$ divides $|G|$. □

Example. Consider the group D_4. We have previously seen the subgroups $U_1 = \{R_0, R_{90}, R_{180}, R_{270}\}$, $U_2 = \{R_0, R_{180}, H, V\}$, and $U_3 = \{R_0, V\}$. These subgroups have order

4, 4, and 2, respectively, all of which divide 8. Note, 3 does not divide 8 and there is no subgroup of order 3.

Corollary 1.67.
For all a in a finite group G, the order of a divides the order of G.

Proof. Let G be a finite group and let $a \in G$. Note, $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem 1.66 the order of $\langle a \rangle$ divides the order of G. Thus, the order of a divides the order of G. □

Example. Consider the group $\mathbb{Z}_6$. Note, $2^3 = 0$ so $|2| = 3$ and $3 \mid 6$. Also, $5^6 = 0$ so $|5| = 6$ and $6 \mid 6$.

Definition 1.68. ⟨ *noun, integer* ⟩
Let G be a group and let U be a subgroup. The **index** of U is the number of distinct left (or right) cosets of U.

Example. Consider the group D_4 and subgroup $U \coloneqq \{R_0, R_{90}, R_{180}, R_{270}\}$. There are two distinct left cosets of U, namely $UR_0 = UR_{90} = UR_{180} = UR_{270} = \{R_0, R_{90}, R_{180}, R_{270}\}$ and $UH = UV = UD = UD' = \{H, V, D, D'\}$. Thus the index of U is 2.

Definition 1.69. ⟨ *adjective, group* ⟩
Let G be a group and let U be a subgroup. If $Ua = aU$ for all $a \in G$ then we say U is a **normal** subgroup of G, and write $U \lhd G$. Equivalently, U is normal if for all $a \in G$, $a^{-1}Ua = U$.

Example. Consider the group D_4 and subgroup $U \coloneqq \{R_0, R_{90}, R_{180}, R_{270}\}$. It can be verified that $R_0U = UR_{90}U = R_{180}U = R_{270}U = UR_0 = UR_{90} = UR_{180} = UR_{270} = \{R_0, R_{90}, R_{180}, R_{270}\}$ and $HU = VU = DU = D'U = UH = UV = UD = UD' = \{H, V, D, D'\}$. Therefore, U is a normal subgroup of D_4.

Notice the property of normalcy is similar to commutativity. It says for $a \in G$ and $u \in U$, there exists $v \in U$ such that $au = va$ (and vice versa). It is clear that all subgroups of an abelian group are normal, as for $a \in G$, $u \in U$, $au = ua$.

Definition 1.70. ⟨ *noun, group* ⟩
Let U be a normal subgroup of a group G. The **quotient group**, or the **factor group**, of G by U is the set

$$G/U \coloneqq \{Ua : a \in G\},$$

with multiplication defined by

$$(Ua)(Ub) = U(ab).$$

Example. As we have seen before, $U = \{R_0, R_{90}, R_{180}, R_{270}\} \lhd D_4$. Thus, the quotient group $D_4/U = \{UR_0, UH\}$. Note D_4/U is easily verified to be a group. We can see $(UH)(UH) = U(HH) = UR_0$, and $(UH)(UR_0) = (UR_0)(UH) = UH$.

Definition 1.71. ⟨ *noun, function* ⟩
Let G and H be groups with identity elements e_G and e_H, respectively. The function $\varphi : G \to H$ is called a **homomorphism** if for all $a, b \in G$,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Theorem 1.72.
For any homomorphism $\varphi : G \to H$,

$$\varphi(e_G) = e_H.$$

Proof. Let G and H be groups with identity elements e_G and e_H, respectively. Let $\varphi : G \to H$ be a homomorphism, and let $a \in G$. Note, $e_H\varphi(a) = \varphi(a) = \varphi(e_G a) = \varphi(e_G)\varphi(a)$, thus $\varphi(e_G) = e_H$. □

Definition 1.73. ⟨ *noun, function* ⟩
Let N be a normal subgroup of a group G. The mapping $\nu_N : G \to G/N$ defined by

$$\nu_N(a) = Na$$

for $a \in G$ is a homomorphism called the **natural homomorphism** onto G/N.

Definition 1.74. ⟨ *noun, function* ⟩
If a homomorphism $\varphi : G \to H$ is bijective, we say that it is an **isomorphism**. In such a case $\varphi^{-1} : H \to G$ is also an isomorphism, and we say that H is **isomorphic** to G, writing $H \simeq G$.

Definition 1.75. ⟨ *noun, set* ⟩
If a homomorphism $\varphi : G \to H$ is surjective, but is not necessarily injective, we say that H is a **homomorphic image** of G.

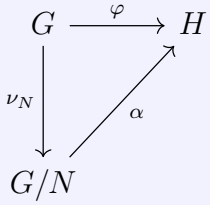
Definition 1.76. ⟨ *noun, set* ⟩
The **kernel** $\ker\varphi$ of a homomorphism $\varphi : G \to H$ is defined by

$$\ker\varphi \coloneqq \varphi^{-1}(e_H) = \{a \in G : \varphi(a) = e_H\}.$$

Theorem 1.77.
For any homomorphism $\varphi : G \to H$, the kernel is a normal subgroup of G.

Proof. Let $\varphi : G \to H$ be a homomorphism and let $a, b \in \ker\varphi$. Note, $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)(\varphi(b))^{-1} = e_H e_H^{-1} = e_H$, thus $ab^{-1} \in \ker\varphi$ and $\ker\varphi$ is a subgroup of G. Now let $a \in G$, $u \in \ker\varphi$. Note $\varphi(a^{-1}ua) = \varphi(a^{-1})\varphi(u)\varphi(a) = \varphi(a)^{-1}e_H\varphi(a) = \varphi(a)^{-1}\varphi(a) = e_H$. Therefore, for all $a \in G$ and $u \in \ker\varphi$, $a^{-1}ua \in \ker\varphi$ thus $a^{-1}\ker\varphi a = \ker\varphi$. Hence, $\ker\varphi$ is a normal subgroup of G. □

Theorem 1.78.
Let G, H be groups, and let φ be a homomorphism from G onto H, with kernel N. There exists a unique isomorphism $\alpha : G/N \to H$ such that the diagram



commutes.

Exercises

1.1 Let R be a ring.

(i) Show that, for all $a \in R$,

$$a0 = 0a = 0.$$

Proof. Let $a \in R$. Note, $a(0) = a(0+0) = a0 + a0$, therefore $0 = a0 - a0 = a0 + a0 - a0 = a0$. Symmetrically, $(0+0)a = 0a + 0a$ and therefore $0 = 0a - 0a = 0a + 0a - 0a = 0a$. So, for all $a \in R$, $a0 = 0a = 0$. □

(ii) Show that, for all $a, b \in R$,

$$a(-b) = (-a)b = -ab, \quad (-a)(-b) = ab.$$

Proof. Let $a, b \in R$. Note, $ab + a(-b) = a(b-b) = a0 = 0$ so $a(-b) = -ab$. Symmetrically, $(-a)b + ab = (-a+a)b = 0b = 0$ so $(-a)b = -ab$. Note, $-ab + (-a)(-b) = a(-b) + (-a)(-b) = (a-a)(-b) = 0(-b) = 0$ so $(-a)(-b) = ab$. □

1.2 What difference does it make if the stipulation that $1 \neq 0$ is omitted from Axiom (R8)?

If $1 \neq 0$ is omitted from Axiom (R8) it would allow for rings with one element, and any ring with $1 = 0$ would have only one element, 0.

Proof. Let R be a ring and suppose there exist a $1 = 0$ in R such that for all $a \in R$, $1a = a1 = a$. So, let $b \in R$. Note $b = 1b = 0b = 0$, therefore the only element in R is 0. □

1.3 Axiom (R8) ensures that a field has at least two elements. Show that there exists a field with exactly two elements.

Proof. Let $R = \{0, 1\}$ with addition modulo 2 and the usual multiplication rule from the field of real numbers. The rules (R1), (R2), (R5), (R7) and (R9) are the rules of modular addition and multiplication so the only rules left to verify are (R3), (R4), (R6), (R8), and (R10). The rule (R3) is true because 0 is an element of R. The rule (R4) can be verified by noting $0 + 0 = 0$ and $1 + 1 = 0$. The rule (R6) can be verified as done below

$$1(1+1) = 1(0) = 1(0+0) = 0 = 1 \cdot 0 + 1 \cdot 0 = 1 \cdot 1 + 1 \cdot 1,$$

$$1(1+0) = 1(0+1) = 1\cdot 0 + 1\cdot 1 = 1\cdot 1 + 1\cdot 0 = 0, \text{ and}$$

$$0(a+b) = 0a + 0b = 0, \forall a, b \in R.$$

It can be verified all cases are covered and the rule $(a+b)c = ac + bc$ is true because of commutativity. The rule (R8) is true because $1 \in R$ and $1 \cdot 1 = 1$, and $1 \cdot 0 = 0$. The finally rule (R10) is true because for all $a \in R$ with $a \neq 0$, there exists an $a^{-1} \in R$ such that $aa^{-1} = 1 \cdot 1 = 1$. Therefore R is a field. □

1.4 Prove the equivalence of (R9) and (R9)′.

Proof. To prove the equivalence of (R9) and (R9)′ we show they imply each other. Let R be a ring be a commutative ring with unity. Suppose for all $a, b, c \in R$ with $c \neq 0$, $ca = cb \implies a = b$. Let $a, b \in R$ with $ab = 0$. Note, $ab = 0 = a0$ implies $b = 0$, or $ba = ab = 0 = b0$ implies $a = 0$. Therefore, (R9) implies (R9)′. Now suppose for all $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$. Let $a, b, c \in R$ with $c \neq 0$ and $ca = cb$. Note $c(a + (-b)) = ca + c(-b) = cb + c(-b) = 0$ so $a + (-b) = 0$ and therefore $a = b$. Hence (R9)′ implies (R9), and the two are equivalent. □

1.5 Show that every finite integral domain is a field.

Proof. Let D be a finite integral domain and let $a \in D\backslash\{0\}$. If $a = 1$ then $aa = 1(1) = 1$ and we are done. If $a \neq 1$ then consider the elements $a, a^2, a^3, \ldots$. Since D is finite there must be two elements in this list that are equal, say a^i and a^j. Without loss of generality say $i > j$. Note, $a^i = a^j \implies a^j a^{i-j} = a^j 1 = \implies a^{i-j} = 1$. Therefore, the inverse of a is a^{i-j-1} because $aa^{i-j-1} = a^{i-j} = 1$. Thus, all nonzero elements of D have inverses, so D is a field. □

1.6 Show that $\sim$, as defined in the text, is an equivalence relation. That is, show that, for all a, b, c in a commutative ring R with unity,

(i) $a \sim a$ (the reflexive property);

Proof. Let R be a commutative ring with unity, let U be the group of units of R, and let $a \in R$. Note, $a = 1a$ so $a \sim a$ since $1 \in U$ by the definition of 1. □

(ii) $a \sim b \implies b \sim a$ (the symmetric property);

Proof. Let R be a commutative ring with unity, let U be the group of units of R, and let $a, b \in R$ with $a \sim b$. There exists a $u \in U$ such that $a = ub$ and since $u \in U$ there exist a $v \in U$ such that $vu = 1$ so $a = ub \implies b = vub = va$ therefore $b \sim a$. □

(iii) $a \sim b$ and $b \sim c \implies a \sim c$ (the transitive property).

Proof. Let R be a commutative ring with unity, let U be the group of units of R, and let $a, b, c \in R$ with $a \sim b$ and $b \sim c$. There exist $u, v \in U$ such that $a = ub$ and $b = vc$. Note, $a = ub = uvc = (uv)c$ and since U is a group $uv \in U$ so $a \sim c$. □

1.7 Let $i = \sqrt{-1}$. Show that, by contrast with Example 1.2, the ring $R = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$ has group of units $\{1, -1\}$.

Proof. Let $R = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$. Let $a, b \in R$ with $ab = 1$. Note multiplication is commutative because complex multiplication is commutative. Note,

$$\begin{aligned} 1 &= ab \\ &= (a_1 + a_2 i\sqrt{2})(b_1 + b_2 i\sqrt{2}) \\ &= (a_1 + a_2 i\sqrt{2})(b_1 + b_2 i\sqrt{2})(a_1 - a_2 i\sqrt{2})(b_1 - b_2 i\sqrt{2}) \\ &= (a_1^2 + 2a_2^2)(b_1^2 + 2b_2^2). \end{aligned}$$

Since, $(a_1^2 + 2a_2^2)$ and $(b_1^2 + 2b_2^2)$ are both positive integers $(a_1^2 + 2a_2^2)(b_1^2 + 2b_2^2) = 1$ only holds if $a = (a_1^2 + 2a_2^2) = 1$ and $b = (b_1^2 + 2b_2^2) = 1$ which implies a and b equal 1 or -1. So, the group of units of R is $\{1, -1\}$. □

1.8 Let D be an integral domain. Show that, for all $a, b \in D\backslash\{0\}$:

(i) $a|a$ (the reflexive property);

Proof. Let $a \in D\backslash\{0\}$. Note, $a = 1a$ so $a|a$. □

(ii) $a|b$ and $b|c \implies a|c$ (the transitive property);

Proof. Let $a, b, c \in D\backslash\{0\}$. Note, there exist $z, x \in D$ such that $az = b$ and $bx = c$, so $a(zx) = (az)x = bx = c$ and therefore $a|c$. □

(iii) $a|b$ and $b|a \implies a \sim b$.

Proof. Let $a, b \in D\backslash\{0\}$ with $a|b$ and $b|a$. There exist $z, x \in D$ such that $az = b$ and $bx = a$. Note, $az = b \implies bxz = b \implies xz = 1$ so x, z are units. □

1.9 Let a be an element of a ring R. Show that $a + a = a$ implies $a = 0$.

Proof. Let R be a ring and let $a \in \mathbb{R}$ with $a+a = a$. Note, $0 = a+(-a) = a+a+(-a) = a + (a + (-a)) = a + 0 = a$. Therefore, if $a + a = a$ then $a = 0$. □

1.10 Show that the two definitions of a subring are equivalent.

Proof. Let R be a ring and U be a nonempty subset of R. We will show the equivalence of both conditions for a subring as defined in definition 1.16, namely,

$$\text{if } a, b \in U \text{ then } a - b, ab \in U$$

and

$$\text{if } a, b \in U \text{ then } a + b, ab \in U,$$

$$\text{if } a \in U \text{ then } -a \in U.$$

Assume the first condition, if $a, b \in U$ then $a - b, ab \in U$. Note, $0 \in U$ so $0 - 0 \in U$, therefore for $a \in U$, $0 - a = -a \in U$. Now let $a, -b \in U$. Note, $a - (-b) = a + b \in U$, and $ab \in U$ by assumption. Therefore, condition one implies condition two.

Now assume the second condition, if $a, b \in U$ then $a + b, ab \in U$, and if $a \in U$ then $-a \in U$. Let $a, b \in U$. Note $ab \in U$ by assumption. Note $-b \in U$, so $a + (-b) = a - b \in U$. Therefore condition two implies condition one.

Hence, the conditions are equivalent. □

1.11 Show that the definition 1.16 is equivalent to the definition of a subring U of a ring R as a subset of R which is a ring with respsect to the operations $+$ and $\cdot$ of R.

Proof. Let R be a ring and let U be a nonempty subset of R with the same operations as R and assume if $a, b \in U$ then $a - b, ab \in U$. We will show that a subset with these properties is a ring. First note associativity of addition, commutativity of addition, associativity of multiplication, and the distributive laws are inherited from R. All that is left to be shown is that $0 \in U$, the existence of negative, and closure of multiplication and addition.

Since U is nonempty, there exists some $a \in U$. Note $a - a = 0 \in U$, so 0 exists. Now let $a \in U$, note $0 - a = -a \in U$ so negatives exists. It can be noted that multiplication is closed by assumption. Now let $a, b \in U$. Since negatives exists, $-b \in U$, therefore $a - (-b) = a + b \in U$ and addition is closed. Hence U is a ring. □

1.12 Show that definition 1.17 is equivalent to the definition of a subfield as a subring which is a field.

Proof. We will show that definition 1.17 is equivalent to the definition of a subfield as a subring which is a field. Let K be a field and let E be a subring of K with the following properties:

(a) if $a, b \in E$ then $a - b \in E$,

(b) if $a, b \in E$ then $ab \in E$,

(c) if $a \in E \backslash \{0\}$ then $a^{-1} \in E$.

We know from E being a subring, and a subset of a field, that E has associativity of addition and multiplication, commutativity of addition and multiplication, the distributive property, the existence of negatives, and the existence of 0. Additionally, E has multiplicative inverses by assumption. Thus all we have left to show is the existence of 1. Let $a \in E \backslash \{0\}$, the element $a^{-1} \in E$. Therefore, $aa^{-1} = 1 \in E$. Thus, 1 exists, and E is a field. The properties (a), (b), (c) are implied by E is a field, therefore the two definitions described above are equivalent. □

1.13 Show that a commutative ring with unity having no proper ideals is a field.

Proof. Let R be a commutative ring with unity and no proper ideals. Let $a \in R$ with $a \neq 0$. Note, the ideal $\langle a \rangle = R$, so $1 \in \langle a \rangle$. Therefore there exists some $b \in R$ such that $ab = 1$, meaning a has an inverse. Therefore, if R is a commutative ring with unity and no proper ideals then R is a field. □

1.14 Show that $\mathbb{Q}(i\sqrt{3}) = \{a + bi\sqrt{3} : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.

Proof. Let $\mathbb{Q}(i\sqrt{3}) \coloneqq \{a + bi\sqrt{3} : a, b \in \mathbb{Q}\}$. Let $a + bi\sqrt{3}, c + di\sqrt{3} \in \mathbb{Q}(i\sqrt{3})$. Note,

$$\begin{aligned} a + bi\sqrt{3} - (c + di\sqrt{3}) &= a + bi\sqrt{3} - c - di\sqrt{3} \\ &= (a - c) + (b - d)i\sqrt{3} \\ &\in \mathbb{Q}(i\sqrt{3}). \end{aligned}$$

Therefore $\mathbb{Q}(i\sqrt{3})$ is closed under subtraction. Note,

$$\begin{aligned} (a + bi\sqrt{3})(c + di\sqrt{3}) &= ac + bdi^2(\sqrt{3})^2 + adi\sqrt{3} + cbi\sqrt{3} \\ &= ac - 3bd + adi\sqrt{3} + cbi\sqrt{3} \\ &= (ac - 3bd) + (ad + cb)i\sqrt{3} \\ &\in \mathbb{Q}(i\sqrt{3}). \end{aligned}$$

Therefore $\mathbb{Q}(i\sqrt{3})$ is closed under multiplication.

Suppose $c + di\sqrt{3} \neq 0$. Note

$$\begin{aligned} (c + di\sqrt{3})\frac{1}{c + di\sqrt{3}} &= (c + di\sqrt{3})\Big(\frac{c}{c^2 + 3d^2} + \frac{-d}{c^2 + 3d^2}i\sqrt{3}\Big) \\ &= \frac{c^2}{c^2 + 3d^2} - \frac{cd}{c^2 + 3d^2}i\sqrt{3} + \frac{cd}{c^2 + 3d^2}i\sqrt{3} + \frac{3d^2}{c^2 + 3d^2} \\ &= \frac{c^2 + 3d^2}{c^2 + 3d^2} \\ &= 1. \end{aligned}$$

Since $\frac{c}{c^2+3d^2}$, and $\frac{-d}{c^2+3d^2}$ are rational numbers, $\frac{c}{c^2+3d^2} + \frac{-d}{c^2+3d^2}i\sqrt{3} = (c + di\sqrt{3})^{-1} \in \mathbb{Q}(i\sqrt{3})$ and inverses exist. Therefore, $\mathbb{Q}(i\sqrt{3})$ is a subfield of $\mathbb{C}$. □

1.15 (i) Show that the set

$$K \coloneqq \left\{ \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$$

is a field with respect to matrix addition and multiplication.

Proof. We will show the set

$$K \coloneqq \left\{ \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$$

is a field. We know matrix addition and multiplication are associative, and matrix

addition is commutative. It is clear to see the zero matrix and the identity matrix,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in K \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in K.$$

Let $A, C \in K$ where

$$A = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \text{ and } C = \begin{pmatrix} c & d \\ -3d & c \end{pmatrix}.$$

It is easy to see negatives exist as

$$-A = \begin{pmatrix} -a & -b \\ -3(-b) & -a \end{pmatrix} \in K.$$

We will now show the closure of addition and multiplication. Note,

$$A + C = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -3(b+d) & a+c \end{pmatrix} \in K,$$

$$AC = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} = \begin{pmatrix} ac-3bd & ad+bc \\ -3(ad+bc) & ac-3bd \end{pmatrix} \in K.$$

Thus addition and multiplication are closed. Next we will show the commutativity of multiplication in K. Note,

$$AC = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} = \begin{pmatrix} ac-3bd & ad+bc \\ -3bc-3ad & -3bd+ac \end{pmatrix},$$

$$CA = \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} = \begin{pmatrix} ac-3bd & ad+bc \\ -3bc-3ad & -3bd+ac \end{pmatrix} = AC.$$

Thus multiplication in K is commutative. We will now show the distributive property holds. Let $A, C, E \in K$ where

$$A = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix}, C = \begin{pmatrix} c & d \\ -3d & c \end{pmatrix}, \text{ and } E = \begin{pmatrix} e & f \\ -3f & e \end{pmatrix}.$$

Note,

$$\begin{aligned} E(A+C) &= \begin{pmatrix} e & f \\ -3f & e \end{pmatrix} \left[\begin{pmatrix} a & b \\ -3b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} \right] \\ &= \begin{pmatrix} e & f \\ -3f & e \end{pmatrix} \begin{pmatrix} a+c & b+d \\ -3(b+d) & a+c \end{pmatrix} \\ &= \begin{pmatrix} e(a+c)+-3f(b+d) & e(b+d)+f(a+c) \\ -3f(a+c)-3e(b+d) & -3f(b+d)+e(a+c) \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} EA+EC &= \begin{pmatrix} e & f \\ -3f & e \end{pmatrix} \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} + \begin{pmatrix} e & f \\ -3f & e \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} \\ &= \begin{pmatrix} ea-3fb & eb+fa \\ -3fa-3eb & -3fb+ea \end{pmatrix} + \begin{pmatrix} ec-3fd & ed+fc \\ -3fc-3ed & -3fd+ec \end{pmatrix} \\ &= \begin{pmatrix} e(a+c)+-3f(b+d) & e(b+d)+f(a+c) \\ -3f(a+c)-3e(b+d) & -3f(b+d)+e(a+c) \end{pmatrix} \\ &= E(A+C). \end{aligned}$$

Since we've shown multiplication is commutative, we know $(A+C)E = AE+CE$. Therefore, the distributive property holds. Finally we will show multiplicative inverses exist. Let A be as defined previously, and suppose $A \neq 0$. From a well known formula for the inverse of 2×2 matrices,

$$A^{-1} = \frac{1}{a^2+3b^2} \begin{pmatrix} a & -b \\ 3b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+3b^2} & \frac{-b}{a^2+3b^2} \\ -3\frac{-b}{a^2+3b^2} & \frac{a}{a^2+3b^2} \end{pmatrix}.$$

Since $a^2+3b^2 \neq 0$ and each entry is a rational number, we know $A^{-1} \in K$. Since addition and multiplication are closed, associative, and commutative in K, and the zero matrix and identity matrix are in K, and both additive and multiplicative inverses exists, we can conclude that K is a field. □

(ii) Show that K is isomorphic to the field $\mathbb{Q}(i\sqrt{3})$ defined in the previous exercise.

Proof. We will show that K is isomorphic to $\mathbb{Q}(i\sqrt{3}) \coloneqq \{a+bi\sqrt{3} : a,b \in \mathbb{Q}\}$.

Consider the function $\varphi : K \to \mathbb{Q}(i\sqrt{3})$ defined by

$$\varphi(a + bi\sqrt{3}) = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix}.$$

First we will show φ is a homomorphism. Let $a + bi\sqrt{3}, c + di\sqrt{3} \in K$. Note,

$$\begin{aligned} \varphi((a + bi\sqrt{3}) + (c + di\sqrt{3})) &= \varphi((a + c) + (b + d)i\sqrt{3}) \\ &= \begin{pmatrix} a + c & b + d \\ -3(b + d) & a + c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} \\ &= \varphi(a + bi\sqrt{3}) + \varphi(c + di\sqrt{3}), \end{aligned}$$

and

$$\begin{aligned} \varphi((a + bi\sqrt{3})(c + di\sqrt{3})) &= \varphi((ac - 3bd) + (ad + bc)i\sqrt{3}) \\ &= \begin{pmatrix} ac - 3bd & ad + bc \\ -3(ad + bc) & ac - 3bd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \begin{pmatrix} c & d \\ -3d & c \end{pmatrix}, \end{aligned}$$

thus φ preserves addition and multiplication and is therefore a homomorphism. Now suppose $a + bi\sqrt{3} \neq c + di\sqrt{3}$. Note,

$$\varphi(a + bi\sqrt{3}) = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \neq \begin{pmatrix} c & d \\ -3d & c \end{pmatrix} = \varphi(c + di\sqrt{3}).$$

So, φ is injective. Let

$$A = \begin{pmatrix} a & b \\ -3b & a \end{pmatrix} \in K.$$

Note, $\varphi(a + bi\sqrt{3}) = A$, so φ is surjective. Therefore, φ is an isomorphism, and K is isomorphic to $\mathbb{Q}(i\sqrt{3})$ as desired. □

1.16 Show that the set $\mathbb{R}(i\sqrt{3}) \coloneqq \{a + bi\sqrt{3} : a, b \in \mathbb{R}\}$ is a subfield of $\mathbb{C}$. Is it true that $\mathbb{R}(\sqrt{3}) \coloneqq \{a + b\sqrt{3} : a, b \in \mathbb{R}\}$ is a subfield of $\mathbb{R}$?

Proof. Let $\mathbb{R}(i\sqrt{3}) \coloneqq \{a + bi\sqrt{3} : a, b \in \mathbb{R}\}$. Let $a + bi\sqrt{3}, c + di\sqrt{3} \in \mathbb{R}(i\sqrt{3})$. Note,

$$\begin{aligned} a + bi\sqrt{3} - (c + di\sqrt{3}) &= a + bi\sqrt{3} - c - di\sqrt{3} \\ &= (a - c) + (b - d)i\sqrt{3} \\ &\in \mathbb{R}(i\sqrt{3}). \end{aligned}$$

Therefore $\mathbb{R}(i\sqrt{3})$ is closed under subtraction. Note,

$$\begin{aligned} (a + bi\sqrt{3})(c + di\sqrt{3}) &= ac + bdi^2(\sqrt{3})^2 + adi\sqrt{3} + cbi\sqrt{3} \\ &= ac - 3bd + adi\sqrt{3} + cbi\sqrt{3} \\ &= (ac - 3bd) + (ad + cb)i\sqrt{3} \\ &\in \mathbb{R}(i\sqrt{3}). \end{aligned}$$

Therefore $\mathbb{R}(i\sqrt{3})$ is closed under multiplication.

Suppose $c + di\sqrt{3} \neq 0$. Note

$$\begin{aligned} (c + di\sqrt{3})\frac{1}{c + di\sqrt{3}} &= (c + di\sqrt{3})\Big(\frac{c}{c^2 + 3d^2} + \frac{-d}{c^2 + 3d^2}i\sqrt{3}\Big) \\ &= \frac{c^2}{c^2 + 3d^2} - \frac{cd}{c^2 + 3d^2}i\sqrt{3} + \frac{cd}{c^2 + 3d^2}i\sqrt{3} + \frac{3d^2}{c^2 + 3d^2} \\ &= \frac{c^2 + 3d^2}{c^2 + 3d^2} \\ &= 1. \end{aligned}$$

Since $\frac{c}{c^2+3d^2}$, and $\frac{-d}{c^2+3d^2}$ are real numbers, $\frac{c}{c^2+3d^2} + \frac{-d}{c^2+3d^2}i\sqrt{3} = (c + di\sqrt{3})^{-1} \in \mathbb{R}(i\sqrt{3})$ and inverses exist. Therefore, $\mathbb{R}(i\sqrt{3})$ is a subfield of $\mathbb{C}$. □

The set $\mathbb{R}(\sqrt{3})$ is a field because it is equal to $\mathbb{R}$. Any number y in $\mathbb{R}$ can be rewritten as $0 + x\sqrt{3}$ where $x = y/\sqrt{3}$.

1.17 Let $\varphi : K \to L$ be a nonzero homomorphism, where K and L are fields. Show that φ is a monomorphism.

Proof. Let $\varphi : K \to L$ be a nonzero homomorphism, where K and L are fields. We will show φ is a monomorphism. Since the kernel of a homomorphism is an ideal and K is a field the $\ker\varphi$ must be either $\{0\}$ or K, but since φ is nonzero, $\ker\varphi = \{0\}$. Let $a, b \in K$ with $a \neq b$. Note, $a - b \neq 0$, so $\varphi(a - b) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b) \neq 0$ meaning $\varphi(a) \neq \varphi(b)$. Hence φ is a monomorphism. □

1.18 Let $\varphi : R \to S$ be a nonzero homomorphism, where R, S are commutative rings with unity, with unity elements $1_R, 1_S$, respectively. If R and S are integral domains, show that $\varphi(1_R) = 1_S$. Show by an example that this need not hold if the integral domain condition is dropped.

Proof. Let $\varphi : R \to S$ be a nonzero homomorphism, where R, S are commutative rings with unity, with unity elements $1_R, 1_S$, respectively. Assume R and S are integral domains. Let $a \in R$ with $a \neq 0$. Note, $\varphi(a)1_S = \varphi(a1_R) \implies \varphi(a)1_S = \varphi(a)\varphi(1_R)$ and since S is an integral domain, we know $1_S = \varphi(1_R)$. □

Consider the commutative ring with unity $\mathbb{Q}$ and the commutative ring with unity element I_2 defined by

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Let $\varphi : \mathbb{Q} \to S$ be defined by

$$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

It is clear to see $\varphi(1) \neq I_2$.

1.19 Verify the associativity of addition in $Q(D)$.

Proof. We will show addition is associative in $Q(D)$. Let $a/b, c/d, e/f \in Q(D)$. Note,

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + cb}{bd} + \frac{e}{f} = \frac{adf + cbf + bde}{bdf},$$

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + cbf + bde}{bdf}.$$

Thus

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right),$$

and addition is associative. □

1.20 What happens to the construction of $Q(D)$ if D is a field?
If D is a field then φ is surjective as well as injective, thus φ is an isomorphism and $D \simeq Q(D)$.

Proof. Let $\varphi : D \to Q(D)$ be the monomorphism defined in Theorem 1.40. Let $a/b \in Q(D)$. Note, $a/b = (a/1)(1/b) = (a/1)(b/1)^{-1} = \varphi(ab^{-1})$, and $ab^{-1} \in D$. Therefore, φ is surjective, and φ is a isomorphism. □

1.21 Determine the characteristic of the ring $\mathbb{Z}_6$ of integers mod 6, and show that, in $\mathbb{Z}_6$,

$$a^2 = 0 \implies a = 0.$$

Note, $6 \cdot 1 = 0$ and 6 is the minimum natural number for which this holds, thus $\mathsf{char}\mathbb{Z}_6 = 6$.

Proof. We will show that in $\mathbb{Z}_6$,

$$a^2 = 0 \implies a = 0.$$

Let $a \in \mathbb{Z}_6$ and suppose that $a^2 = 0$. Thus, $6 \mid a^2$. Therefore, $6 \mid a$ which implies $2 \mid a$ and $3 \mid a$, but no nonzero integer in this set satisfies this property. Thus, $a = 0$. □

1.22 Write down the multiplication table for $\mathbb{Z}_7$, and list the inverses of all the non-zero elements.

The multiplication table is shown below.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The inverses of nonzero elements are listed as follows $1 : 1$, $2 : 4$, $3 : 5$, $4 : 2$, $5 : 3$, $6 : 6$.

1.23 Prove, by induction on n, that the **binomial theorem**,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r,$$

is valid in a commutative ring R with unity.

Proof. Let R be a commutative ring R with unity. We will prove the binomial theorem using induction. Let $a, b \in R$. Note,

$$(a+b)^1 = a+b = \binom{1}{0}a^1b^0 + \binom{1}{1}a^0b^1 = \sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r.$$

So the base case holds. Now suppose the equation holds for some $k \in \mathbb{N}$. In showing the bridge case holds, we will use the well known formula $\binom{m}{r} + \binom{m}{r-1} = \binom{m+1}{r}$. Note,

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)(a+b)^k \\
&= (a+b)\sum_{r=0}^{k}\binom{k}{r}a^{k-r}b^r \\
&= \sum_{r=0}^{k}\binom{k}{r}a^{k-r+1}b^r + \sum_{r=0}^{k}\binom{k}{r}a^{k-r}b^{r+1} \\
&= \sum_{r=0}^{k}\binom{k}{r}a^{k+1-r}b^r + \sum_{r=1}^{k+1}\binom{k}{r-1}a^{k+1-r}b^r \\
&= \binom{k}{0}a^{k+1} + \binom{k}{k}b^{k+1} + \sum_{r=1}^{k}\binom{k}{r}a^{k+1-r}b^r + \sum_{r=1}^{k}\binom{k}{r-1}a^{k+1-r}b^r \\
&= \binom{k}{0}a^{k+1} + \binom{k}{k}b^{k+1} + \sum_{r=1}^{k}\binom{k+1}{r}a^{k+1-r}b^r \\
&= \sum_{r=0}^{k+1}\binom{k+1}{r}a^{k+1-r}b^r.
\end{aligned}$$

Thus, the bridge case holds. Therefore, if R is a commutative ring with unity and $a, b \in R$, then

$$(a+b)^n = \sum_{r=0}^{n}\binom{n}{r}a^{n-r}b^r$$

holds for all $n \in \mathbb{N}$. □

1.24 Show that, in a field of finite characteristic p,

$$(x-y)^p = x^p - y^p.$$

Proof. Let x, y be elements of a field with characteristic p. We will need two lemmas for this proof. They are stated below.

Lemma 1. In a field, $-x = (-1)x$.

Lemma 2. In a field, $(-1)^{2n} = 1$ for $n \in \mathbb{N}$.

By Theorem 1.50, Lemma 1. and Lemma 2. if $p \neq 2$ then

$$\begin{aligned}(x-y)^p &= (x+(-y)^p \\ &= x^p + (-y)^p \\ &= x^p + ((-1)y)^p \\ &= x^p + (-1)^p y^p \\ &= x^p - y^p.\end{aligned}$$

It is more complicated if $p = 2$. First note for y in a field of characteristic 2, $2y = 0 \implies y + y = 0 \implies y = -y$. Therefore we can conclude

$$\begin{aligned}(x-y)^p &= (x-y)^2 \\ &= x^2 - 2xy + y^2 \\ &= x^2 - y^2\end{aligned}$$

as desired. □

1.25 Let K be a field of characteristic p. By using Theorem 1.50, deduce, by induction on n, that

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n}, \quad (x, y \in K, n \in \mathbb{N}).$$

1.26 Show that every subgroup of index 2 is normal.

Proof. □

1.27 Show that, for every $n \geq 2$, the additive group $(\mathbb{Z}_n, +)$ is cyclic.

1.28 Show that every subgroup of a cyclic group is cyclic.

Proof. □

1.29 Consider a group G of order 8 given by the multiplication table

	e	a	b	c	p	q	r	s
e	e	a	b	c	p	q	r	s
a	a	b	c	e	q	r	s	p
b	b	c	e	a	r	s	p	q
c	c	e	a	b	s	p	q	r
p	p	s	r	q	e	c	b	a
q	q	p	s	r	a	e	c	b
r	r	q	p	s	b	a	e	c
s	s	r	q	p	c	b	a	e

(i) Show that $B = \{e, b\}$ and $Q = \{e, q\}$ are subgroups.

Proof. Let $B = \{e, b\}$ and $Q = \{e, q\}$. It is clear from the multiplication table that $b^{-1} = b$, so for any $x, y \in B$, $xy^{-1} \in B$. Additionally, it is clear from the multiplication table that $q^{-1} = q$, so for any $x, y \in Q$, $xy^{-1} \in Q$. Thus B and Q are subgroups. □

(ii) List the left and right cosets of B and Q, and deduce that B is normal and Q is not.

Proof. We will show through exhaustion that B is normal and Q is not. Note, $Be = Bb = eB = bB\{e, b\}$, $Ba = Bc = aB = cB = \{a, c\}$, $Bp = Br = pB = rB = \{p, r\}$, and $Bq = Bs = qB = sB = \{q, s\}$. Thus B is normal. Note, $Qa = \{a, p\} \neq \{r, a\} = aQ$ so Q is not normal. □

(iii) Let H be the group given by the table

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Describe a homomorphism φ from G onto H with kernel B.

1.30 Let $g, h \in A$, where A is a finite abelian group. Show that $o(gh)$ divides $o(g)o(h)$. By considering the group given by

	e	a	b	x	y	z
e	e	a	b	x	y	z
a	a	b	e	z	x	y
b	b	e	a	y	z	x
x	x	y	z	e	a	b
y	y	z	x	b	e	a
z	z	x	y	a	b	e

show that this is not necessarily true in a non-abelian group.

1.31 Let G be a group and N be a normal subgroup of G. Show that every subgroup H of G/N can be written K/N, where K is a subgroup of G containing N, and is normal if and only if H is normal.

2 Integral Domains and Polynomials

2.1 Euclidean Domains

Chapter 3 is a more serious study of fields, but more needs to be established about polynomials before we reach that point.

Definition 2.1. ⟨ *noun, integral domain* ⟩
An integral domain D is called an **euclidean domain** if there is some mapping δ from D into $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$ with the property that $\delta(0) = 0$, and for all $a, b \in D$ with $b \neq 0$, there exists $q, r \in D$ such that

$$a = qb + r \quad \text{and} \quad \delta(r) < \delta(b).$$

Below lie a couple examples and non-examples of euclidean domains.

- The integers are the primordial example of a euclidean domain. For integers $m, n \in \mathbb{Z}$ we can find $q, r \in \mathbb{Z}$ (namely $q = \lfloor m/n \rfloor$ and $r = m \mod n$ for $m, n > 0$) such that $m = qn + r$.
- The gaussian integers form a euclidean domain $\mathbb{Z}[i] \coloneqq \{a + bi : a, b \in \mathbb{Z}\}$.
- The integral domain $\mathbb{Z}[i\sqrt{3}]$ does **not** form a euclidean domain. We will prove this below.

  Proof. Consider $\mathbb{Z}[i\sqrt{3}]$. Note, 2 is an irreducible element of $\mathbb{Z}[i\sqrt{3}]$ and $2 \mid 4 = (1+i\sqrt{3})(1-i\sqrt{3})$ but 2 does not divide $(1 \pm i\sqrt{3})$ in $\mathbb{Z}[i\sqrt{3}]$. Using the contrapositive of Theorem 2.13, we know $\mathbb{Z}[i\sqrt{3}]$ is not a principal ideal domain. Therefore $\mathbb{Z}[i\sqrt{3}]$ is not a euclidean domains by the contrapositive of Theorem 2.6. □

Remark 2.2.
It should be noted that $\delta^{-1}\{0\} = \{0\}$ because if $\delta(b) = 0$ there would be no r such that $\delta(r) < \delta(b)$.

Theorem 2.3.
Every field is a euclidean domain.

Proof. Let K be a field and let $a, b \in K$ with $b \neq 0$ and let $\delta : K \to \mathbb{N}^0$ with $\delta(x) = 0$ if and only if $x = 0$. Note, K is an integral domain. $a = (ab^{-1})b + 0 = a(b^{-1}b) = a1$ and $\delta(0) < \delta(b)$ by definition. Thus, K is a euclidean domain. □

Definition 2.4. ⟨ *noun, algorithm* ⟩
In the ring $\mathbb{Z}$, where $\delta(a) = |a|$, the **division algorithm** is the process of dividing a by b to obtain a **quotient** q and **remainder** r.

Below lie a few examples of the division algorithm in $\mathbb{Z}$.

- Note, $37 = 5 \cdot 7 + 2$, so $a = 37, b = 7, q = 5, r = 2$ and $2 < 7$.
- Note, $129 = 11 \cdot 11 + 8$ so $a = 129, b = 11, q = 11, r = 8$ and $8 < 11$.
- Note, $26 = 13 \cdot 2 + 0$ so $a = 26$, $b = 2$, $q = 13, r = 2$ and $2 < 13$.
- Note $0 = 0 \cdot 19 + 0$ and $0 < 19$.
- Note, $-73 = -4 \cdot 18 - 1$ and $|-1| < 18$.

Definition 2.5. ⟨ *noun, integral domain* ⟩
An integral domain D is called a **principal ideal domain** if all of its ideals are principal.

Example. The integers form a principal ideal domain. Consider the ideal generated by $\{3, 4\}$ is equal to $\langle 1 \rangle$ and the ideal generated by $\{6, 15\}$ is equal to the ideal $\langle 3 \rangle$.

Theorem 2.6.
Every euclidean domain is a principal ideal domain.

Proof. Let D be a euclidean domain. The ideal $\{0\}$ is principal. Let I be a nonzero ideal. Note, there exists $b \in I$ such that $\delta(b) = \mathsf{min}\{\delta(x) : x \in I \backslash \{0\}\}$ by the well ordering principle. Let $a \in I$. There exist $q, r \in I$ such that $a = qb + r$ and $\delta(r) < \delta(b)$. Note, $r = a - qb \in I$ but since $\delta(r) < \delta(b)$, r must be 0. Thus $a = qb$. So, $I = Db = \langle b \rangle$ which is a principal ideal. □

Definition 2.7. ⟨ *noun, element* ⟩
Let D be a principal ideal domain and let a and b be nonzero elements of D. There exists a d such that $\langle d\rangle = \langle a, b\rangle \coloneqq \{sa + tb : s, t \in D\}$. It should be noted that $d \mid a$ and $d \mid b$. We call d the **greatest common divisor**, or **highest common factor** of a and b, denoted $d = \mathsf{gcd}(a, b)$.

Example. Knowing the integers form a principal ideal domain, we can see $\langle 6, 15\rangle = \langle 3\rangle$ and thus $3 = \mathsf{gcd}(6, 15)$.

Theorem 2.8. Properties of Greatest Common Divisor:
In a principal ideal domain D, the greatest common divisor d of a and b has the following properties:

1. $d \mid a$ and $d \mid b$,
2. if $d' \mid a$ and $d' \mid b$ then, $d' \mid d$.

Proof. Let D be a principal ideal domain, and let $d \in D$ be the greatest common divisor of $a, b \in D$. We will show $d \mid a$ and $d \mid b$. It is easy to see $\langle a\rangle \subseteq \langle d\rangle$ because $\langle d\rangle = \{sa + tb : s, t \in D\}$ and $\langle a\rangle = \{sa + 0b : s \in D\}$. By Theorem 1.22 we know in an integral domain $\langle a\rangle \subseteq \langle d\rangle$ if and only if $d \mid a$, therefore $d \mid a$. The same argument can be used to show $d \mid b$.

Now we will show if $d' \mid a$ and $d' \mid b$ then $d' \mid d$. Let $d' \in D$ such that if $d' \mid a$ and $d' \mid b$. Note, since $d \in \langle a, b\rangle$ there exists $s, t \in D$ such that $d = sa + tb$. Since $d' \mid a$ and $d' \mid b$, there exists $p, q \in D$ such that $pd' = a$ and $qd' = b$. Therefore, $d = spd' + tqd' = (sp + tq)d'$ and thus $d' \mid d$. □

Definition 2.9. ⟨ *adjective, two elements* ⟩
Let D be a principal ideal domain and let a and b be nonzero elements of D. If $\mathsf{gcd}(a, b) \sim 1$ we say a and b are **coprime**, or **relatively prime**.

Example. Consider the principal ideal domain $\mathbb{Z}$. Note, $\langle 18, 35\rangle = \langle 1\rangle = \langle -1\rangle$. The integers 18 and 35 are relatively prime.

Theorem 2.10.
In a principal ideal domain D, every finite set $\{a_1, a_2, \ldots, a_n\} \subseteq D$ has a greatest common divisor.

This theorem is an extension of the definition the greatest common divisor of two elements. We will prove it below.

Proof. Let D be a principal ideal domain. Let $\{a_1, a_2, \ldots, a_n\}$ be a finite subset of D. Since D is a principal ideal domain there exists $d_1 \in D$ such that $\langle d_1 \rangle = \langle a_1, a_2 \rangle$, also there exists $d_2 \in D$ such that $\langle d_2 \rangle = \langle d_1, a_3 \rangle$ and so on until we get $d_{n-1} \in D$ such that $\langle d_{n-1} \rangle = \langle d_{n-2}, a_n \rangle$. Note, for $k \leq n$, $\langle a_k \rangle \subseteq \langle d_{n-1} \rangle$ so $d_{n-1} \mid a_k$. Thus $\{a_1, a_2, \ldots, a_n\}$ has a greatest common divisor d_{n-1}. □

Definition 2.11. ⟨ *noun, algorithm* ⟩
Suppose a and b are nonzero elements of a euclidean domain D, and suppose without loss of generality $\delta(b) \leq \delta(a)$. The following algorithm we describe is referred to as **the Euclidean algorithm**. There exist $q_1, q_2, \ldots, q_k$ and $r_1, r_2, \ldots, r_{k-1}$ such that

$$\begin{aligned}
a &= q_1 b + r_1, \quad \delta(r_1) < \delta(b), \\
b &= q_2 r_1 + r_2, \quad \delta(r_2) < \delta(r_1), \\
r_1 &= q_3 r_2 + r_3, \quad \delta(r_3) < \delta(r_2), \\
r_2 &= q_4 r_3 + r_4, \quad \delta(r_4) < \delta(r_3), \\
&\vdots \\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, \quad \delta(r_{k-1}) < \delta(r_{k-2}), \\
r_{k-2} &= q_k r_{k-1}.
\end{aligned}$$

It follows that r_{k-1} is the greatest common divisor of a and b.

Example. We will use the euclidean algorithm to find the greatest common divisor of 615 and 345.

Note,

$$\begin{aligned}
615 &= 1 \cdot 345 + 270 \\
345 &= 1 \cdot 270 + 75 \\
270 &= 3 \cdot 75 + 45 \\
75 &= 1 \cdot 45 + 30 \\
45 &= 1 \cdot 30 + 15 \\
30 &= 2 \cdot 15 + 0,
\end{aligned}$$

thus 15 is the greatest common divisor of 615 and 345. We can represent 15 as $a \cdot 615 + b \cdot 345$ as so,

$$\begin{aligned} 15 &= 45 - 30 = 45 - (75 - 45) = 2 \cdot 45 - 75 \\ &= 2 \cdot (270 - 3 \cdot 75) - 75 = 2 \cdot 270 - 7 \cdot 75 \\ &= 2 \cdot 270 - 7 \cdot (345 - 270) = 9 \cdot 270 - 7 \cdot 345 \\ &= 9 \cdot (615 - 345) - 7 \cdot 345 \\ &= 9 \cdot 615 - 16 \cdot 345. \end{aligned}$$

2.2 Unique Factorisation

Definition 2.12. ⟨ *adjective, element* ⟩
Let D be an integral domain with group of units U and let $p \in D$ be such that $p \neq 0$ and $p \notin U$. Then p is said to be **irreducible** if it has no proper factors.

Example. In the integral domain $\mathbb{Z}$ there exists no numbers $a, b \in \mathbb{Z}$ with $a, b \neq 1, -1, 17, -17$ such that $ab = 17$.

The previous definition is a generalization of prime numbers. Prime numbers have many convenient properties, one of which is the fact that if p is prime and $p|ab$, then we know $p|a$ or $p|b$. We provide the generalization of this theorem to principal ideal domains below.

Theorem 2.13.
Let D be a principal ideal domain, let p be an irreducible element in D, and let $a, b \in D$. Then

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proof. Let D be a principal ideal domain, and let p be an irreducible element in D, let $a, b \in D$. Suppose that $p \mid ab$ and $p \nmid a$. Then the greatest common divisor of a and p must be 1, and so there exists $s, t \in D$ such that $sa + tp = 1$. Hence $sab + tpb = b$, it is clear that p divides sab and tpd, so p divides $sab + tpb$, it follows that $p \mid b$. □

Corollary 2.14.
Let D be a principal ideal domain and let p be an irreducible element in D, and let $a_1, a_2, \ldots, a_m \in D$. Then

$$p \mid a_1 a_2 \cdots a_m \implies p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \text{ or } p \mid a_m.$$

Proof. Let D be a principal ideal domain and let p be an irreducible element in D, and let $a_1, a_2, \ldots, a_n \in D$ for $n \geq 2$. We will show by induction that

$$p \mid a_1 a_2 \cdots a_n \implies p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \text{ or } p \mid a_n$$

for $n \geq 2$. Note, by Theorem 2.13 we know if $p \mid a_1 a_2$ then $p \mid a_1$ or $p \mid a_2$. Now suppose inductively

$$p \mid a_1 a_2 \cdots a_k \implies p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \text{ or } p \mid a_k$$

for some $k \geq 2$. Now suppose $p \mid a_1 a_2 \cdots a_k a_{k+1}$ for $a_{k+1} \in D$. By assumption $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_k$. So, it is true to say $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_k$ or $p \mid a_{k+1}$. Therefore, for $n \geq 2$

$$p \mid a_1 a_2 \cdots a_n \implies p \mid a_1 \text{ or } p \mid a_2 \text{ or } \cdots \text{ or } p \mid a_n,$$

as desired. □

Theorem 2.15.
Let p be an element of a principal ideal domain D. Then the following statements are equivalent:

(i) p is irreducible;

(ii) $\langle p \rangle$ is a maximal proper ideal of D;

(iii) $D/\langle p \rangle$ is a field.

Proof. Let p be an element of a principal ideal domain D. We will show statements (i), (ii), and (iii) in Theorem 2.15 are equivalent.

First we will show (i) $\implies$ (ii). Suppose the p is irreducible. Then p is not a unit, and so $\langle p \rangle$ is a proper ideal of D by Theorem 1.22. Suppose by way of contradiction, that there is a principal ideal $\langle q \rangle$ such that $\langle p \rangle \subset \langle q \rangle \subset D$. Then $p \in \langle q \rangle$, and so $p = aq$ for some non-unit a which contradicts the fact that p is irreducible. Thus $\langle p \rangle$ is a maximal proper ideal of D.

Next we will show (ii) $\implies$ (iii). Suppose $\langle p \rangle$ is a maximal proper ideal of D. Let $a + \langle p \rangle$ be a non-zero element of $D/\langle p \rangle$. Then $a \notin \langle p \rangle$, and so the ideal $\langle a \rangle + \langle p \rangle$ properly contains $\langle p \rangle$. Since we are assuming that $\langle p \rangle$ is maximal, and so it follows that $\langle a \rangle + \langle p \rangle = \{sa + tp : s, t \in D\} = D$. Hence there exists $s, t \in D$ such that $sa + tp = 1$, and from this we deduce that $(s + \langle p \rangle)(a + \langle p \rangle) = 1 + \langle p \rangle$. Therefore $D/\langle p \rangle$ is a field.

Finally we will show (iii) $\implies$ (i). If p is not irreducible, then there exists non-units q, r

such that $p = qr$. Then $q + \langle p \rangle$ and $r + \langle p \rangle$ are both non-zero elements of $D/\langle p \rangle$, but

$$(q + \langle p \rangle)(r + \langle p \rangle) = p + \langle p \rangle = 0 + \langle p \rangle.$$

Thus $D/\langle p \rangle$ has zero divisors and is not a field. By contraposition, we know if $D/\langle p \rangle$ is a field, then p is irreducible.

Therefore, (i), (ii), and (iii) are equivalent. □

Definition 2.16. ⟨ *noun, product* ⟩
Let d be an element of an integral domain D. The element d has a **factorization into irreducible elements** if there exists irreducible elements $p_1, p_2, \ldots, p_k$ such that $d = p_1 p_2 \cdots p_k$.

This is essentially the fundamental theorem of arithmetic generalized to integral domains.

Definition 2.17. ⟨ *adjective, factorization* ⟩
Let d be an element of an integral domain D with a factorization into irreducible elements $d = p_1 p_2 \cdots p_k$. The factorization is **essentially unique** if, for irreducible elements $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$,

$$d = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

implies that $k = l$ and, for some permutation $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$,

$$p_i \sim q_{\sigma(i)}, \quad \forall i \in \{1, 2, \ldots, k\}.$$

Definition 2.18. ⟨ *noun, integral domain* ⟩
An integral domain D is said to be a **factorial domain**, or to be a **unique factorization domain**, if every non-unit, non-zero element a of D has an essentially unique factorization into irreducible elements.

Theorem 2.19.
Every principal ideal domain is a factorial domain.

Proof. The following proof relies on a few lemmas, which are be proved below. Let D be a principal ideal domain. First we will show any $a \neq 0$ in D can be expressed as a product of irreducible elements. Let a be a non-unit in D. Then either a is irreducible, or it has a

proper divisor a_1. Similarly, either a_1 is irreducible or a_1 has a proper divisor a_2. Continuing, we obtain a sequence $a = a_0, a_1, a_2, \ldots$ in which, for $i = 1, 2, \ldots$, a_i is a proper divisor of a_{i-1}. The sequence must terminate at some a_k, since otherwise we would have an infinite chain of ascending sequences

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

and Lemma 2.20 would be contradicted. Hence a has a proper irreducible divisor $a_k = z_1$, and $a = z_1 b_1$ for some $b_1 \in D$. If b_1 is irreducible, then the proof is complete. Otherwise we can repeat the argument we used for a to find a proper irreducible divisor z_2 of b_1 and $a = z_1 z_2 b_2$. We continue this process, which too must terminate, since otherwise we would have an infinite ascending sequence

$$\langle a \rangle \subset \langle b_1 \rangle \subset \langle b_2 \rangle \subset \cdots,$$

in contradiction to Lemma 2.20. Hence some b_l must be irreducible, and so $a = z_1 z_2 \cdots z_{l-1} b_l$ is a product of irreducible elements.

To show the product is essentially unique we can extend Theorem 2.13 to more than two elements as in Corollary 2.14. Suppose that

$$p_1 p_2 \cdots p_k \sim q_1 q_2 \cdots q_l,$$

where $p_1, p_2, \cdots, p_k$ and $q_1, q_2, \cdots, q_l$ are irreducible. Suppose first that $k = 1$. Then $l = 1$, since $q_1 q_2 \cdots q_l$ is irreducible, and so $p_1 \sim q_1$. Suppose inductively that for all $n \geq 2$ and all $k \leq n$, any statement of the form

$$p_1 p_2 \cdots p_k \sim q_1 q_2 \cdots q_l$$

implies that $k = l$ and that, for some permutation σ of $\{1, 2, \ldots, k\}$,

$$q_i \sim p_{\sigma(i)} \quad \text{for } (i = 1, 2, \ldots, k).$$

Let $k = n$. Since $p_1 \mid q_1 q_2 \cdots q_l$, it follows from Corollary 2.14 that $p_1 \mid q_j$ for some $j \in \{1, 2, \ldots, l\}$. Since q_j is irreducible and p_1 is not a unit, we deduce that $p_1 \sim q_j$ and by cancellation we have

$$p_2 \cdots p_k \sim q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_l.$$

By the induction hypothesis, we have that $n - 1 = l - 1$ and that fro $i \in \{1, 2, \ldots, n\} \backslash \{j\}$, $q_i \sim p_{\sigma(i)}$ for some permutation σ of $\{2, 3, \ldots, n\}$. Hence, extending σ to permutation of

$\{1, 2, \ldots, n\}$ by defining $\sigma(1) = j$, we obtain the desired result. □

Lemma 2.20.
In a principal ideal domain there are no infinite ascending chains of ideals.

Proof. Let D be an integral domain and let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an ascending chain of ideals. We will show $I = \bigcup_{j\geq 1} I_j$ is an ideal. Let $a, b \in I$, then there exists k, l such that $a \in I_k$ and $b \in I_l$, and so $a - b \in I_{\max\{k,l\}} \subseteq I$. Also, if $a \in I$ and $s \in D$, then $a \in I_k$ for some k, and so $sa \in I_k \subseteq I$.

Now suppose that D is a principal ideal domain, and let

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \cdots$$

be an ascending chain of principal ideals. From the previous paragraph, we know that the union of all the ideals in this chain must be an ideal, and by our assumption about D, this must be a principal ideal $\langle a \rangle$. Since $a \in \bigcup_{j\geq 1} \langle a_j \rangle$, we must have that $a \in \langle a_k \rangle$ for some k. Thus $\langle a \rangle \subseteq \langle a_k \rangle$ and since it is clear that we also have $\langle a_k \langle \subseteq \langle a \rangle$, it follows that $\langle a \rangle = \langle a_k \rangle$. Hence

$$\langle a_k \rangle = \langle a_{k+1} \rangle = \langle a_{k+2} \rangle = \cdots = \langle a \rangle,$$

and so the infinite chain of inclusions terminates at $\langle a_k \rangle$. □

Corollary 2.21.
Every euclidean domain is a factorial domain.

Proof. Let D be a euclidean domain. We know D is a principal ideal domain and by 2.19 we know D is a factorial domain as desired. □

Remark 2.22.
We have now seen several theorems relating certain types of integral domains. We will use loose notation to describe this relationship below,

$$\begin{aligned} \text{Field} &\implies \text{Euclidean Domain} \\ &\implies \text{Principal Ideal Domain} \\ &\implies \text{Factorial Domain} \\ &\implies \text{Integral Domain} \\ &\implies \text{Ring.} \end{aligned}$$

2.3 Polynomials

Definition 2.23. ⟨ *noun, sequence* ⟩
A **polynomial** f with coefficients in an integral domain R is a sequence $(a_0, a_1, \ldots)$, where $a_i \in R$ for all $i \geq 0$, and where only finitely many of $\{a_0, a_1, \ldots\}$ are non-zero.

Definition 2.24. ⟨ *noun, number* ⟩
A polynomial f, $(a_0, a_1, \ldots)$, with a_n being the last nonzero term, has **degree**[a] n, denoted $\partial f = n$. The entry a_n is called the **leading coefficient** of f.

[a] If *all* coefficients are zero we say f has degree $-\infty$.

Definition 2.25. ⟨ *adjective, polynomial* ⟩
A polynomial with leading coefficient 1 is called **monic**.

Definition 2.26. ⟨ *adjective, polynomial* ⟩
A polynomial of degree 0 or $-\infty$ is called **constant**.

Definition 2.27. ⟨ *noun, processes* ⟩
Let $(a_0, a_1, \ldots)$ and $(b_0, b_1, \ldots)$ be polynomials. **Addition** is defined as follows,

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

Multiplication is defined as follows,

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

where for $k = 0, 1, 2 \ldots$,

$$c_k = \sum_{\{(i,j)\,:\,i+j=k\}} a_i b_j.$$

Theorem 2.28.
The set P of all polynomials with coefficients in an integral domain R is a commutative ring with unity with respect to addition and multiplication as defined in Definition 2.27.

Definition 2.29. ⟨ *noun, polynomial* ⟩
A polynomial $f = (a_0, a_1, \ldots)$ with coefficients from an integral domain R can be written in the form

$$f = f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_x X^n,$$

where X the a polynomial of the form $(0, 1, 0, 0, \ldots)$. We say that f is a **polynomial over R in the indeterminate X**. The ring P of all such polynomials is written $R[X]$ and referred to as the **polynomial ring** of R.

Let $X = (0, 1, 0, 0, \ldots)$ be a polynomial. Then

$$X^m = (x_0, x_1, \ldots), \text{ where } x_m = \begin{cases} 1 & \text{if } m = n \\ 0 & \text{otherwise.} \end{cases}$$

As an example, $X^3 = (0, 0, 0, 1, 0, \ldots)$.

Theorem 2.30.
Let D be an integral domain, and let $D[X]$ be the polynomial ring of D. Then,

(i) $D[x]$ is an integral domain,

(ii) if $p, q \in D[X]$, then $\partial(p+q) \leq \max\{\partial p, \partial q\}$,

(iii) for all $p, q \in D[X]$, $\partial(pq) = \partial p + \partial q$,

(iv) The group of units of $D[X]$ coincides with the group of units of D.

Remark 2.31.
Since the ring of polynomials over an integral domain D is itself an integral domain, we can repeat the process and form a ring of polynomials with coefficients from $D[X]$. We will use Y as the indeterminate for the new ring, so we have $(D[X])[Y]$, or as more usually denoted, $D[X, Y]$. This can be repeated to acquire the integral domain $D[X_1, X_2, \ldots, X_n]$.

Definition 2.32. ⟨ *noun, polynomial* ⟩
The field of fraction of $D[X]$ consists of **rational forms**

$$\frac{a_0 + a_1X + a_2X^2 + \cdots + a_mX^m}{b_0 + b_1X + b_2X^2 + \cdots + b_nX^n},$$

where the denominator is not the zero polynomial. This field is denoted by $D(X)$.

Theorem 2.33.
Let D, D' be integral domains, and let $\varphi : D \to D'$ be an isomorphism. Then the mapping $\hat{\varphi} : D[X] \to D'[X]$ defined by

$$\hat{\varphi}(a_0 + a_1X + \cdots a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$$

is an isomorphism, and $\hat{\varphi}$ is called the **canonical extension** of φ. A further extension $\varphi^* : D(X) \to D'(X)$ is defined by

$$\varphi^*(f/g) = \hat{\varphi}(f)/\hat{\varphi}(g) \quad f, g \in D(X).$$

Theorem 2.34.
Let K be a field, and let f, g be elements of the polynomial ring $K[X]$, with $g \neq 0$. Then there exists unique elements $q, r \in K[X]$ such that $f = qg + r$ and $\partial r < \partial g$.

Theorem 2.35.
If K is a field, then $K[X]$ is a euclidean domain.

Theorem 2.36.
Let K be a field. Then,

(i) every pair (f, g) of polynomials in $K[X]$ has a greatest common divisor d, which can be expressed as $af + bg$, with $a, b \in K[X]$,

(ii) $K[X]$ is a principal ideal domain,

(iii) $K[X]$ is a factorial domain,

(iv) if $f \in K[X]$, then $K[X]/\langle f \rangle$ is a field if and only if f is irreducible.

Theorem 2.37. The Remainder Theorem:
If K is a field, let $\beta \in K$ and let f be a non-zero polynomial in $K[X]$. Then the remainder upon dividing f by $X - \beta$ is $f(\beta)$. In particular, β is a root of f if and only if $(X - \beta) \mid f$.

2.4 Irreducible Polynomials

Theorem 2.38.
If K is a field, and let $g(X)$ be an irreducible polynomial in $K[X]$. Then $K[X]/\langle g(X) \rangle$ is a field containing K up to isomorphism.

Theorem 2.39.
The irreducible elements of the polynomial ring $\mathbb{R}[X]$ are either linear or quadratic. Every polynomial

$$g(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

in $\mathbb{R}[X]$ has a unique factorization

$$a_n (X - \beta_1) \cdots (X - \beta_r)(X^2 + \lambda_1 X + \mu_1) \cdots (X^2 + \lambda_s X + \mu_s),$$

in $\mathbb{R}[X]$, where $a_n \in \mathbb{R}$, $r, s \geq 0$ and $r + 2s = n$.

Theorem 2.40.
Let $g(X) = X^2 + a_1 X + a_0$ be a polynomial with coefficients in $\mathbb{Q}$. Then,

(i) if $g(X)$ is irreducible over $\mathbb{R}$, then it is irreducible over $\mathbb{Q}$,

(ii) if $g(X) = (X - \beta_1)(X - \beta_2)$, with $\beta_1, \beta_2 \in \mathbb{R}$, then $g(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if β_1 and β_2 are irrational.

Theorem 2.41. Gauss's Lemma:
Let f be a polynomial in $\mathbb{Z}[X]$, irreducible over $\mathbb{Z}$. Then f, considered as a polynomial in $\mathbb{Q}[X]$, is irreducible over $\mathbb{Q}$.

Proof. Let f be a polynomial in $\mathbb{Z}[X]$ that is irreducible over $\mathbb{Z}$. Suppose f, as considered as a polynomial in $\mathbb{Q}[X]$, is not irreducible and $f = gh$ for $g, h \in \mathbb{Q}[X]$ with $\partial g, \partial h < \partial f$. There exists a positive integer $n \in \mathbb{Z}$ such that $nf = g'h'$ where $g', h' \in \mathbb{Z}[X]$. Suppose n is the smallest positive integer with this property. Let

$$g' = a_0 + a_1 X + \cdots a_k X^k \text{ and } h' = b_0 + b_1 X + \cdots b_l X^l.$$

If $n = 1$ then $g' = g, h' = h$ and we have an immediate contradiction. Otherwise, let p be a prime factor of n. By Lemma 2.42 we may suppose without loss of generality, p divides each coefficient in g', and thus $g' = pg''$ for $g'' \in \mathbb{Z}[X]$. Thus, $(n/p)f = g''h'$. But, n/p is smaller than n which is a contradiction because we assumed n was the least positive integer with this property. Thus, $f \neq gh$ and f is irreducible. □

Lemma 2.42.
Either p divides all the coefficients of g', or p divides all the coefficients of h'.

Proof. For $f = c_0 + c_1X + \cdots c_mX^m$, $nc_0 = a_0b_0$, therefore p must divide either a_0 or b_0. Now suppose by way of contradiction p divides $a_0, a_1, \ldots, a_{i-1}$ but not a_i, and p divides $b_0, b_1, \ldots, b_{j-1}$ but not b_j. The coefficient of X^{i+j} in nf is

$$a_0b_{i+j} + \cdots + a_ib_j + \cdots + a_{i+j}b_0.$$

Note, p divides all the terms preceding and following a_ib_j, but not a_ib_j. It follows that the coefficient of X^{i+j} in nf is not divisible by p. This is a contradiction because we assumed p is a factor of n, since the coefficients in f are integers p would divide each coefficient in nf. Hence, p must either divide all the coefficients in g' or h'. □

Theorem 2.43. Eisenstein's Criterion:
Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial in $\mathbb{Z}[X]$. Suppose that there exists a prime number p such that

(i) $p \nmid a_n$,

(ii) $p \mid a_i$, $(i = 0, 1, \ldots, n-1)$,

(iii) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

We have seen several theorems relating the factorizability of polynomials in one polynomial ring to another. We will summarize the theorems thusly. Irreducibility over $\mathbb{R}$ implies irreducibility over $\mathbb{Q}$. Irreducibility over $\mathbb{Q}$ implies irreducibility over $\mathbb{Z}$. Irreducibility over $\mathbb{Z}$ implies irreducibility over $\mathbb{Q}$, but irreducibility over $\mathbb{Q}$ does **not** imply irreducibility over $\mathbb{R}$. Factorizability over $\mathbb{Z}$ implies factorizability over $\mathbb{Q}$. Factorizability over $\mathbb{Q}$ implies factorizability over $\mathbb{R}$.

Exercises

2.1 For the following pair (a, b) of integers, find the greatest common divisor, and express it as $sa + tb$, where $s, t \in \mathbb{Z}$

(i) $(1218, 846)$;

Proof. By the euclidean algorithm we can see,

$$\begin{aligned} 1218 &= 1 \cdot 846 + 372 \\ 846 &= 2 \cdot 372 + 102 \\ 372 &= 3 \cdot 102 + 66 \\ 102 &= 1 \cdot 66 + 36 \\ 66 &= 1 \cdot 36 + 30 \\ 36 &= 1 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0. \end{aligned}$$

Thus $\mathsf{gcd}(1218, 846) = 6$. Going in reverse we can see,

$$6 = 36 - 30 = MORETODO$$

□

(ii) $(851, 779)$.

2.2 Show that a commutative ring with unity is embeddable in a field if and only if it is an integral domain.

2.3 For another example of a euclidean domain consider the set $\Gamma = \{x + yi : x, y \in \mathbb{Z}\}$ of gaussian integers.

(i) Show that Γ is an integral domain.

(ii) For each $z = x + yi$ in Γ, define $\delta(z) = |x + yi|^2 = x^2 + y^2$. Let $a, b \in \Gamma$, with $b \neq 0$. Then $ab^{-1} = u + iv$, where $u, v \in \mathbb{Q}$. There exist integers u', v' such that $|u - u'| \leq \frac{1}{2}$, $|v - v'| \leq \frac{1}{2}$. Let $q = u' + iv'$. Show that $a = qb + r$, where $r \in \Gamma$ and $\delta(r) \leq \frac{1}{2}\delta(b)$.

2.4 Let p be a prime number, and let

$$D_p \coloneqq \left\{ \frac{r}{s} \in \mathbb{Q} : \mathsf{gcd}(r, s) = 1 \text{ and } p \not| s \right\}.$$

(i) Show that D_p is a subring of $\mathbb{Q}$.

Proof. Let

$$D_p \coloneqq \left\{ \frac{r}{s} \in \mathbb{Q} : \mathsf{gcd}(r, s) = 1 \text{ and } p \not| s \right\}$$

for a prime p. We will show D_p is a subring of $\mathbb{Q}$. Let $\frac{a}{b}, \frac{c}{d} \in D_p$. Note, $\frac{a}{b} - \frac{c}{d} = \frac{a}{b} + (-\frac{c}{d}) = \frac{ad-cd}{bd} = \frac{x}{y}$ where $\frac{x}{y}$ is obtained by dividing $ab - cd$ and bd by their greatest common divisors. Since p doesn't divide b or d, p does not divide bd, and therefore does not divide y, a factor of bd. Then by the choice of x, y their greatest common divisor is clearly 1. So, $\frac{a}{b} - \frac{c}{d} \in D_p$. Note, $\frac{a}{b} \cdot \frac{c}{d} \in D_p = \frac{ac}{bd} = \frac{x}{y}$ where $\frac{x}{y}$ is obtained by dividing ac and bd by their greatest common divisors. Since p doesn't divide b or d, p does not divide bd, and therefore does not divide y, a factor of bd. Then by the choice of x, y their greatest common divisor is clearly 1. So, $\frac{a}{b} \cdot \frac{c}{d} \in D_p$, and D_p is a subring. □

(ii) Describe the units of D_p.

The units of D_p are

$$U = \left\{ \frac{r}{s} \in D_p : p \not| r \right\}.$$

(iii) Show that D_p is a principal ideal domain.

2.5

2.6

2.7

2.8

2.9

2.10

2.11

2.12

2.13

2.14

2.15

2.16

2.17

3 Field Extensions

3.1 The Degree of an Extension

Definition 3.1. ⟨ *noun, field* ⟩
If K, L are fields and $\varphi : K \to L$ is a monomorphism, we say that L is an **extension** of K, and write $L : K$ is a (field) extension. The field L can be regarded as a vector space over K since all the vector space axioms are consequences of field axioms for L. Hence there exists a **basis** of L over K.

Definition 3.2. ⟨ *noun, set* ⟩
A **vector space**[a] over a field F is a non-empty set V with an addition over V and a scalar multiplication on V such that the following properties hold:

V1. *associativity of addition*, for all $x, y, z \in V$,

$$(x + y) + z = x + (y + z)$$

V2. *commutativity of addition*, for all $x, y \in V$,

$$x + y = y + x$$

V3. *existence of* 0, there exists a $0 \in V$ such that for all $x \in V$,

$$x + 0 = x$$

V4. *existence of negatives*, for all $x \in V$, there exists $-x \in V$ such that

$$x + (-x) = 0$$

V5. *distributive property I*, for all $a \in F$ and $x, y \in V$,

$$a(x + y) = ax + ay$$

V6. *distributive property II*, for all $a, b \in F$ and $x \in V$,

$$(a + b)x = ax + bx$$

V7. *associativity of scalar multiplication*, for all $a, b \in F$ and $x \in V$,

$$(ab)x = a(bx)$$

V8. *multiplicative identity*, for all $x \in V$,

$$1x = x.$$

[a] See Axler (pg. 12) [1]

Definition 3.3. ⟨ *noun, number* ⟩
If $L : K$ is a field extension then the **dimension** of L, is the cardinality of an arbitrarily chosen basis. This is also called the **degree of L over K**, or the **degree of the extension** $L : K$, denoted by $[L : K]$.

Definition 3.4. ⟨ *noun, extension* ⟩
If $L : K$ is a field extension we say that L is a **finite extension** of K if $[L : K]$ is finite; otherwise L is an **infinite extension**.

Theorem 3.5.
Let $L : K$ be a field extension. The $L = K$ if and only if $[L : K] = 1$.

Theorem 3.6.
Let $L : K$ and $M : L$ be field extensions. Then

$$[M : L][L : K] = [M : K].$$

Corollary 3.7.
Let $K_1, K_2, \ldots, K_n$ be fields, and suppose that $K_{i+1} : K_i$ is an extension for $1 \leq i \leq n - 1$. Then,

$$[K_n : K_1] = [K_n : N_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1].$$

3.2 Extensions and Polynomials

Definition 3.8. ⟨ *noun, subfield* ⟩
Let K be a subfield of a field L, and let S be a subset of L. Let[a] $K(S)$ be the intersection of all subfields of L containing $K \cup S$. Then $K(S)$ is a subfield of L and it is the smallest subfield containing $K \cup S$. We call $K(S)$ the **subfield of L generated over K by S**. If $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is finite, we write $K(S)$ as $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

[a] There is guaranteed to be at least one, namely L.

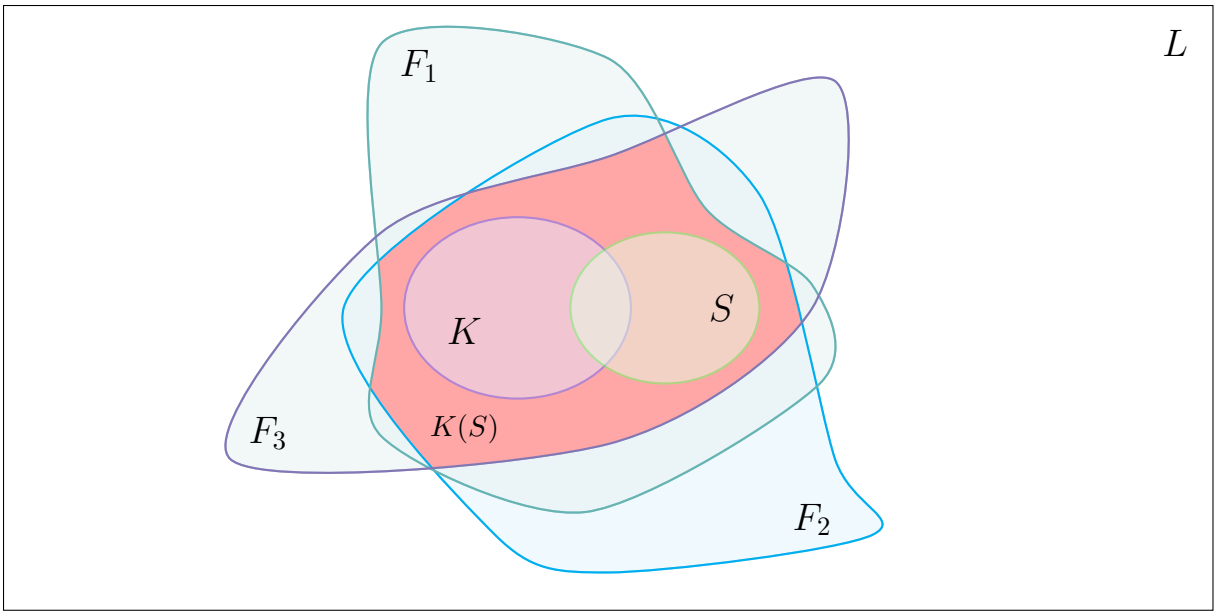


Figure 3.1: Diagram of $K(S)$

Theorem 3.9.
The subfield $K(S)$ of L coincides with the set E of all elements of L that can be expressed as quotients of finite linear combinations (with coefficients in K) of finite products of elements of S.

Definition 3.10. ⟨ *noun, field extension* ⟩
If the K is a subfield of L, and $\alpha \in L \backslash K$ then $K(\{\alpha\}) = K(\alpha)$ is the set of all quotients of polynomials in α with coefficients in K. We say $K(\alpha)$ is a **simple extension** of K.

Theorem 3.11.
Let L be a field and let K be a subfield of L, and let $\alpha \in L$. Then either

(i) $K(\alpha)$ is isomorphic to $K(X)$, the field of all rational forms with coefficients in K; or

(ii) there exists a unique monic polynomial $m \in K[X]$ with the property that, for all $f \in K[X]$,

(a) $f(\alpha) = 0$ if and only if $m \mid f$;

(b) the field $K(\alpha)$ coincides with $K[\alpha]$, the ring of polynomials in α with coefficients in K; and

(c) $[K(\alpha) : K] = \partial m$.

Definition 3.12. ⟨ *noun, polynomial* ⟩
The polynomial m defined in Theorem 3.11 is called the **minimum polynomial** of the element α.

Definition 3.13. ⟨ *adjective, field extension* ⟩
If an element α in a field L with subfield K has a minimum polynomial over K we say that α is **algebraic over** K and that $K[\alpha] = K(\alpha)$ is a **simple algebraic extension** of K.

Definition 3.14. ⟨ *noun, number* ⟩
A complex number that is algebraic over $\mathbb{Q}$ is called an **algebraic number**.

Definition 3.15. ⟨ *adjective, field extension* ⟩
Let $L : K$ be a field extension with $\alpha \in L$. If $K(\alpha)$ is isomorphic to the field $K(X)$ of rational functions, we say that α is **transcendental over** K and that $K(\alpha)$ is a **simple transcendental extension over** K.

Definition 3.16. ⟨ *noun, number* ⟩
A complex number that is transcendental over $\mathbb{Q}$ is called an **transcendental number**.

Theorem 3.17.
Let $K(\alpha)$ be a simple transcendental extension of a field K. Then the degree of $K(\alpha)$ over K is infinite.

Definition 3.18. ⟨ *adjective, field extension* ⟩
An extension L of K is said to be an **algebraic extension** if every element of L is algebraic over K. Otherwise L is a **transcendental extension**.

Theorem 3.19.
Every finite extension is algebraic.

Theorem 3.20.
Let $L : K$ and $M : L$ be field extensions, and let $\alpha \in M$. If α is algebraic over K, then it is also algebraic over L.

Theorem 3.21.
Let L be an extension of a field K, and let $\mathcal{A}(L)$ be the set of all elements in L that are algebraic over K. Then $\mathcal{A}(L)$ is a subfield of L.

Definition 3.22. ⟨ *noun, field* ⟩
If we take K as the field $\mathbb{Q}$ of rational numbers and L as the field $\mathbb{C}$ of complex numbers, then $\mathcal{A}(L)$ is the field $\mathbb{A}$ of **algebraic numbers**.

Theorem 3.23.
The field $\mathbb{A}$ of algebraic numbers is countable.

Theorem 3.24.
Transcendental numbers exist.

Theorem 3.25.
Let L be an extension of F, and let the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of L have minimum polynomials $m_1, m_2, \ldots, m_n$, respectively, over F. Then

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \leq \partial m_1 \partial m_2 \cdots \partial m_n.$$

3.3 Polynomials and Extensions

Theorem 3.26.
Let K be a field and let m be a monic irreducible polynomial with coefficients in K. Then $L = K[X]/\langle m\rangle$ is a simple algebraic extension $K[\alpha]$ of K, and $\alpha = X + \langle m\rangle$ has a minimum polynomial m over K.

Theorem 3.27.
Let K, K' be fields and let $\varphi : K \to K'$ be an isomorphism with canonical extension $\hat{\varphi} : K[X] \to K'[X]$. Let $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ be an irreducible polynomial of degree n with coefficients in K, and let $f' = \hat{\varphi}(f) = \varphi(a_n)X^n + \varphi(a_{n-1})X^{n-1} + \cdots + \varphi(a_0)$. Let L be an extension of K containing a root α of f, and let L' be an extension of K' containing a root α' of f'. Then there is an isomorphism ψ for $K[\alpha]$ onto $K'[\alpha']$, an extension of φ.

Corollary 3.28.
Let K be a field, and let f be an irreducible polynomial with coefficients in K. If L, L' are extensions of K containing roots α, α' of f, respectively, then there is an isomorphism from $K[\alpha]$ onto $K[\alpha']$ which fixes every element of K.

Definition 3.29. $\langle$ *noun, isomorphism* $\rangle$
A **K-isomorphism** α from L onto L' is an isomorphism with the property that $\alpha(x) = x$ for every element in K.

Exercises

3.1 Let $L : K$ and $M : L$ be field extensions and let $[M : K]$ be finite. Note, if $L : K$ and $M : L$ are field extensions then $K \subseteq L \subseteq M$. Show that

(i) if $[M : K] = [L : K]$, then $M = L$;

Proof. Let $L : K$ and $M : L$ be field extensions and let $[M : K]$ be finite. Suppose $[M : K] = [L : K]$. Then, $[M : L][L : K] = [M : K] \implies [M : L][M : K] = [M : K] \implies [M : L] = 1$, and therefore $M = L$. □

(ii) if $[M : L] = [M : K]$, then $L = K$.

Proof. Let $L : K$ and $M : L$ be field extensions and let $[M : K]$ be finite. Assume $[M : L] = [M : K]$. Then, $[M : L][L : K] = [M : K] \implies [M : K][L : K] = [M : K] \implies [L : K] = 1$, and therefore $L = K$. □

3.2 Let $L : K$ be a field extension such that $[L : K]$ is a prime number. Show that there is no subfield E of L such that $K \subset E \subset L$.

Proof. Let $L : K$ be a field extension such that $[L : K]$ is a prime number. Suppose by way of contradiction there exists a subfield E of L such that $K \subset E \subset L$. Thus, $[L : E][E : K] = [L : K]$ but since $[L : K]$ is prime, either $[L : E] = 1$ or $[E : K] = 1$. Therefore, either $L = E$ or $E = K$, but this contradicts the assumption that $K \subset E \subset L$. Therefore, there is no subfield E of L such that $K \subset E \subset L$ when $[L : K]$ is prime. □

3.3 Show that, if n is not a perfect square, the field $\mathbb{Q}[\sqrt{n}]$ is isomorphic to the field

$$K = \left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Why does this fail if n is a perfect square?

3.4 For arbitrary $a, b \in \mathbb{Q}$, find the minimum polynomial of $a + b\sqrt{2}$ over $\mathbb{Q}$.

3.5 Let $L : K$ be a field extension such that $[L : K] = 2$. Show that $L = K(\beta)$, where β is an arbitrarily chosen element of $L \backslash K$ and has a minimum polynomial of degree 2.

3.6 Let α be a root in $\mathbb{C}$ of the polynomial $X^2 + 2X + 5$. Express the element

$$\frac{\alpha^3 + \alpha - 2}{\alpha^2 - 3}$$

of $\mathbb{Q}(\alpha)$ as a linear combination of the basis $\{1, \alpha\}$.

3.7 Show that $f(X) = X^3 + X + 1$ is irreducible over $\mathbb{Q}$. Let α be a root of f in $\mathbb{C}$. Express

$$\frac{1}{\alpha} \text{ and } \frac{1}{\alpha + 2}$$

as linear combinations of $\{1, \alpha, \alpha^2\}$.

3.8

3.9

3.10

3.11

3.12

3.13

3.14

3.15

3.16

3.17 Let K be a field of characteristic 0, and suppose that $X^4 - 16X + 4$ is irreducible over K. Let α be the element $X + \langle X^4 - 16X + 4\rangle$ in the field $L = K[X]/\langle X^4 - 16X + 4\rangle$. Determine the minimum polynomials of $\beta_1 := \alpha^2, \beta_2 := \alpha^3 - 14\alpha$, and $\beta_3 := \alpha^3 - 18\alpha$.

Solution. We will determine the minimum polynomial for β_1, β_2, and β_3.

(a) Minimum polynomial for β_1: There is no $k \in K$ such that $\beta_1 - k = 0$, so the degree of the minimum polynomial must be at least 2. Note, $\beta_1^2 = \alpha^4 = X^4 + \langle X^4 - 16X + 4\rangle = 16X^2 - 4 + \langle X^4 - 16X + 4\rangle$. Thus we have $\beta_1^2 - 16\beta_1 + 4 = 16X^2 - 4 - 16X^2 + 4 = 0$. Thus, the minimum polynomial of β_1 is $X^2 - 16X + 4$.

(b) Minimum polynomial for β_2: Similarly, the minimum polynomial for β_2 is of degree at least 2. Note, $\beta_2^2 = \alpha^6 - 28\alpha^4 - 196\alpha^2 = \alpha^2(\alpha^4 - 16\alpha^2 + 4) - 12(\alpha^4 - 16\alpha^2 + 4) + 48 = 48$ (note, this is an indirect use of the division algorithm). Thus the minimum polynomial for β_2 is $X^2 - 48$.

(c) Minimum polynomial for β_3: Again, the minimum polynomial for β_3 is of degree at least 2. Note, $\beta_3^2 = \alpha^6 - 36\alpha^4 + 324\alpha^2 = \alpha^2(\alpha^4 - 16\alpha^2 + 4) - 20(\alpha^4 - 16\alpha^2 + 4) + 80 = 80$. Thus, the minimum polynomial for β_3 is $X^2 - 80$.

□

3.18 Show that the polynomial $X^3 + X + 1$ is irreducible over $\mathbb{Z}_2 = \{0, 1\}$, and let α be the element $X + \langle X^3 + X + 1\rangle$ in the field $K = \mathbb{Z}_2/\langle X^3 + X + 1\rangle$. List 8 elements of K, and show that $K\backslash\{0\}$ is a cyclic group of order 7, generated by α.

Solution. We will first show $X^3 + X + 1$ is irreducible over $\mathbb{Z}_2$. Note, $0^3 + 0 + 1 = 1$ and $1^3 + 1 + 1 = 1$, so $X^3 + X + 1$ is irreducible. The 8 elements of K are listed below.

0	a	a^2	a^3	a^4	a^5	a^6	a^7
0	X	X^2	$X+1$	X^2+X	X^2+X+1	X^2+1	1

Associativity, closure, and identity are all inherited from the fact that K is a ring. For $1 \leq n \leq 6$, the inverse of α^n is α^{7-n}. Thus $K\backslash\{0\}$ is a group. □

4 Applications to Geometry

4.1 Ruler and Compasses Constructions

Example. Let A and B be distinct points on a plane and find the perpendicular bisector of AB.

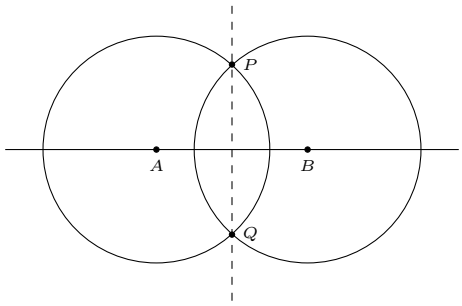


Figure 4.1: Perpendicular bisector of AB

Two circles of the same radius centered as A and B, with radius large enough that the circles intersect at two points. We will call the intersection points P and Q. The line PQ is the perpendicular bisector of AB.

Example. Let A, B be distinct points on the plane, and let C be a point not on the line segment AB. Find a line through C perpendicular to AB. This is called **dropping a perpendicular**.

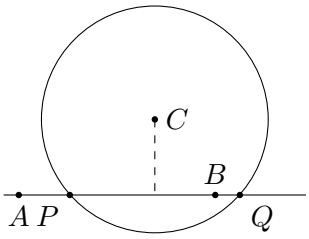


Figure 4.2: Line through C perpendicular to AB

Draw a circle with center C, intersecting the lin AB at points P, Q. Then draw the perpendicular bisector of PQ as in Figure 4.1.

Example. Let A, B be distinct points on the plane. Construct a square on AB.

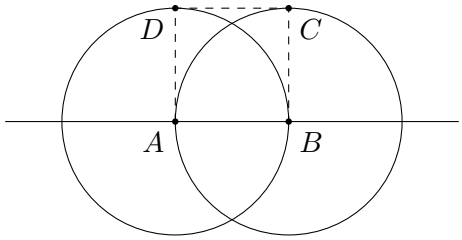


Figure 4.3: Square on AB

Draw circle $\mathcal{K}_1$ with center A, passing through B, and circle $\mathcal{K}_2$ with center B, passing through A. Draw a line perpendicular to AB intersecting AB and point A meeting $\mathcal{K}_1$ at point D. Draw a line perpendicular to AB intersecting AB and point B meeting $\mathcal{K}_2$ at point C. Then $ABCD$ is the required square.

Example. Let L be a line and A a point not on L. Construct a line through A parallel to L.

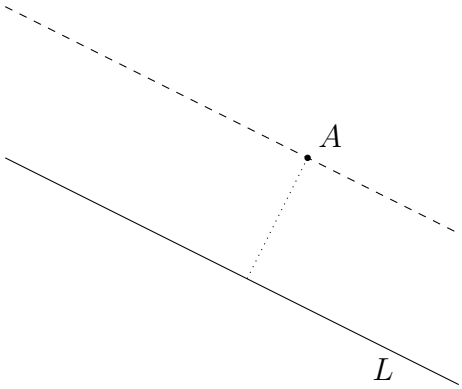


Figure 4.4: Line parallel to L

Drop a perpendicular from A on to the line L, meeting L at the point B. Then draw the perpendicular to the line AB at the point A.

Example. Construct a square equal in area to a given rectangle.

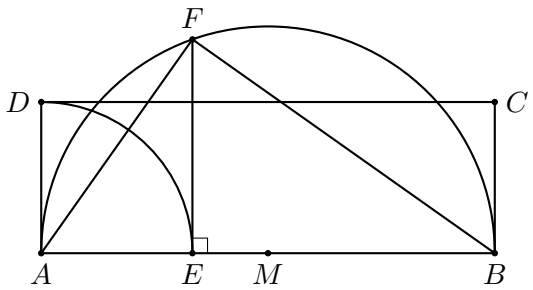


Figure 4.5: Square equal in area to $ABCD$

Suppose that $AD < AB$ Draw a circle with center A passing through D, meeting the line segment AB in E. Let M be the midpoint of AB and draw a circle $\mathcal{K}$ centered at M with diameter AB. Draw the line through E perpendicular to AB, meeting the circle $\mathcal{K}$ in F. The angle AFB is a right angle, and the triangles AFB and AEF are similar. Hence

$$\frac{AE}{AF} = \frac{AF}{AB},$$

and so $AF^2 = AE \cdot AB = AD \cdot AB$. The square constructed on AF has the same area as the rectangle $ABCD$.

4.2 An Algebraic Approach

A cartesian coordinate system in the plane depends on

(i) specifying two axes at right angles to each other, meeting at a point O, the origin;

(ii) choosing a point I, distinct from O, on one of the axes, and giving it coordinates $(1, 0)$.

Let B_0 be the set of points on the plane. There are two permitted operations on the points of B_0:

1. (Ruler) through any two points of B_0, draw a straight line;
2. (Compasses) draw a circle whose center is a point in B_0, and whose radius is the distance between two points in B_0.

Definition 4.1. ⟨ *verb, point* ⟩
Any point which is the intersection of two lines, intersection of two circles, or the intersection of a line and a circle, obtained via ruler and compass operations is said to be **constructed from B_0 in one step**.

Definition 4.2. ⟨ *adjective, point* ⟩
Denote the set $\mathcal{C}(B_0)$ as the set of all points constructed from B_0 in one step. For $n \in \mathbb{N}$, we define

$$B_n = B_{n-1} \cup \mathcal{C}(B_{n-1}).$$

A point is said to be **constructable from** B_0 if it belongs to B_n for some n. A point that is constructable from $\{O, I\}$ is said to be **constructable**.

Theorem 4.3.
Let P be a constructable point, belonging to B_n, where $B_0 = \{(0,0),(1,0)\}$. For $n \in \mathbb{N}^0$, let K_n be the field generated over $\mathbb{Q}$ by the coordinates of points in B_n. Then $[K_n : \mathbb{Q}]$ is a power of 2.

Proof. let K_n be the field generated over $\mathbb{Q}$ by B_n, where $B_0 = \{(0,0),(1,0)\}$. We will show $[K_n : \mathbb{Q}]$ is a power of 2 through induction. Note, K_0 is the field containing the points $(0,0)$ and $(1,0)$, and since there does not exists a $m \in \mathbb{N}$ with $m \neq 0$ such that $m1 = 0$, we know the characteristic of K_0 is 0, and by Theorem 1.48 K_0 is isomorphic to $\mathbb{Q}$ and thus $[K_0 : \mathbb{Q}] = 1 = 2^0$. We suppose inductively that for some $n-1 \in \mathbb{N}$, $[K_{n-1} : \mathbb{Q}] = 2^k$ for some $k \geq 0$. Since $[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : \mathbb{Q}]$ we are only required to show $[K_n : K_{n-1}]$ is a power of 2. There are three cases in which new points in B_n are obtained. They are as follows,

1. the intersection of two lines;
2. the intersection of a line and a circle;
3. the intersection of two circles.

We will break this into cases.

Case 1. Suppose that we have lines AB and CD, where $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, and $D = (d_1, d_2)$ where each are coordinates in B_{n-1}. The equations of the lines are

$$(y - b_2)(a_1 - b_1) = (x - b_1)(a_2 - b_2) \text{ and } (y - d_2)(c_1 - d_1) = (x - d_1)(c_2 - d_2).$$

Their intersection is obtained by solving the equations. Rewriting the equations we have

$$\begin{aligned}
(y - b_2)(a_1 - b_1) &= (x - b_1)(a_2 - b_2) \\
a_1y - b_1y - b_2a_1 + b_2b_1 &= a_2x - b_2x - b_1a_2 + b_1b_2 \\
y(a_1 - b_1) &= x(a_2 - b_2) - b_1a_2 + b_2a_1 \\
y &= x\frac{a_2 - b_2}{a_1 - b_1} + \frac{-b_1a_2 + b_2a_1}{a_1 - b_1},
\end{aligned}$$

and

$$\begin{aligned}(y-d_2)(c_1-d_1) &= (x-d_1)(c_2-d_2)\\ c_1y-d_1y-d_2c_1+d_2d_1 &= c_2x-d_2x-d_1c_2+d_1d_2\\ y(c_1-d_1) &= x(c_2-d_2)-d_1c_2+d_2c_1\\ y &= x\frac{c_2-d_2}{c_1-d_1}+\frac{-d_1c_2+d_2c_1}{c_1-d_1}.\end{aligned}$$

Substituting we can see

$$\begin{aligned}x\frac{a_2-b_2}{a_1-b_1}+\frac{-b_1a_2+b_2a_1}{a_1-b_1} &= x\frac{c_2-d_2}{c_1-d_1}+\frac{-d_1c_2+d_2c_1}{c_1-d_1}\\ x\frac{a_2-b_2}{a_1-b_1}-x\frac{c_2-d_2}{c_1-d_1} &= \frac{-d_1c_2+d_2c_1}{c_1-d_1}-\frac{-b_1a_2+b_2a_1}{a_1-b_1}\\ x\left(\frac{a_2-b_2}{a_1-b_1}-\frac{c_2-d_2}{c_1-d_1}\right) &= \frac{-d_1c_2+d_2c_1}{c_1-d_1}-\frac{-b_1a_2+b_2a_1}{a_1-b_1}\\ x &= \frac{\frac{-d_1c_2+d_2c_1}{c_1-d_1}-\frac{-b_1a_2+b_2a_1}{a_1-b_1}}{\frac{a_2-b_2}{a_1-b_1}-\frac{c_2-d_2}{c_1-d_1}},\end{aligned}$$

and

$$\begin{aligned}y &= x\frac{a_2-b_2}{a_1-b_1}+\frac{-b_1a_2+b_2a_1}{a_1-b_1}\\ y &= \left(\frac{\frac{-d_1c_2+d_2c_1}{c_1-d_1}-\frac{-b_1a_2+b_2a_1}{a_1-b_1}}{\frac{a_2-b_2}{a_1-b_1}-\frac{c_2-d_2}{c_1-d_1}}\right)\left(\frac{a_2-b_2}{a_1-b_1}\right)+\frac{-b_1a_2+b_2a_1}{a_1-b_1}.\end{aligned}$$

It is easy to see the solutions were obtained only using the operations of addition, subtraction, multiplication, and division, and thus take place entirely in K_{n-1}. Thus the coordinates of the intersection of AB and CD lie inside of K_{n-1}.

Case 2. Suppose we have a line AB intersecting a circle centered at C with radius PQ, where A, B, P, Q are points with coordinates in K_{n-1}. The equations of AB and the circle centered at C are as follows,

$$(y-b_2)(a_1-b_1)=(x-b_1)(a_2-b_2) \text{ and } (x-c_1)^2+(y-c_2)^2=r^2,$$

where $r^2 \in K_{n-1}$. Substituting we can see,

$$\begin{aligned}
r^2 &= (x-c_1)^2 + (y-c_2)^2 \\
r^2 &= (x-c_1)^2 + \left(x\frac{a_2-b_2}{a_1-b_1} + \frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2 \right)^2 \\
r^2 &= x^2 - 2xc_1 + c_1^2 + x^2\left(\frac{a_2-b_2}{a_1-b_1}\right)^2 + 2x\frac{a_2-b_2}{a_1-b_1}\left(\frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2\right) \\
&\quad + \left(\frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2\right)^2 \\
0 &= x^2\left[1 + \left(\frac{a_2-b_2}{a_1-b_1}\right)^2\right] + x\left[-2 + \frac{a_2-b_2}{a_1-b_1}\left(\frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2\right)\right] \\
&\quad + \left[c_1^2 + \left(\frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2\right)^2 - r^2\right].
\end{aligned}$$

Thus we have discriminant

$$\Delta = \left[-2+\frac{a_2-b_2}{a_1-b_1}\left(\frac{-b_1a_2+b_2a_1}{a_1-b_1}-c_2\right)\right]^2 - 4\left[1+\left(\frac{a_2-b_2}{a_1-b_1}\right)^2\right]\left[c_1^2+\left(\frac{-b_1a_2+b_2a_1}{a_1-b_1}-c_2\right)^2 - r^2\right].$$

Note, $\Delta \geq 0$ because we assumed the line and circle intersect. It is clear that $\Delta \in K_{n-1}$ because the operations addition, subtraction, multiplication, and division are closed in K_{n-1}. If we let

$$\alpha \coloneqq \left[1 + \left(\frac{a_2-b_2}{a_1-b_1}\right)^2\right] \text{ and } \beta \coloneqq \left[-2 + \frac{a_2-b_2}{a_1-b_1}\left(\frac{-b_1a_2+b_2a_1}{a_1-b_1} - c_2\right)\right]$$

then we have

$$x = \frac{-\beta \pm \sqrt{\Delta}}{2\alpha}.$$

If by chance $\sqrt{\Delta} \in K_{n-1}$, it is clear that x and

$$y = \left(\frac{-\beta \pm \sqrt{\Delta}}{2\alpha}\right)\left(\frac{a_2-b_2}{a_1-b_1}\right) + \frac{-b_1a_2+b_2a_1}{a_1-b_1}$$

are both elements of K_{n-1}. If $\sqrt{\Delta}$ is not in K_{n-1} then the coordinates of the intersection belong to the field $K_{n-1}[\sqrt{\Delta}]$.

Case 3. Assume that we have a circle centered at A with radius r and a circle centered at B with radius s, where $r, s \in K_{n-1}$, and the two circles intersect. We are presented with two equations

$$(x-a_1)^2+(y-a_2)^2=r^2 \text{ and } (x-b_1)^2+(y-b_2)^2=s^2.$$

By subtraction we get

$$\begin{gathered}(x-a_1)^2+(y-a_2)^2-(x-b_1)^2-(y-b_2)^2=r^2-s^2\\ x^2-2xa_1+a_1^2+y^2-2ya_2+a_2^2-x^2+2xb_1-b_1^2-y^2+2yb_2-b_2^2=r^2-s^2\\ x(-2a_1+2b_1)+y(-2a_2+2b_2)+a_1^2+a_2^2-b_1^2-b_2^2=r^2-s^2\\ y(-2a_2+2b_2)=-x(-2a_1+2b_1)+(r^2-s^2-a_1^2-a_2^2+b_1^2+b_2^2)\end{gathered}$$

and thus this is reduced to case 2, and so the coordinates belong to the points of intersection belong to either K_{n-1} or $K_{n-1}[\sqrt{\Delta'}]$.

We conclude the points of K_n either belong to K_{n-1} or $K_{n-1}[\sqrt{\Delta}]$ for some $\Delta \in K_{n-1}$. Therefore, $K_n = K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_l})$ for $l \geq 0$. We will now show that

$$[K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_l}) : K_{n-1}]$$

is a power of 2 through induction. If $\sqrt{\Delta_1} \in K_{n-1}$ then $[K_{n-1}(\sqrt{\Delta_1}) : K_{n-1}] = 1$. If not, then the minimum polynomial for $\sqrt{\Delta_1}$ is $m_1 = X^2 - \Delta_1$ thus $[K_{n-1}(\sqrt{\Delta_1}) : K_{n-1}] = 2$. Now suppose for some $1 \leq j \leq l-1$ we have

$$[K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}}) : K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-2}})]$$

is a power of 2. Note, either $\sqrt{\Delta_j} \in K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}})$ or not. If $\sqrt{\Delta_j} \in K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-2}})$ then we have

$$[K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}}) : K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-2}})] = 1.$$

Otherwise, the minimum polynomial for $\sqrt{\Delta_j}$ is $m_j = X^2 - \Delta_j$ and thus

$$[K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}}) : K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-2}})] = 2.$$

Therefore,

$$[K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_j}) : K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}})]$$

is a power of 2 for $1 \leq j \leq l$. Thus

$$\begin{aligned} K_n &= [K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_l}) : K_{n-1}] \\ &= \prod_{j=1}^{l} [K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_j}) : K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_{j-1}})] \\ &= 2^d \end{aligned}$$

for some $d \in \mathbb{N}^0$. Therefore $[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : \mathbb{Q}] = 2^{d+k}$ which is a power of two. Therefore for all $n \in \mathbb{N}$, $[K_n : \mathbb{Q}]$ is a power of two. □

Exercises

4.1

4.2

4.3

4.4

5 Splitting Fields

Definition 5.1. ⟨ *adjective, field* ⟩
Let E be an extension of a field K and let f be a polynomial in $K[X]$ of degree $n \geq 1$. We say f **splits completely** over E if there exist elements, $a \in K$, $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ such that

$$f = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Below lie a few examples and non-examples of polynomials splitting completely.

- Consider the irreducible polynomial $f = X^2 - 2$ over $\mathbb{Q}$. Over the field extension $[\mathbb{R} : \mathbb{Q}]$, we are now able to factor f as such

$$f = X^2 - 2 = (X + \sqrt{2})(X - \sqrt{2}).$$

  We say that f splits completely over $\mathbb{R}$.

- Consider the polynomial $g = X^3 - 1$ over $\mathbb{Q}$. Note, g is reducible over $\mathbb{Q}$ as we can factorize g like so

$$g = X^3 - 1 = (X - 1)(X^2 + X + 1).$$

  Over the field extension $\mathbb{Q}[-\frac{1}{2} + i\frac{\sqrt{3}}{2}] = \mathbb{Q}[e^{\frac{2i\pi}{3}}]$ the polynomial g splits completely,

$$g = (X - 1)(X - e^{\frac{2i\pi}{3}})(X - e^{\frac{-2i\pi}{3}}).$$

- Consider the polynomial $h = 3X^2 - 19X - 14$ over the field $\mathbb{Q}$. Note,

$$h = 3X^2 - 19X - 14 = (3X + 2)(X - 7) = 3\Big(\frac{1}{3}X + \frac{2}{3}\Big)(X - 7)$$

  so h splits completely over $\mathbb{Q}$.

- Consider the polynomial $k = X^4 - 4$ over $\mathbb{Q}$. The polynomial k can be split into factors $k = (X^2 - 2)(X^2 + 2)$ over $\mathbb{Q}$ but can not be split further. Consider the field extension $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$. The polynomial k does **not** split completely over $\mathbb{Q}[\sqrt{2}]$. Over $\mathbb{Q}[\sqrt{2}]$, k splits into

$$k = (X - \sqrt{2})(X + \sqrt{2})(X^2 + 2),$$

  but to split completely, the field extension $\mathbb{Q}[i\sqrt{2}]$ must be considered.

Definition 5.2. ⟨ *noun, field extension* ⟩
Let K be a field and let f be a polynomial in $K[X]$. We say that an extension L of K is a **splitting field** for f over K, that $L : K$ is a **splitting field extension**, if

(i) f splits completely over L;

(ii) f does not split completely over any subfield E of L.

Consider the polynomials f, g, h, k and field extensions described previously.

- The field $\mathbb{Q}[e^{\frac{2i\pi}{3}}]$ is a splitting field for $g = X^3 - 1$ over $\mathbb{Q}$ because there is no subfield of $\mathbb{Q}[e^{\frac{2i\pi}{3}}]$ over which g splits completely.
- The field $\mathbb{Q}$ is a splitting field for the polynomial $h = 3X^2 - 19X - 14 = 3(\frac{1}{3}X + \frac{2}{3})(X - 7)$ over $\mathbb{Q}$.
- The field $\mathbb{Q}[i\sqrt{2}]$ is a splitting field for $k = X^4 - 4$ over $\mathbb{Q}$. The polynomial k splits as such
$$k = (X - \sqrt{2})(X + \sqrt{2})(X - i\sqrt{2})(X + i\sqrt{2}).$$
- The polynomial $f = X^2 - 2$ is irreducible over $\mathbb{Q}$, but splits completely over the field extension $[\mathbb{R} : \mathbb{Q}]$. The field $\mathbb{R}$ is **not** called a splitting field for f because there are subfields of $\mathbb{R}$ for which f splits completely. The smallest field for which f splits completely is $\mathbb{Q}[\sqrt{2}]$. We say $\mathbb{Q}[\sqrt{2}]$ is a splitting field for f over $\mathbb{Q}$.

Theorem 5.3.
Let K be a field and let $f \in K[X]$ have degree n. Then there exists a splitting field L for f over K, and $[L : K] \leq n!$.

Proof. Let K be a field and let $f \in K[X]$ have degree n. The polynomial f must have at least one irreducible factor g. By Theorem 3.26 we can form the field $E_1 = K[X]/\langle g \rangle$ and $\alpha = X + \langle g \rangle$ has a minimum polynomial g over K. Then $g(\alpha) = 0$ so g has a linear factor $Y - \alpha$ in the polynomial ring $E_1[Y]$. Additionally, $[E_1 : K] = \partial g \leq n$. We now proceed inductively, suppose for each $1 \leq r \leq n - 1$ we have constructed an extension E_r of K such that f has at least r linear factors in $E_r[X]$, and

$$[E_r : K] \leq n(n-1)\cdots(n-r+1).$$

Thus, in $E_r[X]$,

$$f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_r) f_r,$$

and $\partial f_r = n - r$. Suppose f_r has irreducible factor g_r. We can construct a field $E_{r+1} = E_r/\langle g_r \rangle$ and let $\alpha_{r+1} = X + \langle g_r \rangle$. Then g_r has the linear factor $X - \alpha_{r+1}$, and $[E_{r+1} : E_r] = \partial g_r \leq n - r$. Thus,

$$[E_{r+1} : K] = [E_{r+1} : E_r][E_r : K] \leq n(n-1) \cdots (n-r).$$

Hence, by induction, there exists a field E_n such that f splits completely over E_n, and $[E_n : K] \leq n!$. Now let $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq E_n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f in E_n (and not necessarily distinct). Then f splits completely over L, and cannot split completely over any proper subfield of L. Additionally, since $L \subseteq E_n$ we have $[L : K] \leq [E_n : K]$. Therefore, we have a splitting field L for f over K with $[L : K] \leq n!$, as desired. □

Example. Consider the polynomial

$$f = X^5 + X^4 - X^3 - 3X^2 - 3X + 3$$

in $\mathbb{Q}[X]$ which has two irreducible factors,

$$f = (X^3 - 3)(X^2 + X - 1).$$

Let $\alpha = \sqrt[3]{3}$, and let $\gamma = \frac{-1+\sqrt{5}}{2}, \delta = \frac{-1-\sqrt{5}}{2}$ be the roots of $X^2 + X - 1$. Following the steps in the proof of Theorem 5.3 we construct the following,

$$\begin{aligned}
&E_1 = \mathbb{Q}(\alpha), && f = (X - \alpha)(X^2 + \alpha X + \alpha^2)(X^2 + X - 1),\\
&E_2 = E_1(\alpha e^{\frac{2i\pi}{3}}), && f = (X - \alpha)(X - \alpha e^{\frac{2i\pi}{3}})(X - \alpha e^{\frac{4i\pi}{3}})(X^2 + X - 1),\\
&E_3 = E_2(\alpha e^{\frac{4i\pi}{3}}), && f = (X - \alpha)(X - \alpha e^{\frac{2i\pi}{3}})(X - \alpha e^{\frac{4i\pi}{3}})(X^2 + X - 1),\\
&E_4 = E_3(\gamma), && f = (X - \alpha)(X - \alpha e^{\frac{2i\pi}{3}})(X - \alpha e^{\frac{4i\pi}{3}})(X - \gamma)(X - \delta),\\
&E_5 = E_4(\delta), && f = (X - \alpha)(X - \alpha e^{\frac{2i\pi}{3}})(X - \alpha e^{\frac{4i\pi}{3}})(X - \gamma)(X - \delta).
\end{aligned}$$

We have

$$[E_1 : \mathbb{Q}] = 3, \quad [E_2 : E_1] = 2, \quad [E_3 : E_2] = 1, \quad [E_4 : E_3] = 2, \quad [E_5 : E_4] = 1,$$

thus $[E_5 : \mathbb{Q}] = 12 \leq 5! = 120$. The field

$$E_5 = \mathbb{Q}(\alpha, \alpha e^{\frac{2i\pi}{3}}, \alpha e^{\frac{4i\pi}{3}}, \gamma, \delta) = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3}, \sqrt{5})$$

is a splitting field for f.

Example. Consider the polynomial $f = X^3 - 2$ over $\mathbb{Q}$. We will determine the splitting field for f, and degree of the extension. Let $\alpha = \sqrt[3]{2}$. We can express f in linear factors as follows,

$$f = (X - \alpha)(X - \alpha e^{\frac{2i\pi}{3}})(X - \alpha e^{\frac{4i\pi}{3}}).$$

Thus f splits completely over the field $\mathbb{Q}(\alpha, \alpha e^{\frac{2i\pi}{3}}, \alpha e^{\frac{4i\pi}{3}}) = \mathbb{Q}(\alpha, e^{\frac{2i\pi}{3}})$. Note, the minimum polynomial for α is f, which has degree 3. The extension $\mathbb{Q}(\alpha) : \mathbb{Q}$ has degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Note, the minimum polynomial of $e^{\frac{2i\pi}{3}}$ over $\mathbb{Q}[\alpha]$ is

$$f_1 = X^2 + X + 1,$$

which is of degree 2. Thus $[\mathbb{Q}(\alpha, e^{\frac{2i\pi}{3}}) : \mathbb{Q}(\alpha)] = 2$. Therefore,

$$[\mathbb{Q}(\alpha, e^{\frac{2i\pi}{3}}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, e^{\frac{2i\pi}{3}}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!$$

and the splitting field for f is $\mathbb{Q}(\alpha, e^{\frac{2i\pi}{3}})$. This example illustrates there are polynomials of degree n, where the degree of the extension of their splitting field is $n!$.

Theorem 5.4.
Let K and K' be fields, and let $\varphi : K \to K'$ be an isomorphism, extending to an isomorphism $\hat{\varphi} : K[X] \to K'[X]$. Let $f \in K[X]$, and let L, L' be splitting fields of f over K and $\hat{\varphi}(f)$ over $K'[X]$, respectively. Then there is an isomorphism $\varphi^* : L \to L'$ extending φ.

Proof. Let K and K' be fields, and let $\varphi : K \to K'$ be an isomorphism, extending to an isomorphism $\hat{\varphi} : K[X] \to K'[X]$. Let $f \in K[X]$ with $\partial f = n$, and let L, L' be splitting fields of f over K and $\hat{\varphi}(f)$ over $K'[X]$, respectively. We will show there is an isomorphism $\varphi^* : L \to L'$ extending φ.

Suppose that in $L[X]$ we have the factorization,

$$f = \alpha(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

where α, the leading coefficient, lies in K, and $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Suppose for some $0 \leq m \leq n$ the roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ are not in K, and $\alpha_{m+1}, \ldots, \alpha_n$ are in K. We will prove the theorem by induction on m. If $m = 0$ then all the roots are in K, so K itself is a splitting

field for f. Hence, in $K'[X]$, we have

$$\hat{\varphi} = \varphi(\alpha)(X - \varphi(\alpha_1))(X - \varphi(\alpha_2)) \cdots (X - \varphi(\alpha_n)),$$

thus K' is a splitting field for $\hat{\varphi}$, and $\varphi^* = \varphi$ is our isomorphism. Suppose inductively that for some $m > 0$ every field E and every polynomial $g \in E[X]$ having fewer than m roots outside of E is a splitting field L of g, every isomorphism of E can be extended to an isomorphism of L. Our assumption that $m > 0$ assures that the irreducible factors of f in $K[X]$ are not all linear. Let f_1 be a non-linear irreducible factor of f. Then $\hat{\varphi}(f_1)$ is an irreducible factor of $\hat{\varphi}(f)$ in K'. The roots of f_1 in the splitting field L are included among the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, and we may suppose, without loss of generality, that α_1 is a root of f_1. Similarly, the list $\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n)$ of roots of $\hat{\varphi}(f_1)$ includes the root $\beta_1 = \varphi(\alpha_i)$ of $\hat{\varphi}(f_1)$ for some i. By Theorem 3.27 there is an isomorphism $\varphi' : K(\alpha_1) \to K'(\beta_1)$ extending φ. Since f now has fewer than m roots outside $K(\alpha_1)$, the inductive hypothesis asserts the existence of an isomorphism $\varphi^* : L \to L'$ extending $\varphi' : K(\alpha_1) \to K'(\beta_1)$, and hence extending $\varphi : K \to K'$.

□

Example. Consider the polynomial ring $\mathbb{Z}_3[X]$ taking $\mathbb{Z}_3 = \{0, 1, -1\}$. There are 9 quadratic monic polynomials

$$\begin{array}{lll} X^2, & X^2 + 1, & X^2 - 1, \\ X^2 + X, & X^2 + X + 1, & X^2 + X - 1, \\ X^2 - X, & X^2 - X + 1, & X^2 - X - 1. \end{array}$$

The quadratic irreducible polynomials are

$$X^2 + 1, \quad X^2 + X - 1, \quad \text{and} \quad X^2 - X - 1.$$

Over the field $L_1 \coloneqq \mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ contains an element $\alpha \coloneqq X + \langle X^2 + 1\rangle$ such that $\alpha^2 + 1 = 0$. In the ring $L_1[X]$ the polynomial $X^2 + 1$ splits completely as

$$(X - \alpha)(X + \alpha),$$

and L_1 is the splitting field for $X^2 + 1$. Similarly, the fields $L_2 \coloneqq \mathbb{Z}_3[X]/\langle X^2 + X - 1\rangle$ and $L_3 \coloneqq \mathbb{Z}_3[X]/\langle X^2 - X - 1\rangle$ are the splitting fields for $X^2 + X - 1$ and $X^2 - X - 1$, respectively.

Exercises

5.1 Determine the degree of the splitting fields over $\mathbb{Q}$ of the following polynomials and find their degrees over $\mathbb{Q}$,

(a) $f_1 = X^4 - 5X^2 + 6$

Solution. Note, f_1 factorizes into $f_1 = (X^2 - 2)(X^2 - 3)$ over $\mathbb{Q}$ and splits completely over $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. The degree is 4.

□

(b) $f_2 = X^4 - 1$

(c) $f_3 = X^4 + 1$

5.2 Determine the splitting fields over $\mathbb{Q}$ of the following polynomials, and find their degrees over $\mathbb{Q}$:

(a) $f_1 = X^6 - 1$;

Solution. Note, f_1 factorizes over $\mathbb{C}$ as

$$f_1 = (X-1)(X+1)(X - e^{\frac{\pi i}{3}})(X - e^{\frac{2\pi i}{3}})(X - e^{\frac{4\pi i}{3}})(X - e^{\frac{5\pi i}{3}}).$$

So f_1 splits completely over $\mathbb{C}$, but the splitting field is $\mathbb{Q}(i\sqrt{3})$. The minimum polynomial of $i\sqrt{3}$ is $X^2 + 3$, hence the degree of the extension over $\mathbb{Q}$ is 2. □

(b) $f_2 = X^6 + 1$;

Solution. Note, f_2 factorizes completely over $\mathbb{C}$ as

$$f_2 = (X-i)(X+i)(X - e^{\frac{\pi i}{6}})(X - e^{\frac{5\pi i}{6}})(X - e^{\frac{7\pi i}{6}})(X - e^{\frac{11\pi i}{6}}).$$

So f_2 splits completely over $\mathbb{C}$ but the splitting field is $\mathbb{Q}(i, \sqrt{3})$. The minimum polynomial for i over $\mathbb{Q}$ is $X^2 + 1$, and the minimum polynomial for $\sqrt{3}$ over $\mathbb{Q}(i)$ is $X^2 - 3$, thus the degree of the extension is 4. □

(c) $f_3 = X^6 - 27$.

5.3

5.4

6 Finite Fields

Definition 6.1. ⟨ *adjective, field* ⟩
Let $f = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial with coefficients in a field K. The **formal derivative** Df of f is defined by

$$Df = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

Theorem 6.2.
Let $f, g \in K[X]$ where K is a field, and let $k \in K$. The following formulae hold,

(i) $D(kf) = k(Df)$;

(ii) $D(f + g) = Df + Dg$;

(iii) $D(fg) = (Df)g + f(Dg)$.

Theorem 6.3. Classification of Finite Fields:

(i) Let K be a finite field. Then $|K| = p^n$ for some prime p and some integer $n \geq 1$. Every element of K is a root of the polynomial $X^{p^n} - X$, and K is a splitting field of this polynomial over the prime subfield $\mathbb{Z}_p$.

(ii) Let p be a prime, and let $n \geq 1$ be an integer. There exists, up to isomorphism, exactly one field of order p^n.

Definition 6.4. ⟨ *adjective, field* ⟩
By Theorem 6.3 we have that for a given prime p and integer n, up to isomorphism, there is exactly one field of order p^n, we call this field the **Galois field** of order p^n, denoted $\mathrm{GF}(p^n)$.

Theorem 6.5.
The group of non-zero elements of the Galois field $\mathrm{GF}(p^n)$ is cyclic.

Definition 6.6. ⟨ *adjective, field* ⟩
Let G be a group. The **exponent** $e = e(G)$ is the smallest positive integer such that $a^e = 1$ for all $a \in G$.

Theorem 6.7.
Let G be a finite abelian group with exponent e. There exists an element $a \in G$ such that $o(a) = e$.

Corollary 6.8.
If G is a finite abelian group such that $e(G) = |G|$, then G is cyclic.

Exercises

6.1 Let f, g be polynomials over a field K, with $\partial f = m$, $\partial g = n$.

(i) Show that $D(f+g) = Df + Dg$.

Proof. Note, if $m = n$ then we have

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n,$$

and thus

$$\begin{aligned} D(f+g) &= (a_1 + b_1) + 2(a_2 + b_2)X + \cdots + n(a_n + b_n)X^{n-1} \\ &= a_1 + 2a_2X + \cdots + na_nX^{n-1} + b_1 + 2b_2X + \cdots + nb_nX^{n-1} \\ &= Df + Dg. \end{aligned}$$

Now we will show this holds for $m \neq n$. Without loss of generality suppose $m > n$. Note,

$$f + g = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n + \cdots + (a_m)X^m.$$

We have

$$\begin{aligned} D(f+g) &= (a_1 + b_1) + 2(a_2 + b_2)X + \cdots + n(a_n + b_n)X^{n-1} + \cdots + m(a_m)X^{m-1} \\ &= a_1 + 2a_2X + \cdots + na_nX^{n-1} + \cdots + ma_mX^{m-1} + b_1 + 2b_2X + \cdots + nb_nX^{n-1} \\ &= Df + Dg. \end{aligned}$$

Therefore, $D(f+g) = Df + Dg$. □

(ii) Show, by induction on $m+n$, that

$$D(fg) = (Df)g + f(Dg). \tag{6.1}$$

Proof. □

6.2 Show by induction on n that $D[(X-\alpha)^n] = n(X-\alpha)^{n-1}$.

Proof. Note, $D(X-\alpha) = 1$. Thus $D[(X-\alpha)^n] = n(X-\alpha)^{n-1}$ holds for $n = 1$. Now suppose it holds for some $k \in \mathbb{N}$. Note,

$$\begin{aligned} D[(X-\alpha)^{n+1}] &= D[(X-\alpha)(X-\alpha)^n] \\ &= D[(X-\alpha)](X-\alpha)^n + (X-\alpha)D[(X-\alpha)^n] \\ &= (X-\alpha)^n + n(X-\alpha)(X-\alpha)^{n-1} \\ &= (X-\alpha)^n + n(X-\alpha)^n \\ &= (n+1)(X-\alpha)^n. \end{aligned}$$

Therefore, if $D[(X-\alpha)^n] = n(X-\alpha)^{n-1}$ holds for $n = k$ then $D[(X-\alpha)^n] = n(X-\alpha)^{n-1}$ holds for $k+1$. Therefore, for all $n \in \mathbb{N}$, $D[(X-\alpha)^n] = n(X-\alpha)^{n-1}$. □

6.3

6.4

6.5 Show that $f = X^4 + X + 1$ is irreducible over $\mathbb{Z}_2$ and list the powers of the element $\alpha = X + \langle X^4 + X + 1\rangle$ of $\mathbb{Z}_2/\langle X^4 + X + 1\rangle$.

Proof. Consider $\mathbb{Z}_2 \coloneqq \{0, 1\}$. Note, $1^4 + 1 + 1 = 1 + (1 + 1) = 1 + 0 = 1 \neq 0$ and $0^4 + 0 + 1 = 1 \neq 0$. Thus neither X nor $X - 1$ divide f. The quadratic polynomials in $\mathbb{Z}_2[X]$ are X^2, $X^2 + 1$, $X^2 + X$, and $X^2 + X + 1$. The first three are irreducible into linear factors, and since f has no linear factors the only possibility for the factorization of f would be $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ which is not equal to f. Thus f must be irreducible. □

We will now list the powers of $\alpha = X + \langle X^4 + X + 1\rangle$[6].

[6]Answers here do not align with the book. Computational evidence suggests answers here are correct, visit `https://github.com/nathaniel-k-green/galois_programs/blob/main/quotient_rings.sage` to verify.

n	1	2	3	4	5	6	7	8
a^n	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha+1$	α^2+1

n	9	10	11	12	13	14
a^n	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+1$	α^3+1	1

6.6 Let K be a field with non-zero characteristic p.

(i) Show that the mapping $\varphi : K \to K$ given by

$$\varphi(a) = a^p$$

is a monomorphism (called the **Frobenius monomorphism**). Show that φ is an automorphism if K is a finite, and that φ is the identity map if $K = \mathbb{Z}_p$.

Proof. First we will show that φ is a monomorphism. Let $a, b \in K$. Note, $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$, thus φ preserves multiplication. Note, $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$ by Theorem 1.50. Thus φ is a homomorphism. Now suppose $\varphi(a) = \varphi(b)$. We have that $a^p = b^p \implies a^p - b^p = 0 \implies (a-b)^p = 0$ which means $a - b = 0$ by modification of Theorem 1.50 (as done in exercises). Therefore, φ is a monomorphism. If K is finite then $|K| = |\varphi(K)|$ and since φ is injective φ must also be surjective, hence φ is an automorphism.

Suppose $K = \mathbb{Z}_p$. Note, by Theorem 6.3 we have that for all $a \in K$, $a^p - a = 0$ and thus φ is the identity map. □

(ii) Give an example of an infinite K where φ does not map onto K.

6.7

7 The Galois Group

7.1 Monomorphisms between Fields

Let K be a field and let S be a non-empty set. Let $\mathcal{M}$ be the set of mappings from S into K. For $\theta, \varphi \in \mathcal{M}$, we define addition by

$$(\theta + \varphi)(s) = \theta(s) + \varphi(s),$$

and so $\theta + \varphi \in \mathcal{M}$. Similarly, if $\theta \in \mathcal{M}$ and $a \in K$, then $a\theta$ defined by

$$(a\theta)(s) = a\theta(s)$$

belongs to $\mathcal{M}$. It is easy to verify that $\mathbb{M}$ is a vector space with respect to these two operations, and the zero vector is $\zeta(s) = 0$.

Theorem 7.1.
Let K and L be fields and let $\theta_1, \theta_2, \ldots, \theta_n$ be distinct monomorphisms from K into L. Then $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a linearly independent set in the vector space $\mathcal{M}$ of all mappings from K into L.

Proof. Let K and L be fields and let $\theta_1, \theta_2, \ldots, \theta_n$ be distinct monomorphisms from K into L. We will show $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a linearly independent set in the vector space $\mathcal{M}$ of all mappings from K into L. Note, for $a_1 \in L$, $a_1\theta_1(s) = 0$ for all $s \in K$ is clearly true if and only if $a_1 = 0$ since θ_1 is injective. Suppose inductively that for each k with $1 \leq k \leq n-1$, $\{\theta_1, \theta_2, \ldots, \theta_k\}$ is a linearly independent set. Now suppose by way of contradiction, there exist $a_1, a_2, \ldots, a_n \in L$ such that

$$a_1\theta_1 + a_2\theta_2 + \cdots + a_n\theta_n = 0 \tag{7.1}$$

where for some i, $a_i \neq 0$. Note, if some $a_i = 0$ then we have would have a set of $n-1$ mappings that are not linearly independent, which contradicts our assumption. Thus there shall be no i such that $a_i = 0$. Dividing 7.1 by a_n we get

$$b_1\theta_1 + b_2\theta_2 + \cdots + b_{n-1}\theta_{n-1} + \theta_n = 0 \tag{7.2}$$

where $b_i = \frac{a_i}{a_n}$. Note, since each θ_i is distinct, there must be some $u \in K$ such that

$\theta_1(u) \neq \theta_n(u)$. Thus for all $z \in K$ we have

$$\begin{aligned} 0 &= b_1\theta_1(uz) + b_2\theta_2(uz) + \cdots + b_{n-1}\theta_{n-1}(uz) + \theta_n(uz) \\ &= b_1\theta_1(u)\theta_1(z) + b_2\theta_2(u)\theta_2(z) + \cdots + b_{n-1}\theta_{n-1}(u)\theta_{n-1}(z) + \theta_n(u)\theta_n(z). \end{aligned}$$

Dividing by $\theta_n(u)$ we have

$$\frac{b_1\theta_1(u)}{\theta_n(u)}\theta_1(z) + \frac{b_2\theta_2(u)}{\theta_n(u)}\theta_2(z) + \cdots + \frac{b_{n-1}\theta_{n-1}(u)}{\theta_n(u)}\theta_{n-1}(z) + \theta_n(z) = 0 = \zeta(z). \tag{7.3}$$

Subtracting 7.3 from 7.2 we get

$$\begin{aligned} 0 &= b_1\theta_1 + b_2\theta_2 + \cdots + b_{n-1}\theta_{n-1} + \theta_n - \zeta \\ &= b_1\left(1 - \frac{\theta_1(u)}{\theta_n(u)}\right)\theta_1(z) + b_2\left(1 - \frac{\theta_2(u)}{\theta_n(u)}\right)\theta_2(z) + \cdots + b_{n-1}\left(1 - \frac{\theta_{n-1}(u)}{\theta_n(u)}\right)\theta_{n-1}(z), \end{aligned}$$

and since $\theta_1(u) \neq \theta_n(u)$ we have $b_1\big(1 - \frac{\theta_1(u)}{\theta_n(u)}\big) \neq 0$. This implies the set $\{\theta_1, \theta_2, \cdots, \theta_{n-1}\}$ is not linearly independent, which is a contradiction. Therefore, the set $\{\theta_1, \theta_2, \cdots, \theta_n\}$ is linearly independent. □

7.2 Automorphisms, Groups, and Subfields

Theorem 7.2.
Let K be a field. Then the set $\operatorname{Aut} K$ of automorphisms of K forms a group under composition of mappings.

Definition 7.3. ⟨ *noun, group* ⟩
We refer to the group $\operatorname{Aut} K$ as the **group of automorphisms** of K.

Definition 7.4. ⟨ *noun, automorphism* ⟩
Let L be an extension of a field K. An automorphism α of L is called a K-**automorphism** if $\alpha(x) = x$ for all $x \in K$

Definition 7.5. ⟨ *noun, group* ⟩
Let L be an extension of a field K. The set of all K-automorphisms of L is denoted $\operatorname{Gal}(L : K)$ and is called the **Galois group of L over K**.

Definition 7.6. ⟨ *noun, group* ⟩
Let L be an extension of a field K. The **Galois group of a polynomial** $f \in K[X]$, denoted by $\mathrm{Gal}(f)$, is defined as $\mathrm{Gal}(L : K)$ where L is a splitting field of f over K.

Definition 7.7. ⟨ *noun, set* ⟩
Let $L : K$ be a field extension of a field K, let E be a subfield of L containing K, and let H be a subgroup of $\mathrm{Gal}(L : K)$. For E we define

$$\Gamma(E) \coloneqq \{\alpha \in \mathrm{Aut}\ L : \alpha(z) = z \text{ for all } z \in E\};$$

and for H we define

$$\Phi(H) \coloneqq \{x \in L : \alpha(x) = x \text{ for all } \alpha \in H\}.$$

Theorem 7.8.
Let $L : K$ be a field extension. Then the set $\mathrm{Gal}(L : K)$ of all K-automorphisms of L is a subgroup of $\mathrm{Aut}\, K$.

Proof. Let $L : K$ be a field extension, and let $\mathrm{Gal}(L : K)$ be the set of all K-automorphisms of L. We will show $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}\, K$. First, the identity map ι is clearly in $\mathrm{Gal}(L : K)$. Additionally, $\mathrm{Gal}(L : K)$ is a subset of $\mathrm{Aut}\, K$ by definition. Now let $\alpha, \beta \in \mathrm{Gal}(L : K)$. Note, for all $x \in K$,

$$x = \beta^{-1}(\beta(x)) = \beta^{-1}(x),$$

and so we have $\alpha(\beta^{-1}(x)) = \alpha(x) = x$ and so $\alpha \circ \beta^{-1} \in \mathrm{Gal}(L : K)$. By the definition of a subgroup, $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}\, K$. □

Theorem 7.9.
Let $L : K$ be a field extension.

(i) For every subfield E of L containing K, the set $\Gamma(E)$ is a subgroup of $\mathrm{Gal}(E)$.

(ii) For every subgroup H of $\mathrm{Gal}(L : K)$, the set $\Phi(H)$ is a subfield of L.

Theorem 7.10.
Let $L : K$ be a field extension.

(i) If E_1 and E_2 are subfields of L containing K, then

$$E_1 \subseteq E_2 \implies \Gamma(E_1) \supseteq \Gamma(E_2).$$

(ii) If H_1 and H_2 are subgroups of $\mathrm{Gal}(L : K)$, then

$$H_1 \subseteq H_2 \implies \Phi(H_1) \supseteq \Phi(H_2).$$

Theorem 7.11.
Let K be a field, let L be an extension of K, and let $z \in L \backslash K$. If z is a root of a polynomial f with coefficients in K, and if $\alpha \in \mathrm{Gal}(L : K)$, then $\alpha(z)$ is also a root of f.

Definition 7.12. ⟨ *noun, correspondence* ⟩
The mappings Φ and Γ together are known as the **Galois correspondence**.

Theorem 7.13.
Let L be an extension of a field K, let E be a subgroup of L containing K, and let H be a subgroup of $\mathrm{Gal}(L : K)$. Then,

$$E \subseteq \Phi(\Gamma(E)), \quad H \subseteq \Gamma(\Phi(H)).$$

Theorem 7.14.
Let L be a finite extension of a field K, and let G be a finite subgroup of $\mathrm{Gal}(L : K)$. Then $[L : \Phi(G)] = |G|$.

7.3 Normal Extensions

Definition 7.15. ⟨ *adjective, field extension* ⟩
A field extension $L : K$ is said to be **normal** if every irreducible polynomial in $K[X]$ with at least one root in L splits completely over L.

Theorem 7.16.
A finite extension L of a field K is normal if and only if it is a splitting field for some polynomial in $K[X]$.

Corollary 7.17.
Let L be a normal extension of finite degree over a field K, and let E be a subfield of L containing K. Then every K-monomorphism from E into L can be extended to a K-automorphism of L

Corollary 7.18.
Let L be a normal extension of finite degree over a field K. If z_1 and z_2 are roots in L of an irreducible polynomial in $K[X]$, then there exists a K-automorphism θ of L such that $\theta(z_1) = z_2$.

Definition 7.19. $\langle$ *adjective, field extension* $\rangle$
If L is a field extension of a field K, a field N containing L is said to be a **normal closure of L over K** if

(i) it is a normal extension of K; and

(ii) if E is a proper subfield of N containing L, then E is not a normal extension of K.

Theorem 7.20.
Let L be a finite field extension of a field K. Then,

(i) there exists a normal closure N of L over K;

(ii) if L' is a finite extension over K such that there is a K-isomorphism $\varphi : L \to L'$, and if N' is a normal closure of L' over K, then there is a K-isomorphism $\psi : N \to N'$ such that the diagram

$$\begin{array}{ccccc} K & \longrightarrow & L & \longrightarrow & N \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ K & \longrightarrow & L' & \longrightarrow & N' \end{array}$$

(where ι denotes the identity map and unmarked maps are inclusions) commutes.

Corollary 7.21.
Let L be a finite extension of K and let N be a normal closure of L. Then

$$N = L_1 \vee L_2 \vee \cdots \vee L_k,$$

where $L_1, L_2, \cdots, L_k$ are subfields containing K, each term of them isomorphic to L.

Theorem 7.22.
Let L be a finite normal extension of a field K, and let E be a subfield of L containing K. Then E is a normal extension of K if and only if every K-isomorphism of E into L is a K-automorphism of E.

7.4 Separable Extensions

Definition 7.23. ⟨ *adjective, polynomial* ⟩
An irreducible polynomial f with coefficients in a field K is said to be **separable over** K if it has no repeated roots in a splitting field. That is, in a splitting field L of f,

$$f = k(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n),$$

where the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all distinct.

Definition 7.24. ⟨ *adjective, polynomial* ⟩
A polynomial g with coefficients in a field K is called **separable over** K if all its irreducible factors are separable over K.

Definition 7.25. ⟨ *adjective, element* ⟩
An algebraic element in an extension L of a field K is called **separable over** K if its minimum polynomial is separable over K.

Definition 7.26. ⟨ *adjective, field extension* ⟩
An extension L of a field K is called **separable** if every α in L is separable over K.

Definition 7.27. ⟨ *adjective, field* ⟩
A field K is called **perfect** if every polynomial in $K[X]$ is separable over K.

Theorem 7.28.
Let K be a field. If every irreducibly polynomial is separable over K, then K is perfect.

Proof. Let K be a field and suppose every irreducible polynomial is separable over K. Let f be a polynomial over K. Note, $f = f_1 f_2 \cdots f_n$ for some $n \in \mathbb{N}$, where each f_i is an irreducible polynomial. By assumption, f_i is separable. Hence, f is separable. Therefore, K is perfect. □

Theorem 7.29.
Let f be an irreducible polynomial with coefficients in a field K.

(i) If K has characteristic 0, then f is separable over K.

(ii) If K has finite characteristic p, then f is separable unless it is of the form

$$b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp}.$$

Corollary 7.30.
Every field of characteristic 0 is perfect.

Theorem 7.31.
Let K be a field with finite characteristic p, and let

$$f(X) = g(X^p) = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp}.$$

The following are equivalent:

(i) f is irreducible in $K[X]$;

(ii) g is irreducible in $K[X]$, and there exists a coefficient b_i that is not a pth power of an element in K.

Theorem 7.32.
Every finite field is perfect.

Theorem 7.33.
Let L be a finite separable extension of a field K, and let E be a subfield of L containing K. Then L is a separable extension of E.

7.5 The Galois Correspondence

Definition 7.34. ⟨ *noun, field extension* ⟩
A finite extension of a field K that is both normal and separable is called a **Galois extension**.

Theorem 7.35.
Let $L : K$ be a separable extension of finite degree n. Then there are precisely n distinct K-monomorphisms of L into a normal closure N of L over K.

Corollary 7.36.
Let L be a Galois extension of K, and let G be the Galois group of L over K. Then $|G| = [L : K]$.

Theorem 7.37.
Let L be a finite extension of K. Then $\Phi(\mathrm{Gal}(L : K)) = K$ if and only if L is a separable normal extension of K.

Theorem 7.38.
Let L be a Galois extension of a field K, and let E be a subfield of L containing K. If $\delta \in \mathrm{Gal}(L : K)$, then $\Gamma(\delta(E)) = \delta\Gamma(E)\delta^{-1}$.

7.6 The Fundamental Theorem

Theorem 7.39. The Fundamental Theorem of Galois Theory:
Let L be a separable normal extension of a field K, with finite degree n.

(i) For all subfield E of L containing K, and all subgroups H of the Galois group $\mathrm{Gal}(L : K)$,

$$\Phi(\Gamma(E)) = E, \quad \Gamma(\Phi(H)) = H.$$

Also,

$$|\Gamma(E)| = [L : E], \quad |\mathrm{Gal}(L : K)|/|\Gamma(E)| = [E : K].$$

(ii) A subfield E is a normal extension of K if and only if $\Gamma(E)$ is a normal subgroup of $\mathrm{Gal}(L : K)$. If E is a normal extension, then $\mathrm{Gal}(E : K)$ is isomorphic to the quotient group $\mathrm{Gal}(L : K)/\Gamma(E)$.

Theorem 7.40.
Let L be a Galois extension of finite degree over K, with Galois group G, and let E_1, E_2 be subfields of L containing K. If $\Gamma(E_1) = H_1$ and $\Gamma(E_2) = H_2$, then

$$\Gamma(E_1 \cap E_2) = H_1 \vee H_2, \quad \Gamma(E_1 \vee E_2) = H_1 \cap H_2.$$

Theorem 7.41.
Let K be a field of characteristic 0, and let $f \in K[X]$. Let

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

be a splitting field for f over K. Let M be a field containing K, and let N be a splitting field of f over M. Then, up to isomorphism, L is a subfield of N, and $\mathrm{Gal}(N : M) \simeq \mathrm{Gal}(L : M \cap L)$.

7.7 An Example

We will now go through an example emphasising most of the topics discussed in this chapter.

Example. Consider the Galios group $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$, and let $v = \sqrt[4]{2}$. The field $\mathbb{Q}(v, i)$ is a splitting field of $X^4 - 2$ over $\mathbb{Q}$. If $\xi \in G$, then by Theorem 7.11, $\xi(i) \in \{i, -i\}$ and $\xi(v) \in \{v, -v, iv, -iv\}$. There are 8 elements in the group G as listed below,

$$\begin{aligned} \iota &: v \mapsto v \\ &: i \mapsto i \end{aligned} \qquad \begin{aligned} \lambda &: v \mapsto v \\ &: i \mapsto -i \end{aligned}$$

$$\begin{aligned} \alpha &: v \mapsto iv \\ &: i \mapsto i \end{aligned} \qquad \begin{aligned} \mu &: v \mapsto iv \\ &: i \mapsto -i \end{aligned}$$

$$\begin{aligned} \beta &: v \mapsto -v \\ &: i \mapsto i \end{aligned} \qquad \begin{aligned} \nu &: v \mapsto -v \\ &: i \mapsto -i \end{aligned}$$

$$\begin{aligned} \gamma &: v \mapsto -iv \\ &: i \mapsto i \end{aligned} \qquad \begin{aligned} \rho &: v \mapsto -iv \\ &: i \mapsto -i. \end{aligned}$$

The multiplication table is given as follows:

	ι	α	β	γ	λ	μ	ν	ρ
ι	ι	α	β	γ	λ	μ	ν	ρ
α	α	β	γ	ι	μ	ν	ρ	λ
β	β	γ	ι	α	ν	ρ	λ	μ
γ	γ	ι	α	β	ρ	λ	μ	ν
λ	λ	ρ	ν	μ	ι	γ	β	α
μ	μ	λ	ρ	ν	α	ι	γ	β
ν	ν	μ	λ	ρ	β	α	ι	γ
ρ	ρ	ν	μ	λ	γ	β	α	ι

As a small example we can see $\alpha(\lambda(v)) = \alpha(v) = iv$ and $\alpha(\lambda(i)) = \alpha(-i) = -i$, thus $\alpha\lambda = \mu$. From $\lambda(\alpha(v)) = \lambda(iv) = \lambda(i)\lambda(v) = -iv$ and $\lambda(\alpha(i)) = \lambda(i) = -i$ we deduce $\lambda\alpha = \rho$. The group G has eight total subgroups, three of order 4, namely

$$H_1 = \{\iota, \alpha, \beta, \gamma\}, \quad H_2 = \{\iota, \beta, \lambda, \nu\}, \quad H_3 = \{\iota, \beta, \mu, \rho\}$$

and five of order 2, namely,

$$H_4 = \{\iota, \beta\}, \quad H_5 = \{\iota, \lambda\}, \quad H_6 = \{\iota, \mu\}, \quad H_7 = \{\iota, \nu\}, \quad H_8 = \{\iota, \rho\}.$$

It is easy to verify $\Phi(H_1) = \mathbb{Q}(i)$ and that $\Phi(H_2) = \mathbb{Q}(v^2) = \mathbb{Q}(\sqrt{2})$, and that $\Phi(H_3) = \mathbb{Q}(i\sqrt{2})$. Continuing, we find that

$$\Phi(H_4) = \mathbb{Q}(i, \sqrt{2}), \quad \Phi(H_5) = \mathbb{Q}(v), \quad \Phi(H_6) = \mathbb{Q}((1+i)v),$$

It is easy to verify $\Phi(H_1) = \mathbb{Q}(i)$ and that $\Phi(H_2) = \mathbb{Q}(v^2) = \mathbb{Q}(\sqrt{2})$, and that $\Phi(H_3) = \mathbb{Q}(i\sqrt{2})$. Continuing, we find that

$$\Phi(H_7) = \mathbb{Q}(iv), \quad \Phi(H_8) = \mathbb{Q}((1-i)v).$$

The lattice of the subgroups of G is

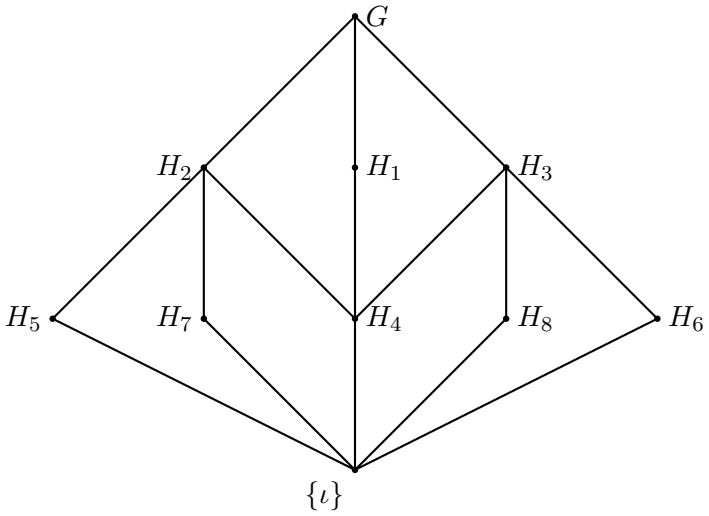


Figure 7.1: Lattice of Subgroups of G

and the lattic of subfields E such that $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(v, i)$ is an upside down version of Figure 7.1, where $\Phi(H_i)$ is denoted by F_i.

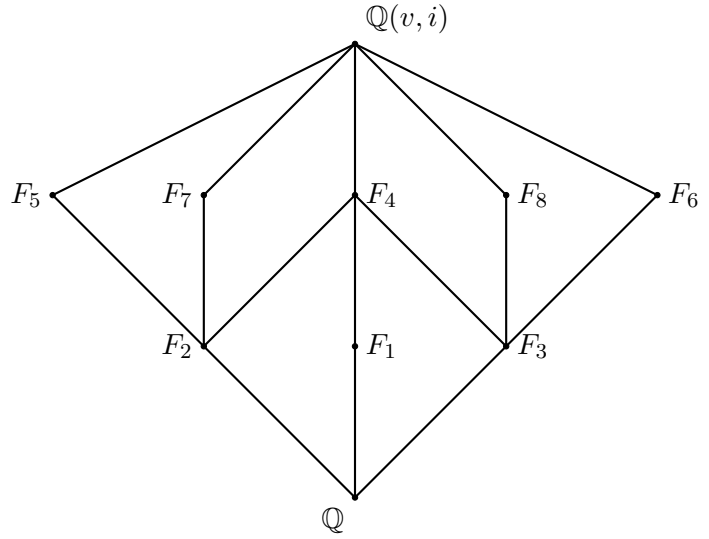


Figure 7.2: Lattice of Subfields of $\mathbb{Q}(v, i)$

The normal subgroups of G are H_1, H_2, H_3, and H_4. The corresponding subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$, and $\mathbb{Q}(i, \sqrt{2})$ are normal extensions, being the splitting fields of $X^2 + 1$, $X^2 - 2$, $X^2 + 2$, and $(X^2 + 1)(X^2 - 2)$, respectively.

Exercises

7.1 Let α be an automorphism of a field K. Show that

(i) $\alpha(0) = 0$, and $\alpha(-x) = -(\alpha(x))$ for all $x \in K$;

Proof. Let $x \in K$. Note, $\alpha(x) = \alpha(x+0) = \alpha(x) + \alpha(0)$, and by subtraction we have $0 = \alpha(0)$. Note, $0 = \alpha(0) = \alpha(x+(-x)) = \alpha(x)+\alpha(-x)$ which implies that $\alpha(-x) = -(\alpha(x))$. □

(ii) $\alpha(1) = 1$, and $\alpha(x^{-1}) = (\alpha(x))^{-1}$ for all $x \in K\backslash\{0\}$.

Proof. Let $x \in K$. Note, $\alpha(x) = \alpha(1x) = \alpha(1)\alpha(x)$, and since K is a field, multiplying by inverses gives us $1 = \alpha(1)$. Now suppose $x \neq 0$. Note, $1 = \alpha(1) = \alpha(xx^{-1}) = \alpha(x)\alpha(x^{-1})$ and thus $\alpha(x^{-1}) = (\alpha(x))^{-1}$. □

7.2 Determine $\operatorname{Aut}\mathbb{Q}$ and $\operatorname{Aut}\mathbb{Z}_p$.

Solution. Note, ι is clearly in $\operatorname{Aut}\mathbb{Q}$. Suppose φ is an automorphism. Then $\varphi(n) = \varphi(1+1+\cdots+1) = 1+1+\cdots+1 = n$. Similarly, $\varphi(-n) = -n$. For $m, n \in \mathbb{Z}$ with $n \neq 0$,

$$\varphi\Big(\frac{m}{n}\Big) = \varphi(m)(\varphi(n))^{-1} = mn^{-1} = \frac{m}{n}.$$

Thus, if φ is an automorphism, then $\varphi = \iota$. So $\operatorname{Aut}\mathbb{Q}$ is the trivial group $\{\iota\}$.

Note, ι is clearly in $\mathbb{Z}_p$. Suppose φ is an automorphism. Then $\varphi(n) = \varphi(1+1+\cdots+1) = 1+1+\cdots+1 = n$. Similarly, $\varphi(-n) = -n$. For $m, n \in \mathbb{Z}_p$ with $n \neq 0$,

$$\varphi(mn^{-1}) = \varphi(m)(\varphi(n))^{-1} = mn^{-1}.$$

Thus, if φ is an automorphism, then $\varphi = \iota$. So $\operatorname{Aut}\mathbb{Z}_p$ is the trivial group $\{\iota\}$. □

7.3 Show that $\Gamma\Phi\Gamma = \Gamma$ and $\Phi\Gamma\Phi = \Phi$.

Proof. Let $L : K$ be a field extension of a field K and let E be a subfield of L containing K. We will show $\Gamma\Phi\Gamma = \Gamma$ and $\Phi\Gamma\Phi = \Phi$. First note by Theorem 7.13 we have that $E \subseteq \Phi(\Gamma(E))$, and applying Theorem 7.10 we have that $\Gamma(E) \supseteq \Gamma(\Phi(\Gamma(E)))$. By Theorem 7.13 we also know that $H' \subseteq \Gamma(\Phi(H'))$, thus replacing H' with $\Gamma(E)$ we have $\Gamma(E) \subseteq \Gamma(\Phi(\Gamma(E)))$. Therefore $\Gamma(E) = \Gamma(\Phi(\Gamma(E)))$. Let H be a subset of $\operatorname{Gal}(L : K)$. Similarly, note by Theorem 7.13 we have that $H \subseteq \Gamma(\Phi(H))$, and thus by Theorem 7.10 we have $\Phi(H) \supseteq \Phi(\Gamma(\Phi(H)))$. From Theorem 7.10 we have $E' \subseteq \Phi(\Gamma(E'))$ and so

replacing E' with $\Phi(H)$ we have $\Phi(H) \subseteq \Phi(\Gamma(\Phi(H)))$. Therefore $\Phi(H) = \Phi(\Gamma(\Phi(H)))$. Finally we have $\Gamma\Phi\Gamma = \Gamma$ and $\Phi\Gamma\Phi = \Phi$. □

7.4 Verify that the mapping τ defined by

$$\tau(a + b\sqrt{2} + ci\sqrt{3} + di\sqrt{6}) = a - b\sqrt{2} + ci\sqrt{3} - di\sqrt{6}$$

is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$.

Proof. Let $x, y \in \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ where $x = a_1 + b_1\sqrt{2} + c_1 i\sqrt{3} + d_1 i\sqrt{6}$, $y = a_2 + b_2\sqrt{2} + c_2 i\sqrt{3} + d_2 i\sqrt{6}$. Note,

$$\begin{aligned}
\tau(x + y) &= \tau((a_1 + b_1\sqrt{2} + c_1 i\sqrt{3} + d_1 i\sqrt{6}) + (a_2 + b_2\sqrt{2} + c_2 i\sqrt{3} + d_2 i\sqrt{6})) \\
&= \tau((a_1 + a_2) + (b_1 + b_2)\sqrt{2} + (c_1 + c_2)i\sqrt{3} + (d_1 + d_2)i\sqrt{6}) \\
&= (a_1 + a_2) - (b_1 + b_2)\sqrt{2} + (c_1 + c_2)i\sqrt{3} - (d_1 + d_2)i\sqrt{6} \\
&= (a_1 - b_1\sqrt{2} + c_1 i\sqrt{3} - d_1 i\sqrt{6}) + (a_2 - b_2\sqrt{2} + c_2 i\sqrt{3} - d_2 i\sqrt{6}) \\
&= \tau(x) + \tau(y).
\end{aligned}$$

□

7.5

7.6

7.7 Let L be a normal extension of a field K, and let E be a subfield of L containing K. Show that L is a normal extension of E.

Proof. Let L be a normal extension of a field K, and let E be a subfield of L containing K. We will show L is a normal extension of E. First note, if $L = E$ then L is a normal extension of E. Now consider the case where $E \subset L$. There exists some $f \in K[X]$ where L is a splitting field for f. By definition of splitting field, f does not split completely over E. But, $f \in E[X]$ and since f splits completely over L we know L is a normal extension of E. □

7.8 Determine the normal closure of $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$.

Solution. Consider the field extension $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$. Consider the polynomial $f = X^4 - 2$. Note, f is irreducible over $\mathbb{Q}$, and f does not split completely over $\mathbb{Q}(\sqrt[4]{2})$ as shown below,

$$f = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt[2]{2}).$$

The polynomial f splits completely over the field $\mathbb{Q}(\sqrt[4]{2}, i)$,

$$f = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}).$$

Note, f does not split completely over any proper subfield E of $\mathbb{Q}(\sqrt[4]{2}, i)$ so $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field for f, and thus $\mathbb{Q}(\sqrt[4]{2}, i)$ is the normal closure of L over K. □

7.9

7.10 Let K be a field with characteristic p. Show that K is perfect if and only if the Frobenius monomorphism $\varphi : a \mapsto a^p$ is an automorphism of K.

Proof. Let K be a field with characteristic p. First we will show if K is perfect then $\varphi : a \mapsto a^p$ is an automorphism of K. Suppose K is perfect. Let f be an irreducible polynomial over K. Since f is separable, it must not be of the form

$$f = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp},$$

by Theorem 7.29. Thus any polynomial f' of the form

$$f' = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp}$$

must not be irreducible. By Theorem 7.31 each b_i of the polynomial is a pth power of an element of K. Thus φ is an automorpism. Now we will show if φ is an automorphism then K is perfect. Suppose φ is an automorphism. Then if $f \in K[X]$ is of the form

$$f = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp},$$

then since φ is an isomorphism, there exists an $a \in K$ such that $a^p = b_i$, in other words each coefficient b_i is a pth power of an element in K, and f is not irreducible by the contrapositive of Theorem 7.31. Thus an irreducible polynomial $f' \in K[X]$ is not of the form

$$f' = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp},$$

and is therefore separable.

□

7.11

7.12

7.13

8 Equations and Groups

8.1 Quadratics, Cubics, and Quartics: Solution by Radicals

Definition 8.1. ⟨ *noun, field extension* ⟩
Let K be a field of characteristic zero. A field L containing K is called an **extension by radicals**, or a **radical extension**, if there is a sequence

$$K = L_0, L_1, \ldots, L_m = L$$

with the property that, for $j \in \{0, 1, \ldots, m-1\}$, $L_{j+1} = L_j(\alpha_j)$, where α_j is a root of an irreducible polynomial in $L_j[X]$ of the form $X^{n_j} - c_j$.

Definition 8.2. ⟨ *adjective, polynomial* ⟩
A polynomial f over a field K with characteristic zero is said to be **soluble by radicals** if there is a splitting field f contained in a radical extension of K.

Theorem 8.3.
Let L be a radical extension of K, and let M be a normal closure of L. Then M is also a radical extension of K.

8.2 Cyclotomic Polynomials

Theorem 8.4.
Let K be a field of characteristic 0 and let L be a splitting field of $f = X^m - 1$ over K. The set $R \coloneqq \{a \in L : f(a) = 0\}$ is an abelian, cyclic, multiplicative subgroup of L.

Definition 8.5. ⟨ *adjective, root* ⟩
We call ω a **primitive** mth root of unity if ω is a generator of the cyclic group R.

Theorem 8.6.
Let ω be a primitive mth root of unity. Then w^j is a primitive mth root of unity if and only if j and m are coprime.

Definition 8.7. ⟨ *adjective, polynomial* ⟩
Let P_m be the set of primitive mth roots of unity. The **cyclotomic** polynomial Φ_m is defined by

$$\Phi_m \coloneqq \prod_{\varepsilon \in P_m} (X - \varepsilon).$$

Theorem 8.8.
Let K be a field with characteristic zero, and let L be a splitting field over K for $X^m - 1$. For $m \geq 1$,

$$X^m - 1 = \prod_{d|m} \Phi_d$$

where m and 1 are in the set of divisors.

Lemma 8.9.
Let K, L be fields with $K \subset L$. Let f, g be polynomials in $L[X]$ such that $f, fg \in K[X]$. Then $g \in K$.

Theorem 8.10.
Let K be a field with characteristic zero, containing mth roots of unity for each $m \in \mathbb{N}$, and let $K_0 \simeq \mathbb{Q}$ be the prime subfield of K. Then, for each divisor d of m (including m itself), the cyclotomic polynomial Φ_d lies in $K_0[X]$.

Theorem 8.11.
For all $m \geq 1$, the cyclotomic polynomial Φ_m is irreducible over $\mathbb{Q}$.

Theorem 8.12.
Let K be a field with characteristic zero, and let L be a splitting field over K of the polynomial $X^m - 1$. Then $\mathrm{Gal}(L : K)$ is isomorphic to R_m, the multiplicative group of residue classes $\bar{r} \mod m$ such that $(r, m) = 1$.

Corollary 8.13.
Let K be a field of characteristic zero, and let L be a splitting field over K of the polynomial $X^p - 1$, where p is prime. Then $\mathrm{Gal}(L : K)$ is cyclic.

8.3 Cyclic Extensions

Definition 8.14. ⟨ *adjective, field extension* ⟩
Let K be a field extension with characteristic zero, and let $L : K$ be field extension of K. We say L is a **cyclic extension** of K if L is normal and separable, and if $\mathrm{Gal}(L : K)$ is a cyclic group.

Definition 8.15. ⟨ *noun, function* ⟩
Let L be an extension of finite degree n over a field K with characteristic zero, and let N be a normal closure of L. By Theorem 7.35 there are exactly n distinct K-monomorphisms of $\tau_1, \tau_2, \ldots, \tau_n$ from L into N. For each element x of L, we define the **norm** $N_{L/K}(x)$ and **trace** $Tr_{L/K}(x)$ by

$$N_{L/K}(x) \coloneqq \prod_{i=1}^{n} \tau_i(x), \qquad Tr_{L/K}(x) \coloneqq \sum_{i=1}^{n} \tau_i(x).$$

Theorem 8.16.
The mapping $N_{L/K}$ is a group homomorphism from $(L^*, \cdot)$ into $(K^*, \cdot)$. The mapping $Tr_{L/K}$ is a group homomorphism from $(L, +)$ into $(K, +)$.

Theorem 8.17.
Let L be a cyclic extension of a field K, and let τ be a generator of the cyclic group $\mathrm{Gal}(L : K)$. If $x \in L$, then $N_{L/K}(x) = 1$ if and only if there is an element $y \in L$ such that $x = \frac{y}{\tau(y)}$, and $Tr_{L/K}(x) = 0$ if and only if there exists an element $z \in L$ such that $x = z - \tau(z)$.

Theorem 8.18.
Let $f = X^m - a \in K[X]$ where K is a field of characteristic zero, and let L be a splitting field of f over K. Then L contains an element ω, a primitive mth root of unity. The group $\mathrm{Gal}(L : K(\omega))$ is cyclic, with order dividing m. The order is equal to m if and only if f is irreducible over $K(\omega)$.

Theorem 8.19.
Let K be a field of characteristic zero, let m be a positive integer, and suppose that $X^m - 1$ splits completely over K. Let L be a cyclic extension of K such that $[L : K] = m$. Then there exists $a \in K$ such that $X^m - a$ is irreducible over K and L is a splitting field for $X^m - a$. Moreover, L is generated over K by a single root of $X^m - a$.

Theorem 8.20. Abel's Theorem:
Let K be a field of characteristic zero, let p be prime, and let $a \in K$. If $X^p - a$ is reducible over K then it has a linear factor $(X - c) \in K[X]$.

Exercises

8.1

8.2

8.3

8.4

8.5

8.6

8.7

8.8

8.9

9 Some Group Theory

9.1 Abelian Groups

Definition 9.1. ⟨ *adjective, field extension* ⟩
An abelian group A with subgroups $U_1, U_2, \ldots, U_k$ is said to be the **direct sum** of $U_1, U_2, \ldots, U_k$ if every element $a \in A$ has a unique expression

$$a = u_1 + u_2 + \cdots + u_k,$$

where $u_i \in U_i$ for each $i \in \{1, 2, \ldots, k\}$. We write

$$A = U_1 \oplus U_2 \oplus \cdots \oplus U_k.$$

Theorem 9.2.
Let A be a abelian group that is the direct product of subgroups $U_1, U_2, \ldots, U_k$. Then,

(a) it follows that $U_i \cap U_j = \{0\}$ whenever $i \neq j$;

(b) and $u_1 + u_2 + \cdots + u_k = 0$ implies $u_1 = u_2 = \cdots = u_k = 0$ where $u_i \in U_i$ for each $i \in \{1, 2, \ldots, k\}$.

Theorem 9.3.
Let A be an element of a finite abelian group A, and suppose that the order of A is mn, where $\gcd(m, n) = 1$. Then a can be written in exactly one way as $b + c$, where $o(b) = m$ and $o(c) = n$.

Corollary 9.4.
Let a be an element of a finite abelian group A and suppose that $o(a) = m_1 m_2 \cdots m_r$, where $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Then a can be written in exactly one way as $a_1 + a_2 + \cdots + a_r$, where $o(a_i) = m_i$ for each $i \in \{1, 2, \ldots, r\}$.

Theorem 9.5.
Every finite abelian group is expressible as the direct sum of abelian p-groups.

Theorem 9.6. The Basis Theorem:
Every finite abelian group is expressible as the direct sum of cyclic groups.

Definition 9.7. ⟨ *adjective, field extension* ⟩
A finite group is called **solvable** if, for some $m \geq 0$, it has a finite series $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$ of subgroups such that for $i \in \{0, 1, \ldots, m-1\}$

(i) $G_i \lhd G_{i+1}$

(ii) G_{i+1}/G_i is cyclic.

9.2 Sylow Subgroups

9.3 Permutation Groups

Definition 9.8. ⟨ *noun, group* ⟩
Let S_n be the **symmetric group on** n **symbols** consisting of all one-to-one mappings of the set $1, 2, \ldots, n$ onto itself, the operations being composition of mappings.

Definition 9.9. ⟨ *noun, permutation* ⟩
A **cycle** of length k, written $\sigma = (a_1, a_2, \ldots, a_k)$, is a permutation such that

$$a_1\sigma = a_2,\ a_2\sigma = a_3,\ \ldots\ a_{k-1}\sigma = a_k,\ a_k\sigma = a_1,$$

and $x\sigma = x$ for all x not in the set $\{a_1, a_2 \ldots, a_k\}$.

Theorem 9.10.
Every π in S_n can be expressed as the product of disjoint cycles. The order of π is the least common multiple of the lengths of each cycles.

Definition 9.11. ⟨ *noun, permutation* ⟩
A cycle of length 2 is called a **transposition**.

Corollary 9.12.
Every cycle can be expressed as a product of transpositions.

Definition 9.13. ⟨ *adjective, permutation* ⟩
A permutation is said to be **even** if it can be expressed by an even number of transpositions. A permutation is said to be **odd** if it can be expressed by an odd number of transpositions.

Definition 9.14. ⟨ *noun, group* ⟩
The set of all even transpositions of S_n is called the **alternating group**, and denoted by A_n.

Theorem 9.15.
The group A_n is a normal subgroup of S_n, and has order $\frac{1}{2}n!$.

Theorem 9.16.
The symmetric group S_3 is solvable.

Theorem 9.17.
The symmetric group S_4 is solvable.

Theorem 9.18.
For $n \geq 3$, the alternating group A_n is generated by the set of all cycles of length 3.

Definition 9.19. ⟨ *noun, group* ⟩
A non-abelian group is called **simple** if it has no proper normal subgroups.

Theorem 9.20.
For $n \geq 5$, the alternating group A_n is simple.

Theorem 9.21.
The symmetric group S_n is generated by the two cycles $(1\ 2)$ and $(1\ 2\ \ldots\ n)$.

9.4 Properties of Solvable Groups

Theorem 9.22.
Let G be a group.

(i) If G is solvable, then every subgroup of G is solvable.

(ii) If G is solvable and N is a normal subgroup of G then G/N is solvable.

(iii) Let $N \lhd G$. Then G is solvable if and only if both N and G/N are solvable.

Corollary 9.23.
For all $n \geq 5$, the symmetric group S_n is not solvable.

Exercises

9.1

9.2

9.3

9.4

9.5

9.6

9.7

10 Groups and Equations

Theorem 10.1.
Let K be a field of characteristic zero. Let f be a polynomial in $K[X]$ whose Galois group $\mathrm{Gal}(f)$ is solvable. Then f is solvable by radicals.

Theorem 10.2.
Let K be a field of characteristic zero, and let $K \subseteq L \subseteq M$, where M is a radical extension. Then $\mathrm{Gal}(L : K)$ is a solvable group.

Theorem 10.3.
A polynomial f with coefficients in a field K of characteristic zero is solvable by radicals if and only if its Galois group is solvable.

10.1 Insoluble Quintics

Theorem 10.4.
Let p be a prime, and let f be a monic irreducible polynomial of degree p, with coefficients in $\mathbb{Q}$. Suppose that f has precisely two zeros in $\mathbb{C}\backslash\mathbb{R}$. Then the Galois group of f is the symmetric group S_p.

10.2 General Polynomials

Definition 10.5. ⟨ *adjective, field elements* ⟩
Let K be a field of characteristic zero, and let L be an extension of K. A subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of L is said to be **algebraically independent** over K if, for all polynomials $f = f(X_1, X_2, \ldots, X_n)$ with coefficients in K,

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0 \text{ only if } f = 0.$$

Definition 10.6. ⟨ *noun, group* ⟩
An extension L of a field K is said to be **finitely generated**, if for some natural number m there exists elements $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

Theorem 10.7.
Let $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a finitely generated extension of K. Then there exists a field E such that $K \subseteq E \subseteq L$ such that, for some m with $0 \leq m \leq n$:

(i) $E = K(\beta_1, \beta_2, \ldots, \beta_m)$, where $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is algebraically independent over K;

(ii) $[L : E]$ is finite.

Definition 10.8. ⟨ *noun, integer* ⟩
The number m featured in Theorem 10.7 is called the **transcendence degree** of L over K.

Definition 10.9. ⟨ *noun, polynomials* ⟩
Let $\mathrm{Aut}_n \coloneqq \{\phi_\sigma : \sigma \in S_n\}$[a]. The fixed field F of Aut_n includes all the **elmentary symmetric polynomials**

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n, \\ s_2 &= t_1t_2 + t_1t_3 + t_1t_4 + \cdots + t_{n-1}t_n, \\ &\vdots \\ s_n &= t_1t_2 \cdots t_n; \end{aligned}$$

and all rational combinations of these polynomials.

[a] The map $\sigma \mapsto \phi_\sigma$ is an isomorphism.

Theorem 10.10.
With the notation from Definition 10.9, $F = K(s_1, s_2, \ldots s_n)$.

Theorem 10.11.
The symmetric polynomials $s_1, s_2, \ldots, s_n$ are algebraically independent.

Definition 10.12. ⟨ *noun, polynomial* ⟩
The **general polynomial** of degree n over $K(s_1, s_2, \ldots, s_n)$ is

$$X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n.$$

Theorem 10.13.
Let K be a field of characteristic zero, and let $g(X)$ be the general polynomial

$$g(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n.$$

Let M be a splitting field for g over $K(s_1, s_2, \ldots, s_n)$. Then the zeros $t_1, t_2, \ldots, t_n$ of g in M are algebraically independent over K, and the Galois group of M over $K(s_1, s_2, \ldots, s_n)$ is the symmetric group S_n.

Theorem 10.14.
If K is a field with characteristic zero and $n \geq 5$, the general polynomial

$$X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n$$

is not solvable by radicals.

References

[1] Sheldon Axler. *Linear Algebra Done Right*. Springer Undergraduate Mathematics Series. Springer International Publishing, third edition, 2015.

[2] Joseph A. Gallian. *Contemporary Abstract Algebra, Ninth Edition*. Cengage Learning, Boston, Massachusetts, ninth edition, 2017.

[3] John M. Howie. *Fields and Galois Theory*. Springer Undergraduate Mathematics Series. Springer London, first edition, 2005.