MTH 411
Lecture Notes
Based on Hungerford, Abstract Algebra

Ulrich Meierfrankenfeld

Department of Mathematics

Michigan State University

East Lansing MI 48824

meier@math.msu.edu

August 28, 2014

Contents

Chapter 1

Groups

1.1 Sets

Naively a set S is collection of object such that for each object x either x is *contained* in S or x is not contained in S. We use the symbol '$\in$' to express containment. So $x \in S$ means that x is contained in S and $x \notin S$ means that x is not contained in S. Thus we have

$$\text{For all objects } x: \quad x \in S \quad \text{or} \quad x \notin S.$$

You might think that every collection of objects is a set. But we will now see that this cannot be true. For this let A be the collection of all sets. Suppose that A is a set. Then A is contained in A. This already seems like a contradiction But maybe a set can be contained in itself. So we need to refine our argument. We say that a set S is nice if S is not contained in S. Now let B be the collection of all nice set. Suppose that B is a set. Then either B is contained in B or B is not contained in B.

Suppose that B is contained in B. Since B is the collection of all nice sets we conclude that B is nice. The definition of nice now implies that that B is not contained in B, a contradiction.

Suppose that B is not contained in B. Then by definition of 'nice', B is a nice set. But B is the collection of all nice sets and so B is contained in B, again a contradiction.

This shows that B cannot be a set. Therefore B is a collection of objects, but is not set.

What kind of collections of objects are sets is studied in Set Theory.

The easiest of all sets is the *empty set* denote by $\{\}$ or $\emptyset$. The empty set is defined by

$$\text{For all objects } x: \quad x \notin \emptyset.$$

So the empty set has no members.

Given an object s we can form the *singleton* $\{s\}$, the set whose only members is s:

$$\text{For all objects } x: \quad x \in \{s\} \text{ if and only if } x = s$$

If A and B is a set then also its union $A \cup B$ is a set. $A \cup B$ is defined by

For all objects $x : x \in A \cup B$ if and only if $x \in A$ or $x \in B$.

The *natural numbers* are defined as follows:

$$\begin{array}{rcccccc}
0 & := & & & & & \emptyset \\
1 & := & 0 \cup \{0\} & = & \{0\} & = & \{\emptyset\} \\
2 & := & 1 \cup \{1\} & = & \{0,1\} & = & \{\emptyset, \{\emptyset\}\} \\
3 & := & 2 \cup \{2\} & = & \{0,1,2\} & = & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 & := & 4 \cup \{4\} & = & \{0,1,2,3\} & = & \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
n+1 & := & n \cup \{n\} & = & \{0,1,2,3,\dots n\} & &
\end{array}$$

One of the axioms of set theory says that the collection of all the natural numbers

$$\{0, 1, 2, 3, 4, \dots\}$$

is set. We denote this set by $\mathbb{N}$.

Addition on $\mathbb{N}$ is defined as follows: $n + 0 := n$, $n + 1 := n \cup \{n\}$ and inductively

$$n + (m + 1) := (n + m) + 1.$$

Multiplication on $\mathbb{N}$ is defined as follows: $n \cdot 0 := n$, $n \cdot 1 := n$ and inductively

$$n \cdot (m + 1) := (n \cdot m) + n.$$

1.2 Functions and Relations

We now introduce two important notations which we will use frequently to construct new sets from old ones. Let $I_1, I_2, \dots I_n$ be sets and let Φ be some formula which for given elements $i_1 \in I_1, i_2 \in I_2, \dots, i_n \in I_n$ allows to compute a new object $\Phi(i_1, i_2, \dots, i_n)$. Then

$$\{\Phi(i_1, i_2, \dots, i_n) \mid i_1 \in I_1, \dots, i_n \in I_n\}$$

is the set defined by

$$x \in \{\Phi(i_1, i_2, \dots, i_n) \mid i_1 \in I_1, \dots, i_n \in I_n\}$$

if and only

there exist objects $i_1, i_2, \dots, i_n$ with $i_1 \in I_1, i_2 \in I_2, \dots, i_n \in I_n$ and $x = \Phi(i_1, i_2, \dots, i_n)$.

In Set Theory it is shown that $\{\Phi(i_1, i_2, \ldots, i_n) \mid i_1 \in I_1, \ldots, i_n \in I_n\}$ is indeed a set.

Let P be a statement involving a variable t. Let I be set. Then

$$\{i \in I \mid P(i)\}$$

is the set defined by

$$x \in \{i \in I \mid P(i)\} \quad \text{if and only if} \quad x \in I \text{ and } P \text{ is true for } t = x.$$

Under appropriate condition it is shown in Set Theory that $\{i \in I \mid P(i)\}$ is a set.

Let a and b be objects. Then the *ordered pair* (a, b) is defined as $(a, b) := \{\{a\}, \{a, b\}\}$. We will prove that

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

For this we first establish a simple lemma:

Lemma 1.2.1. *Let u, a, b be objects with $\{u, a\} = \{u, b\}$. Then $a = b$.*

Proof. We consider the two cases $a = u$ and $a \neq u$.

Suppose first that $a = u$. Then $b \in \{u, b\} = \{u, a\} = \{a\}$ and so $a = b$.

Suppose next that $a \neq u$. Since $a \in \{u, a\} = \{u, b\}$, $a = u$ or $a = b$. But $a \neq u$ and so $a = b$. □

Proposition 1.2.2. *Let a, b, c, d be objects. Then*

$$(a, b) = (c, d) \textit{ if and only if } a = c \textit{ and } b = d.$$

Proof. Suppose $(a, b) = (c, d)$. We need to show that $a = c$.

We will first show that $a = b$. Since

$$\{a\} \in \{\{a\}, \{a, b\}\} = (a, b) = (c, d) = \{\{c\}, \{c, d\}\},$$

we have

$$\{a\} = \{c\} \quad \text{or} \quad \{a\} = \{c, d\}.$$

In the first case $a = c$ and in the second $c = d$ and again $a = c$.

From $a = c$ we get $\{\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\} = \{\{a\}, \{a, d\}$. So by 1.2.1 $\{a, b\} = \{a, d\}$ and applying 1.2.1 again, $b = d$. □

If I and J are sets we define $I \times J := \{(i, j) \mid i \in I, j \in J\}$.

A *relation* on I and J is triple $r = (I, J, R)$ where R is a subset $I \times J$. If $i \in I$ and $j \in J$ we write irj if $(i, j) \in R$.

For example let $R := \{(n, m) \mid n, m \in \mathbb{N}, n \in m\}$ and let $<$ be the triple $(\mathbb{N}, \mathbb{N}, R)$. Let $n, m \in \mathbb{N}$. Then $n < m$ if and only if $n \in m$. Since $m = \{0, 1, 2, \ldots, m - 1\}$ we see that $n < m$ if and only if n is one of $0, 1, 2, 3, \ldots, m - 1$.

A *function* from I to J is a relation $f = (I, J, R)$ on I and J such that for each $i \in I$ there exists a unique $j \in J$ with $(i, j) \in R$. We denote this unique j by $f(i)$. So for $i \in I$ and $j \in J$ the following three statements are equivalent:

$$ifj \iff (i, j) \in R \iff j = f(i).$$

We denote the function $f = (I, J, R)$ by

$$f : I \to J, \quad i \to f(i).$$

So $R = \{(i, f(i)) \mid i \in I\}$.

For example

$$f : \mathbb{N} \to \mathbb{N}, \quad m \to m^2$$

denotes the function $(\mathbb{N}, \mathbb{N}, \{(m, m^2) \mid n \in \mathbb{N}\})$

Informally, a function f from I to J is a rule which assigns to each element i of I a unique element $f(i)$ in J.

A function $f : I \to J$ is called *1-1* if $i = k$ whenever $i, k \in I$ with $f(i) = f(k)$.

f is called *onto* if for each $j \in I$ there exists $i \in I$ with $f(i) = j$. Observe that f is 1-1 and onto if and only if for each $j \in J$ there exists a unique $i \in I$ with $f(i) = j$.

If $f : I \to J$ and $g : J \to K$ are functions, then the *composition* $g \circ f$ of g and f is the function from I to K defined by $(g \circ f)(i) = g(f(i))$ for all $i \in I$.

1.3 Definition and Examples

Definition 1.3.1. *Let S be a set. A binary operation is a function $* : S \times S \to S$. We denote the image of (s, t) under $*$ by $s * t$.*

Let I be a set. Given a formula ϕ which assigns to each pair of element $a, b \in I$ some object $\phi(a, b)$. Then ϕ determines a binary operation $* : I \times I \to I, (a, b) \to \phi(a, b)$ provided for all $a, b \in I$:

(i) $\phi(a, b)$ can be evaluated and $\phi(a, b)$ only depends on a and b; and

(ii) $\phi(a, b)$ is an element of I.

If (i) holds we say that $*$ is *well-defined*. And if (ii) holds we say that I is *closed* under $*$.

Example 1.3.2.

(1) $+ : \mathbb{Z} \times \mathbb{Z}, (n, m) \to n + m$ is a binary operation.

(2) $\cdot : \mathbb{Z} \times \mathbb{Z}, (n, m) \to nm$ is a binary operation.

(3) $\cdot : \mathbb{Q} \times \mathbb{Q}, (n, m) \to nm$ is a binary operation.

(4) Let $I = \{a, b, c, d\}$ and define $* : I \times I \to I$ by

$*$	a	b	c	d
a	b	a	c	a
b	a	b	c	d
c	d	b	a	a
d	a	d	a	b

Here for $x, y \in I$, $x * y$ is the entree in row x, column y. For example $b * c = c$ and $c * b = b$.

Then $*$ is a binary operation.

(5)

$\square$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	a	a
d	a	a	a	a

$\square$ is a binary operation on I.

(6)

$*$	a	b	c	d
a	b	a	c	a
b	a	e	c	d
c	d	b	a	a
d	a	d	a	b

is **not** a binary operation. Indeed, according to the table, $b * b = e$, but e is not an element of I. Hence I is not closed under $*$ and so $*$ is not a binary operation on I.

(7) Let I be a set . A 1-1 and onto function $f : I \to I$ is called a *permutation* of I.

Sym(I) denotes the set of all permutations of I. If f and g are permutations of I then by A.2.3(c) also the composition $f \circ g$ is a permutation of I. Hence the map

$$\circ : \mathrm{Sym}(I) \times \mathrm{Sym}(I), (f, g) \to f \circ g$$

is a binary operation on Sym(I).

(8) $\diamond : \mathbb{Z}_3 \times \mathbb{Z}_3, ([a]_3, [b]_3) \to [a^{b^2+1}]_3$, where $[a]_3$ denotes the congruence class of a modulo 3, is not a binary operation. Indeed we have $[0]_3 = [3]_3$ but

$$[(-1)^{0^2+1}]_3 = [(-1)^1]_3 = [-1]_3 \neq [1]_3 = [(-1)^{10}]_3 = [(-1)^{3^2+1}]_3$$

and so $\diamond$ is not well-defined.

(9) $\oplus : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, (a, b) \to \frac{a}{b}$ is not a binary operation. Since $\frac{1}{0}$ is not defined, $\oplus$ is not well-defined.

Definition 1.3.3. *Let $*$ be a binary operation on a set I. Then $*$ is called* associative *if*

$$(a * b) * c = a * (b * c) \textit{ for all } a, b, c \in I$$

Example 1.3.4.

We investigate which of the binary operations in 1.3.2 are associative.

(1) Addition on $\mathbb{Z}$ is associative.

(2) Multiplication on $\mathbb{Z}$ is associative.

(3) Multiplication on $\mathbb{Q}$ is associative.

(4) $*$ in 1.3.2(4) is not associative. For example

$$a * (d * c) = a * a = b \text{ and } (a * d) * c = a * c = c.$$

(5) $\square$ in 1.3.2(5) is associative since $x * (y * z) = a = (x * y) * z$ for any $x, y, z \in \{a, b, c, d\}$.

(7) Composition of functions is associative: Let $f : I \to J$, $g : J \to K$ and $h : K \to L$ be functions. Then for all $i \in I$,

$$((f \circ g) \circ h)(i) = (f \circ g)(h(i)) = f(g(h(i)))$$

and

$$(f \circ (g \circ h))(i) = f((g \circ h)(i)) = f(g(h(i))).$$

Thus $f \circ (g \circ h) = (f \circ g) \circ h$.

Definition 1.3.5. *Let I be a set and $*$ a binary operation on I. An* identity *of $*$ in I is a element $e \in I$ with $e * i = i$ and $i = i * e$ for all $i \in I$.*

Example 1.3.6.

We investigate which of the binary operations in 1.3.2 have an identity:

(1) 0 is an identity of $+$ in $\mathbb{Z}$.

(2) 1 is an identity of $\cdot$ in $\mathbb{Z}$.

(3) 1 is an identity for $\cdot$ in $\mathbb{Q}$.

(4) Suppose that x is an identity of $*$ in 1.3.2(4). From $x * y = y$ for all $y \in I$ we conclude that row x of the multiplication table must be equal to the header row of the table. This shows that $x = b$. Thus $y * b = y$ for all $y \in I$ and we conclude that the column b must be equal to the header column. But this is not the case. Hence $*$ does not have an identity.

(5) No row of the multiplication table in 1.3.2(5) is equal to the header row. Thus $\square$ does not have an identity.

(7) Let I be set. Define $\mathrm{id}_I\colon I \to I$, $i \to i$. id_I is called the *identity* function on I. Let $f \in \mathrm{Sym}(I)$. Then for any $i \in I$,

$$(f \circ \mathrm{id}_I)(i) = f(\mathrm{id}_I(i)) = f(i)$$

and so $f \circ \mathrm{id}_i = f$.

$$(\mathrm{id}I \circ f)(i) = \mathrm{id}_I(f(i)) = f(i)$$

and so $\mathrm{id}_I \circ f = f$.

Thus id_I is an identity of $\circ$ in $\mathrm{Sym}(I)$.

Lemma 1.3.7. *Let $*$ be a binary operation on the set I, then $*$ has at most one identity in I.*

Proof. Let e and f be identities of $*$. Then $e * f = f$ since e is an identity and $e * f = e$ since f is an identity. Hence $e = f$. So any two identities of $*$ are equal. $\square$

Definition 1.3.8. *Let $*$ be a binary operation on the set I with identity e. The $a \in I$ is called* invertible *if there exists $b \in I$ with $a * b = e$ and $b * a = e$. Any such b is called an* inverse *of a with respect to $*$.*

Example 1.3.9.

(1) $-n$ is an inverse of $n \in \mathbb{Z}$ with respect to addition.

(2) 2 does not have an inverse in $\mathbb{Z}$ with respect to multiplication.

(3) $\frac{1}{2}$ is an inverse of 2 with respect to multiplication in $\mathbb{Q}$.

(4) If I is a set and $f \in \mathrm{Sym}(I)$ we define $g : I \to I$ by $g(i) = j$ where j is the unique element of I with $f(j) = i$. So

$$f(g(i)) = f(j) = i = \mathrm{id}_I(i).$$

Moreover, if $g(f(i)) = k$, then by definition of g, $f(k) = f(i)$. Since f is 1-1 this implies $k = i$. Thus $g(f(i)) = i = \mathrm{id}_I(i)$. Thus $f \circ g = \mathrm{id}_I$ and $g \circ f = \mathrm{id}_I$. Hence f is invertible with inverse g.

Lemma 1.3.10. *Let $*$ be an associative binary operation on the set I with identity e. Then each $a \in I$ has at most one inverse in I with respect to $*$.*

Proof. Let b and c be inverses of a in I with respect to $*$. Then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

and so the inverse of a is unique. □

Consider the binary operation

$$\begin{array}{c|ccc} * & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{array}.$$

0 is an identity of $*$. We have $1 * 1 = 0$ and so 1 is an inverse of 1. Also $1 * 2 = 0 = 2 * 1$ and so also is an inverse of 1. Hence inverses do not have to be unique if $*$ is not associative.

Definition 1.3.11. *A* group *is tuple $(G, *)$ such that G is a set and*

(i) $* : G \times G \to G$ is a binary operation.

(ii) $*$ is associative.

(iii) $*$ has an identity e in G.

(iv) Each $a \in G$ is invertible in G with respect to $*$.

Example 1.3.12.

(1) $(\mathbb{Z}, +)$ is a group.

(2) $(\mathbb{Z}, \cdot)$ is not a group since 2 is not invertible with respect to multiplication.

(3) $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group.

(4) $(I, *)$ in 1.3.2(4) is not a group since its $*$ is not associative.

(5) $(I, \Box)$ in 1.3.2(5) is not a group since it has no identity.

(6) $(I, \diamond)$ in 1.3.2(6) is not a group since $\diamond$ is not a binary operation.

(7) Let I be a set. By 1.3.2(7) $\circ$ is binary operation on $\mathrm{Sym}(I)$; by 1.3.4(7), $\circ$ is associative; by 1.3.6(7) id_I is an identity for $\circ$; and by 1.3.9(4) every $f \in \mathrm{Sym}(I)$ is invertible. Thus $(\mathrm{Sym}(I), \circ)$ is a group. $\mathrm{Sym}(I)$ is called the *symmetric group on I.*

Sets of permutations will be our primary source for groups. We therefore introduce some notation which allows us to easily compute with permutations. $[1 \dots n]$ denotes the set $\{i \in \mathbb{N} \mid 1 \leq i \leq n\} = \{1, 2, 3, \dots, n\}$. $\mathrm{Sym}(n)$ stands for $\mathrm{Sym}([1 \dots n])$. Let $\pi \in \mathrm{Sym}(n)$. Then we denote π by

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n-1) & \pi(n) \\ \end{pmatrix}.$$

For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

denotes the permutation of π of $[1 \dots 5]$ with $\pi(1) = 2, \pi(2) = 1, \pi(3) = 4, \pi(4) = 5$ and $\pi(5) = 3$.

Almost always we will use the more convenient *cycle* notation:

$$(a_{1,1}, a_{2,1}, a_{3,1}, \dots a_{k_1,1})(a_{1,2}, a_{2,2} \dots a_{k_2,2}) \dots (a_{1,l}, a_{2,l} \dots a_{k_l,l})$$

denotes the permutation π with $\pi(a_{i,j}) = a_{i+1,j}$ and $\pi(a_{k_j,j}) = a_{1,j}$ for all $1 \leq i < k_j$ and $1 \leq j \leq l$.

So $(1, 3, 4)(2, 6)(5)$ denotes the permutation of $[1 \dots 6]$ with $\pi(1) = 3$, $\pi(3) = 4$, $\pi(4) = 1$,$\pi(2) = 6$, $\pi(6) = 2$ and $\pi(5) = 5$.

Each $(a_{1,j}, a_{2,j}, \dots a_{k_j,j})$ is called a *cycle* of π. We usually will omit cycles of length 1 in the cycle notation of π.

As an example we compute $(1, 3)(2, 4) \circ (1, 4)(2, 5, 6)$.

We have

	$(1,4)(2,5,6)$		$(1,3)(2,4)$	
1	$\to$	4	$\to$	2
2	$\to$	5	$\to$	5
5	$\to$	6	$\to$	6
6	$\to$	2	$\to$	4
4	$\to$	1	$\to$	3
3	$\to$	3	$\to$	1

and so

$$(1,3)(2,4) \circ (1,4)(2,5,6) = (1,2,5,6,4,3).$$

It is very easy to compute the inverse of a permutation in cycle notation. One just needs to write each of the cycles in reversed order. For example the inverse of $(1,4,5,6,8)(2,3,7)$ is $(8,6,5,4,1)(7,3,2)$.

Example 1.3.13.

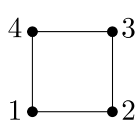
In cycle notation the elements of Sym(3) are

$$(1),(1,2,3),(1,3,2),(1,2),(1,3),(2,3).$$

Keep here in mind that $(1) = (1)(2)(3)$, $(1,2) = (1,2)(3)$ and so on. The multiplication table of Sym(3) is as follows:

$\circ$	(1)	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
(1)	(1)	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	(1)	$(1,3)$	$(2,3)$	$(1,2)$
$(1,3,2)$	$(1,3,2)$	(1)	$(1,2,3)$	$(2,3)$	$(1,2)$	$(1,3)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	(1)	$(1,3,2)$	$(1,2,3)$
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,2,3)$	(1)	$(1,3,2)$
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	$(1,3,2)$	$(1,2,3)$	(1)

Example 1.3.14.

Consider the square 

.

Let D_4 be the set of all permutations of $\{1,2,3,4\}$ which map the edges (of the square) to edges.

For example $(1,3)(2,4)$ maps the edge $\{1,2\}$ to $\{3,4\}$, $\{2,3\}$ to $\{4,1\}$, $\{3,4\}$ to $\{1,2\}$ and $\{4,1\}$ to $\{2,3\}$. So $(1,3)(2,4) \in D_4$.

But $(1,2)$ maps $\{2,3\}$ to $\{1,3\}$, which is not an edge. So $(1,2) \notin D_4$.

Which permutations are in D_4? We have counterclockwise rotations by $0°, 90°, 180°$ and $270°$:

$$(1),(1,2,3,4),(1,3)(2,4),(1,4,3,2),$$

and reflections at $y=0, x=0$, $x=y$ and $x=-y$:

$$(1,4)(2,3),(1,2)(3,4),(2,4),(1,3)$$

Are these all the elements of D_4? Let's count the number of elements. Let $\pi \in D_4$. Then $\pi(1)$ can be $1,2,3$,or 4. So there are 4 choices for $\pi(1)$, $\pi(2)$ can be any of the two neighbors of $\pi(1)$. So there are two choice for $\pi(2)$. $\pi(3)$ must be the neighbor of $\pi(2)$ different from $\pi(1)$. So there is only one choice for $\pi(3)$. $\pi(4)$ is the point different from $\pi(1), \pi(2)$ and $\pi(3)$. So there is also only one choice for $\pi(4)$. All together there are $4 \cdot 2 \cdot 1 \cdot 1 = 8$ possibilities for π. Thus $|D_4| = 8$ and

$$D_4 = \{(1),(1,2,3,4,),(1,3)(2,4),(1,4,3,2),(1,4)(2,3),(1,2)(3,4),(2,4),(1,3)\}.$$

If $\alpha, \beta \in \mathrm{Sym}(4)$ maps edges to edges, then also $\alpha \circ \beta$ and the inverse of α map edges to edges. Thus $\circ$ is an associative binary operation on D_4, (1) is an identity and each α in D_4 is invertible. Hence $(D_4, \circ)$ is a group. D_4 is called the *dihedral group of degree* 4.

1.4 Basic Properties of Groups

Notation 1.4.1. *Let $(G,*)$ be a group and $g \in G$. Then g^{-1} denotes the inverse of g in G. The identity element is denote by e_G or e. We will often just write ab for $a*b$. And abusing notation we will call G itself a group.*

Lemma 1.4.2. *Let G be a group and $a, b \in G$.*

(a) $(a^{-1})^{-1} = a$.

(b) $a^{-1}(ab) = b$, $(ba)a^{-1} = b$, $(ba^{-1})a = b$ and $a(a^{-1}b) = b$.

Proof. (a) By definition of a^{-1}, $aa^{-1} = e$ and $a^{-1}a = e$. So a is an inverse of a^{-1}, that is $a = (a^{-1})^{-1}$.

(b)

$$\begin{aligned} & a^{-1}(ab) \\ = \; & (a^{-1}a)b && - \; * \text{ is associative} \\ = \; & eb && - \; \text{definition of } a^{-1} \\ = \; & b && - \; \text{definition of identity} \end{aligned}$$

The remaining assertion are proved similarly. □

Lemma 1.4.3. *Let G be a group and $a, b, c \in G$. Then*

$$\begin{aligned} & ab = ac \\ \Longleftrightarrow \; & b = c \\ \Longleftrightarrow \; & ba = ca \; . \end{aligned}$$

Proof. Suppose first that $ab = ac$. Multiplication with a^{-1} from the right gives $a^{-1}(ab) = a^{-1}(ac)$ and so by 1.4.2 $a = b$.

If $b = c$, the clearly $ab = ac$. So the first two statement are equivalent. Similarly the last two statements are equivalent. □

Lemma 1.4.4. *Let G be a group and $a, b \in G$.*

(a) The equation $ax = b$ has a unique solution in G, namely $x = a^{-1}b$.

(b) The equation $ya = b$ has a unique solution in G, namely $y = ba^{-1}$.

(c) $b = a^{-1}$ if and only if $ab = e$ and if and only if $ba = e$.

(d) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. (a) By 1.4.3 $ax = b$ if and only if $a^{-1}(ax) = a^{-1}b$ and so (by 1.4.2) if and only if $x = a^{-1}b$.

(b) is proved similarly.

(c) By (a) $ab = e$ if and only if $b = a^{-1}e$. Since e is an identity, this is the case if and only if $b = a^{-1}$. Similarly using (b), $ba = e$ if and only if $b = a^{-1}$.

(d)

$$\begin{aligned} & (ab)(b^{-1}a^{-1}) \\ = \; & a(b(b^{-1}a^{-1})) && - \; * \text{ is associative} \\ = \; & aa^{-1} && - \; 1.4.2(b) \\ = \; & e && - \; \text{definition of } a^{-1} \end{aligned}$$

So by (c), $b^{-1}a^{-1} = (ab)^{-1}$. □

Definition 1.4.5. *Let G be a group, $a \in G$ and $n \in \mathbb{N}$. Then*

(a) $a^0 := e$,

(b) Inductively $a^{n+1} := a^n a$.

(c) $a^{-n} := (a^{-1})^n$.

(d) We say that a has finite order *if there exists a positive integer n with $a^n = e$. The smallest such positive integer is called the order of a and is denoted by $|a|$.*

We have $a^1 = a^0 a = ea = a$, $a^2 = a^1 a = aa$, $a^3 = a^2 a = (aa)a$, $a^4 = a^3 a = ((aa)a)a$ and

$$a^n = \underbrace{((\ldots(((aa)a)a)\ldots a)a)a}_{n\text{-times}}$$

Example 1.4.6.

$(1,2,3,4,5)^2 = (1,2,3,4,5) \circ (1,2,3,4,5) = (1,3,5,2,4)$.
$(1,2,3,4,5)^3 = (1,2,3,4,5)^2 \circ (1,2,3,4,5) = (1,3,5,2,4) \circ (1,2,3,4,5) = (1,4,2,5,3)$.
$(1,2,3,4,5)^4 = (1,2,3,4,5)^3 \circ (1,2,3,4,5) = (1,4,2,5,3)) \circ (1,2,3,4,5) = (1,5,4,3,2)$.
$(1,2,3,4,5)^5 = (1,2,3,4,5)^5 \circ (1,2,3,4,5) = (1,5,4,3,2)) \circ (1,2,3,4,5) = (1)(2)(3)(4)(5)$.
So $(1,2,3,4,5)$ has order 5.

Lemma 1.4.7. *Let G be a group, $a \in G$ and $n, m \in \mathbb{Z}$. Then*

(a) $a^n a^m = a^{n+m}$.

(b) $a^{nm} = (a^n)^m$.

Before we start the formal proof here is an informal argument:

$$a^n a^m = (\underbrace{aaa\ldots a}_{n\text{-times}})(\underbrace{aaa\ldots a}_{m\text{-times}}) = \underbrace{aaa\ldots a}_{n+m\text{-times}} = a^{n+m}$$

$$(a^n)^m = \underbrace{(\underbrace{aaa\ldots a}_{n\text{-times}})(\underbrace{aaa\ldots a}_{n\text{-times}})\ldots(\underbrace{aaa\ldots a}_{n\text{-times}})}_{m\text{-times}} = \underbrace{aaa\ldots a}_{nm\text{-times}} = a^{nm}$$

This informal proof has a couple of problems:
1. It only treats the case where n, m are positive.
2. The associative law is used implicitly and its not clear how.

Proof. (a) We first use induction on m to treat the case where $m \geq 0$. If $m = 0$, then $a^n a^0 = a^n e = a^n = a^{n+0}$ and (a) is true.

If $m = 1$ and $n \geq 0$, then $a^n a^1 = a^n a = a^{n+1}$ by definition of a^{n+1}. If $m = 1$ and $n < 0$, then

$$a^n a^1 = (a^{-1})^{(-n)} a = (a^{-1})^{(-n-1)} a^{-1}) a = a^{-1} - (n+1) = a^{n+1},$$

and so (a) holds for $m = 1$.

Suppose inductively that (a) is true for m. Then

$$a^n a^m = a^{n+m}, \tag{1}$$

and so

$$a^n a^{m+1} = a^n (a^m a) = (a^n a^m) a \overset{(1)}{=} a^{n+m} a = a^{(n+m)+1} = a^{n+(m+1)}.$$

So (a) holds for $m+1$ and so by The Principal of Mathematical Induction for all $m \in \mathbb{N}$.

Let m be an arbitrary positive integer. From (a) applied with $n = -m$ we conclude that $a^{-m} a^m = a^0 = a$ and so for all $m \in \mathbb{N}$,

$$a^{-m} = (a^m)^{-1}. \tag{2}$$

From (a) applied with $n - m$ in place of n, $a^{n-m} a^m = a^n$. Multiplication from left with a^{-m} and using (2) gives $a^{n-m} = a^n a^{-m}$. Since m is an arbitrary positive integer, $-m$ is an arbitrary negative integer. So (a) also holds for negative integers.

(b) Again we first use induction on m to prove (b) in the case that $m \in \mathbb{N}$. For $m = 0$ both sides in (b) equal e. Suppose now that (b) holds for $m \in \mathbb{N}$. Then

$$a^{n(m+1)} = a^{nm+n} = a^{nm} a^n = (a^n)^m (a^n)^1 = (a^m)^{m+1}.$$

So (b) holds also for $m+1$ and so by induction for all $m \in \mathbb{N}$.

We compute

$$a^{n(-m)} = a^{-(nm)} = (a^{nm})^{-1} = ((a^n)^m)^{-1} = (a^n)^{-m},$$

and so (b) also holds for negative integers. $\square$

1.5 Subgroups

Definition 1.5.1. *Let $(G, *)$ and $(H, \triangle)$ be groups. Then $(H, \triangle)$ is called a* subgroup *of $(G, *)$ provided that*

(a) $H \subseteq G$.

(b) $a \triangle b = a * b$ for all $a, b \in H$.

If often just say that H is a subgroup of G and write $H \leq G$ if $(H, \triangle)$ is a subgroup of $(G, *)$.

Example 1.5.2.

(1) $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$.

(2) $(\mathbb{Q}\setminus\{0\},\cdot)$ is a subgroup of $(\mathbb{R}\setminus\{0\},\cdot)$.

(3) $(D_4,\circ)$ is a subgroup of $(\mathrm{Sym}(4),\circ)$.

(4) Sym(4) is not a subgroup of Sym(5), since Sym(4) is not subset of Sym(5).

Proposition 1.5.3 (Subgroup Proposition). *(a) Let $(G,*)$ be a group and H a subset of G. Suppose that*

(i) H is closed under $*$, that is $a*b\in H$ for all $a,b\in H$.

(ii) $e_G\in H$.

(iii) H is closed under inverses, that is $a^{-1}\in H$ for all $a\in H$.(where a^{-1} is the inverse of a in G with respect to $*$.

Define $\triangle : H\times H\to H,(a,b)\to a*b$. Then $\triangle$ is a well-defined binary operation on H and $(H,\triangle)$ is a subgroup of $(G,*)$.

(b) Suppose $(H,\triangle)$ is a subgroup of $(G,*)$. Then

(a) (a:i),(a:ii) and (a:iii) hold.

(b) $e_H=e_G$.

(c) Let $a\in H$. Then the inverse of a in H with respect to $\triangle$ is the same as the inverse of a in G with respect to $*$.

Proof. (a) We will first verify that $(H,\triangle)$ is a group.

By (a:i), $\triangle$ really is a function from $H\times H$ to H and so $\triangle$ is a well-defined binary operation on H.

Let $a,b,c\in H$. Then since $H\subseteq G$, a,b,c are in H. Thus since $*$ is associative,

$$(a\triangle b)\triangle c=(a*b)*c=a*(b*c)=a\triangle(b\triangle c)$$

and so $\triangle$ is associative.

By (a:ii), $e_G\in H$. Let $h\in H$. Then $e_G\triangle h=e_G*h=h$ and $h\triangle e_G=h*e_G=h$ for all $h\in h$. So e_G is an identity of $\triangle$ in H.

Let $h\in H$. Then by (a:iii), $h^{-1}\in H$. Thus $h\triangle h^{-1}=h*h^{-1}=e$ and $h^{-1}\triangle h=h^{-1}*h=e$. So h^{-1} is an inverse of h with respect to $\triangle$.

So $(H,\triangle)$ is a group. By assumption H is a subset of G and by definition of $\triangle$, $a\triangle b=a*b$ for all $a,b\in H$. So $(H,\triangle)$ is a subgroup of $(G,*)$.

(b) Let $a, b \in H$. Then by definition of a subgroup $a * b = a \triangle b$. Since $\triangle$ is a binary operation on H, $a \triangle b \in H$ and so $a * b \in H$. (a:i) holds. Since $(H, \triangle)$ is a group it has an identity e_H. In particular, $e_H = e_H \triangle e_H = e_H * e_H$. Since $e_H \in G$ we also have $e_H = e_H * e_G$ and the Cancellation Law 1.4.3 gives $e_G = e_H$. Thus $e_H = e_G \in H$ and (a:iii) holds. Since $(H, \triangle)$ is a group, a has an inverse $b \in H$ with respect to $\triangle$. Thus $a * b = a \triangle b = e_H = e$ and so $b = a^{-1}$. Thus $a^{-1} = b \in H$ and (a:ii) holds. □

Lemma 1.5.4. *Let G be a group.*

(a) Let A and B be subgroups of G. Then $A \cap B$ is a subgroup of G.

(b) Let $(G_i, i \in I)$ a family of subgroups of G, i.e. I is a set and for each $i \in I, G_i$ is a subgroup of G. Then

$$\bigcap_{i \in I} G_i$$

is a subgroup of G.

Proof. Note that (a) follow from (b) if we set $I = \{1, 2\}$, $G_1 = A$ and $G_2 = B$. So it suffices to prove (b).

Let $H = \bigcap_{i \in I} G_i$. Then for $g \in G$.

$$(*) \qquad g \in H \text{ if and only if } g \in G_i \text{ for all } i \in I$$

To show that H is a subgroup of G we use 1.5.3

Let $a, b \in H$. We need to show

(i) $ab \in H$. (ii) $e \in H$ (iii) $a^{-1} \in H$.

Since $a, b \in H$ (*) implies $a, b \in G_i$ for all $i \in I$. Since G_i is a subgroup of G, $ab \in G_i$ for all $i \in I$ and so by (*), $ab \in H$. So (i) holds.

Since G_i is a subgroup of G, $e \in G_i$ and so by (*), $e \in H$ and (ii) holds.

Since G_i is a subgroup of G and $a \in G_i$, $a^{-1} \in G_i$ and so by (*), $a^{-1} \in H$. Thus (iii) holds. □

Lemma 1.5.5. *Let I be a subset of the group G.*

- *Put $H_1 := \bigcap_{I \subseteq H \leq G} H$. In words, H_1 is the intersection of all the subgroups of G containing I.*

- *Let H_2 be a subgroup of G such that $I \subseteq H$ and whenever K is a subgroup of G with $I \subseteq K$, then $H_2 \subseteq K$.*

- *Let J be subset of G. We say that e is* product *of length* 0 *of J. Inductively, we say that $g \in G$ is a product of length $k+1$ of J if $g = hj$ where h is a product of length k of J and $j \in J$. Set $I^{-1} = \{i^{-1} \mid i \in I\}$ and let H_3 be the set of all products of arbitrary length of $I \cup I^{-1}$.*

Then $H_1 = H_2 = H_3$.

Proof. It suffices to proof that $H_1 \subseteq H_2$, $H_2 \subseteq H_2$ and $H_3 \subseteq H_1$.

Since H_2 is a subgroup of G containing I and H_1 is the intersection of all such subgroups, $H_1 \subseteq H_2$.

We will show that H_3 is a subgroup of G. For this we show:

1°. *Let $J \subseteq G$, $k, l \in \mathbb{N}$, g a product of length k and h a product of length l of J. Then gh is a product of length $k+l$ of J.*

The proof is by induction on l. If $l = 0$, then $h = e$ and so $gh = g$ is a product of length $k = k + 0$. So (1°) holds for $l = 0$. Suppose (1°) holds for $l = t$ and let h be product of length $t+1$. Then by definition $h = fj$ where f is a product of length t and $j \in J$. We have $gh = g(fj) = (gf)j$. By induction gf is a product of length $k+t$ and so by definition $gh = (gf)j$ is a product of length $(k+t)+1 = k+(t+1)$. So (1°) also holds for $k = t+1$. Hence by the Principal of Mathematical Induction, (1°) holds for all k.

Next we show:

2°. *Let $J \subseteq G$ with $J = J^{-1}$, let $n \in \mathbb{N}$ and let g be a product of length n of J. Then g^{-1} is also a product of length n of J.*

Again the proof is by induction on n. If $n = 0$, then $g = e = g^{-1}$ and (2°) holds. So suppose (2°) holds for $n = k$ and let g be a product of length $k+1$. Then $g = hj$ with h a product of length k and $j \in J$. By induction, h^{-1} is a product of length k. Now $g^{-1} = (hj)^{-1} = j^{-1}h^{-1}$. By assumption $j^{-1} \in J$ and so $j^{-1} = ej^{-1}$ is a product of length 1. So by (1°), $g^{-1} = j^{-1}k^{-1}$ is a product of length $k+1$. So (2°) holds for $n = k+1$. Thus (2°) follows from the Principal of Mathematical Induction.

Note that (1°) implies that H_3 is is closed under multiplication. e is the product of length 0 of $I \cup I^{-1}$ and so $e \in H_3$. By (2°), H_2 is closed under inverses. Hence by 1.5.3 I is a subgroup of H. Clearly $I \subseteq H_3$ (products of length 1) and so by the assumptions on H_2, $H_2 \subseteq H_3$.

Let K be a subgroup of G with $I \subseteq K$. Since K is closed under inverses (1.5.3), $I^{-1} \subseteq K$. Since K is closed under multiplication an easy induction proof shows that any product of elements of $I \cup I^{-1}$ is in K. Thus $H_3 \subseteq K$. Since this holds for all such K, $H_3 \subseteq H_1$. □

Definition 1.5.6. *Let I be a subset of the group G. Then*

$$\langle I \rangle = \bigcap_{I \subseteq H \leq G} H$$

$\langle I \rangle$ is called the subgroup of G generated by I

By 1.5.5 $\langle I\rangle$ as the smallest subgroup of G containing I.

Example 1.5.7.

(1) We compute $\langle(1,2),(2,3)\}$ in Sym(4). Let $I=\{(1,2),(2,3)\}$. Then

$$I^{-1}=\{i^{-1}\mid i\in I\}=\{(1,2)^{-1},(2,3)^{-1}\}=\{(1,2),(2,3)\}=I$$

and so

$$I\cup I^{-1}=I=\{(1,2),(2,3)\}$$

So we have to compute all possible products of $\{(1,2),(2,3)\}$. In the following we say that g is a new product of length k, if g is a product of length k of $\{(1,2),(2,3)\}$, but not a product of $\{(1,2),(2,3)\}$ of any length less than k. Observe that any new product of length k is of the form hj there h is a new product of length $k-1$ and j is one of $(1,2)$ and $(2,3)$.

Products of length 0: (1)

Products of length 1: (1,2), (2,3).

Products of length 2:

$(1,2)\circ(1,2)=(1)$

$(1,2)\circ(2,3)=(1,2,3)$

$(2,3)\circ(1,2)=(1,3,2)$

$(2,3)\circ(2,3)=(1)$

New Products of length 2: $(1,2,3),(1,3,2)$

New Products of length 3: Note that a new product of length three is of the form hj with h a new product of length two (and so $h=(1,2,3)$ or $(1,3,2)$) and $j=(1,2)$ or $(2,3)$.

$(1,2,3)\circ(1,2)=(1,3)$

$(1,2,3)\circ(2,3)=(1,2)$

$(1,3,2)\circ(1,2)=(2,3)$

$(1,3,2)\circ(2,3)=(1,3)$

Only new product of length 3: $(1,3)$

Possible new products of length 4:

$(1,3)\circ(1,2)=(1,2,3)$

$(1,3)\circ(2,3)=(1,3,2)$

There is no new product of length 4 and so also no new product of length larger then 4. Thus

$$\langle(1,2),(2,3)\rangle=\{(1,(1,2),(2,3),(1,2,3),(1,3,2),(2,3)\}.$$

(2) Let G be any group and $a \in G$. Put $H = \{a^n \mid n \in \mathbb{Z}\}$. We claim that $H = \langle a \rangle$. We first show that H is a subgroup of G. Indeed, $a^n a^m = a^{n+m}$, so H is closed under multiplication. $e = a^0 \in H$ and $(a^n)^{-1} = a^{-n}$, so H is closed under inverses. Thus by the Subgroup Proposition, H is a subgroup. Clearly any subgroup of G containing a must contain H and so by 1.5.5, $H = \langle a \rangle$.

(3) We will show that $D_4 = \langle (1,3), (1,2)(3,4) \rangle$. For this it suffices to write every element in D_4 as a product of elements from $(1,3)$ and $(1,2)(3,4)$. Straightforward computation show that

$$\begin{array}{rclcrcl}
(1) & = & \text{empty product} & & (1,2,3,4) & = & (1,3)\circ(1,2)(3,4) \\
(1,3)(2,4) & = & ((1,3)\circ(1,2)(3,4))^2 & & (1,4,3,2) & = & (1,2)(3,4)\circ(1,3) \\
(1,4)(2,3) & = & (1,3)\circ(1,2)(3,4)\circ(1,3) & & (1,2)(3,4) & = & (1,2)(3,4) \\
(2,4) & = & (1,2)(3,4)\circ(1,3)\circ(1,2)(3,4) & & (1,3) & = & (1,3)
\end{array}.$$

(4) Let G be a group and $g \in G$ with $|g| = n$ for some $n \in \mathbb{Z}^+$. By (2),

$$G = \{g^m \mid m \in \mathbb{Z}\}.$$

Let $m \in \mathbb{Z}$. By the Division Algorithm, [Hung, Theorem 1.1] $m = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $g^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r$. Thus

$$\langle g \rangle = \{g^r \mid 0 \leq r < n\}.$$

Suppose that $0 \leq r < s < n$. Then $0 < s - r < n$ and so by the definition of $|g|$, $g^{s-r} \neq e$. Multiplication with g^r gives $g^s \neq g^r$. So the elements $g^r, 0 \leq r < n$ are pairwise distinct and therefore

$$|\langle g \rangle| = n = |g|.$$

1.6 Homomorphisms

Definition 1.6.1. *Let $f : A \to B$ be a function. Then* $\operatorname{Im} f := \{f(a) \mid a \in A\}$. $\operatorname{Im} f$ *is called the* image *of f.*

Lemma 1.6.2. *Let $f : A \to B$ be a function and define $g : A \to \operatorname{Im} f, a \to f(a)$.*

(a) g is onto.

(b) f is 1-1 if and only if g is 1-1.

Proof. (a) Let $b \in \operatorname{Im} f$. Then by definition of $\operatorname{Im} f$, $b = f(a)$ for some $a \in A$. Thus $g(a) = f(a) = b$ and so g is onto.

(b) Suppose f is 1-1 and let $a, d \in A$ with $g(a) = g(d)$. Then by definition of g, $g(a) = f(a)$ and $g(d) = f(d)$. Thus $f(a) = f(d)$. Since f is 1-1, $a = d$. Hence g is 1-1.

Similarly if g is 1-1, then also f is 1-1. □

Definition 1.6.3. *Let $(G, *)$ and $(H, \Box)$ be groups.*

(a) A homomorphism *from $(G, *)$ from to $(H, \Box)$ is a function $f : G \to H$ such that*

$$f(a * b) = f(a) \Box f(b)$$

for all $a, b \in G$.

(b) An isomorphism *from G to H is a 1-1 and onto homomorphism from G to H.*

(c) If there exists an isomorphism from G to H we say that G is isomorphic *to H and write $G \cong H$.*

Example 1.6.4.

(1) Let $(H, *)$ be any group, $h \in H$ and define $f : \mathbb{Z} \to H, m \to h^m$. By 1.4.7(a), $f(n + m) = h^{n+m} = h^n * h^m = f(n) * f(m)$. So f is a homomorphism from $(\mathbb{Z}, +)$ to $(H, *)$.

(2) Let I and J be sets with $I \subseteq J$. For $f \in \operatorname{Sym}(I)$ define $\phi_f : I \to I$ by

$$\phi_f(j) = \begin{cases} f(j) & \text{if } j \in I \\ j & \text{if } j \notin I \end{cases}.$$

Let $f, g \in \operatorname{Sym}(I)$ we will show that

$$(*) \qquad \phi_f \circ \phi_g = \phi_{f \circ g}.$$

Note that this is the case if and only if $(\phi_f \circ \phi_g)(j) = \phi_{f \circ g}(j)$ for all $j \in J$. We consider the two cases $j \in I$ and $j \notin I$ separately.

If $j \in I$, then since g is a permutation of I, also $g(j) \in I$. So

$$(\phi_f \circ \phi_g)(j) = \phi_f(\phi_g(j)) = \phi_f(g(j)) = f(g(j)) = (f \circ g)(j) = \Phi(f \circ g)(j).$$

If $j \notin I$ then

$$\phi_g(j) = \phi_f(\phi_g(j)) = \phi_f(j)) = j = \Phi(f \circ g)(j).$$

So in both cases $(\phi_f \circ \phi_f)(j) = \Phi(f \circ g)(j)$. So (*) holds.

For (*) applied with $g = f^{-1}$,

$$\phi_f \circ \phi_{f^{-1}} = \phi_{f \circ f^{-1}} = \phi_{\mathrm{id}_I} = \phi_J.$$

It follows that ϕ_f is a bijection. Hence $\phi_f \in \mathrm{Sym}(J)$ and so we can can define

$$\Phi : \mathrm{Sym}(I) \to \mathrm{Sym}(J), f \to \phi_f.$$

We claim that Φ is a 1-1 homomorphism.

To show that Φ is 1-1 let $f, g \in \mathrm{Sym}(I)$ with $\phi_f = \phi_g$. Then for all $i \in I$, $f(i) = \phi_f(i) = \phi_g(i) = g(i)$ and so $f = g$. Hence Φ is 1-1.

By (*)

$$\Phi(f \circ g) = \phi_{f \circ g} = \phi_f \circ \phi_g = \Phi(f) \circ \Phi(g)$$

and so Φ is a homomorphism.

Lemma 1.6.5. *Let $f : G \to H$ be a homomorphism of groups.*

(a) $f(e_G) = e_H$.

(b) $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$.

(c) $\mathrm{Im}\, f$ *is a subgroup of* H.

(d) If f *is 1-1, then* $G \cong \mathrm{Im}\, f$.

Proof. (a) $f(e_G)f(e_G) \overset{\text{f hom}}{=} f(e_G e_G) \overset{\text{def } e_G}{=} f(e_G) \overset{\text{def } e_H}{=} e_H f(e_G)$. So the Cancellation Law 1.4.3 implies $f(e_G) = e_H$.

(b) $f(a)f(a^{-1}) \overset{\text{f hom}}{=} f(aa^{-1}) \overset{\text{def } a^{-1}}{=} f(e_G) \overset{\text{(a)}}{=} e_H$ and so by 1.4.4(c) , $f(a^{-1}) = f(a)^{-1}$.

(c) We apply 1.5.3. Let $x, y \in \mathrm{Im}\, f$. Then by definition of $\mathrm{Im}\, f$, $x = f(a)$ and $y = f(b)$ for some $a, b \in G$.

Thus $xy = f(a)f(b) = f(ab) \in \mathrm{Im}\, f$.

By (a), $e_H = f(e_G) \in \mathrm{Im}\, f$.

By (b), $x^{-1} = f(a)^{-1} = f(a^{-1}) \in \mathrm{Im}\, F$. So $\mathrm{Im}\, f$ fulfills all three conditions in 1.5.3 and so $\mathrm{Im}\, f$ is a subgroup of H.

(d) Define $g : G \to \mathrm{Im}\, f, a \to f(a)$. Since f is 1-1, 1.6.2 implies that g is 1-1 and onto. Since f is homomorphism, $g(ab) = f(ab) = f(a)f(b) = g(a)g(b)$ for all $a, b \in G$ and so also g is a 1-1 homomorphism. Hence g is an isomorphism and so $G \cong \mathrm{Im}\, f$. $\square$

Definition 1.6.6. *Let G be a group. Then G is called a* group of permutations *or a* permutation group *if $G \leq \mathrm{Sym}(I)$ for some set I.*

Theorem 1.6.7 (Cayley's Theorem)**.** *Every group is isomorphic to group of permutations.*

Proof. We will show that G is isomorphic to a subgroup of $\mathrm{Sym}(G)$. For $g \in G$ define

$$\phi_g : G \to G, x \to gx.$$

We claim that $\phi_g \in \mathrm{Sym}(G)$, that is ϕ_g is 1-1 and onto.

To show that ϕ_g is 1-1, let $x, y \in G$ with $\phi_g(x) = \phi_g(y)$ for some $x, y \in G$, then $gx = gy$ and so by the Cancellation Law 1.4.3 $x = y$. So ϕ_g is 1-1.

To show that ϕ_g is onto, let $x \in G$. Then $\phi_g(g^{-1}x) = g(g^{-1}x) = x$ and ϕ_g is onto. Define

$$f : G \to \mathrm{Sym}(G), g \to \phi_g.$$

To show that f is a homomorphism let $a, b \in G$. Then for all $x \in G$

$$f(ab)(x) = \phi_{ab}(x) = (ab)x = a(bx)$$

and

$$(f(a) \circ f(b)(x) = (\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x) = \phi_a(bx) = a(bx)$$

So $f(ab) = f(a) \circ f(b)$ and f is a homomorphism.

Finally to show that f is 1-1, let $a, b \in G$ with $f(a) = f(b)$. Then $\phi_a = \phi_b$ and so

$$a = ae = \phi_a(e) = \phi_b(e) = be = b$$

Hence $a = b$ and f is 1-1. Hence by 1.6.5(d), G is isomorphic to the subgroup $\mathrm{Im}\, f$ of $\mathrm{Sym}(G)$. □

Example 1.6.8.

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Put

$$a = (0,0), b = (1,0), c = (0,1) \text{ and } d = (1,1).$$

Then $G = \{a, b, c, d\}$. For each $g \in G$ we will compute ϕ_g.

For $x \in G$ we have $\phi_a(x) = (0,0) + x = x$. So

$$\phi_a = \mathrm{id}_G = (a)(b)(c)(d).$$

$\phi_b(a) = b + a = (1,0) + (0,0) = (1,0) = b.$
$\phi_b(b) = b + b = (1,0) + (1,0) = (0,0) = a.$
$\phi_b(c) = b + c = (1,0) + (0,1) = (1,1) = d.$
$\phi_b(d) = b + d = (1,0) + (1,1) = (0,1) = c.$

Thus

$$\phi_b = (a,b)(c,d).$$

$\phi_c(a) = c + a = (0,1) + (0,0) = (0,1) = c.$
$\phi_c(c) = c + c = (0,1) + (0,1) = (0,0) = a.$
$\phi_c(b) = c + b = (0,1) + (1,0) = (1,1) = d.$
$\phi_c(d) = c + d = (0,1) + (1,1) = (1,0) = b.$
Thus

$$\phi_c = (a,c)(b,d).$$

$\phi_d(a) = c + a = (1,1) + (0,0) = (1,1) = d.$
$\phi_d(d) = d + d = (1,1) + (1,1) = (0,0) = a.$
$\phi_d(b) = d + b = (1,1) + (1,0) = (0,1) = c.$
$\phi_d(c) = d + c = (1,1) + (0,1) = (1,0) = b.$
Thus

$$\phi_d = (a,d)(b,c).$$

(We could also have computed ϕ_d as follows: Since $d = a + c$, $\phi_c = \phi_a \circ \phi_b = (a,b)(c,d) \circ (a,c)(b,d) = (a,d)(b,c)$)

Hence

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \cong (\{(a), (a,b)(c,d), (a,c)(b,d), (a,d)(b,c)\}, \circ).$$

Using $1, 2, 3, 4$ in place of a, b, c, d we conclude (see Homework 3#7 for the details)

$$(\mathbb{Z}_2 \times \mathbb{Z}_2, +) \cong (\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}, \circ)$$

In general we see that a finite group of order n is isomorphic to a subgroup of $\mathrm{Sym}(n)$.

1.7 Lagrange's Theorem

Definition 1.7.1. *Let K be a subgroup of the group G and $a, b \in G$. Then we say that a is* congruent *to b modulo K and write $a \equiv b \pmod{K}$ if $a^{-1}b \in K$.*

Notice the the definition of $' \equiv \pmod{K}'$ given here is different than in Hungerford. In Hungerford the above relation is called "left congruent" and denoted by $' \approx \pmod{K}'$.

Example 1.7.2.

Let $G = \mathrm{Sym}(3)$, $K = \langle(1,2)\rangle = \{(1), (1,2)\}$, $a = (2,3)$, $b = (1,2,3)$ and $c = (1,3,2)$. Then

$$a^{-1}b = (2,3) \circ (1,2,3) = (1,3) \notin K$$

and

$$a^{-1}c = (2,3) \circ (1,3,2) = (1,2) \in K.$$

Hence

$$(2,3) \not\equiv (1,2,3) \pmod K$$

and

$$(2,3) \equiv (1,3,2) \pmod K.$$

Proposition 1.7.3. *Let K be a subgroup of the group G. Then $' \equiv \pmod K'$ is an equivalence relation on G.*

Proof. We need to show that $' \equiv \pmod K'$ is reflexive, symmetric and transitive. Let $a, b, c \in G$.

Since $a^{-1}a = e \in K$, we have $a \equiv a \pmod K$ and so $' \equiv \pmod K'$ is reflexive.

Suppose that $a \equiv b \pmod K$. Then $a^{-1}b \in K$. Since K is closed under inverses, $(a^{-1}b)^{-1} \in K$ and so $b^{-1}a \in K$. Hence $b \equiv a \pmod K$ and $' \equiv \pmod K'$ is symmetric.

Suppose that $a \equiv b \pmod K$ and $b \equiv c \pmod K$. Then $a^{-1}b \in K$ and $b^{-1}c \in K$. Since K is closed under multiplication, $(a^{-1}b)(b^{-1}c) \in K$ and thus $a^{-1}c \in K$. Hence $a \equiv c \pmod K$ and $' \equiv \pmod K'$ is transitive. □

Definition 1.7.4. *Let $(G, *)$ be a group and $g \in G$*

(a) Let A, B be subsets of G and $g \in G$. Then

$$A * B := \{a * b \mid a \in A, b \in B\},$$

$$g * A = \{g * a \mid a \in A\}$$

and

$$A * g := \{a * g \mid a \in A\}.$$

We often just write AB, gA and Ag for $A * B, g * A$ and $A * g$.

(b) Let K be a subgroup of the group $(G, *)$. Then $g * K$ called the left coset *of g in G with respect to K. Put*

$$G/K := \{gK \mid g \in G\}.$$

So G/K is the set of left cosets of K in G.

Example 1.7.5.

Let $G = \mathrm{Sym}(3)$, $K = \{(1), (1,2)\}$, $a = (2,3)$. Then

$$a \circ K = \{(1,2) \circ k \mid k \in K\} = \{(2,3) \circ (1), (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}.$$

Proposition 1.7.6. *Let K be a subgroup of the group G and $a, b \in G$. Then aK is the equivalence class of $' \equiv \pmod K'$ containing a. Moreover, the following statements are equivalent* *(a)* $b = ak$ *for some* $k \in K$.

(b) $a^{-1}b = k$ *for some* $k \in K$.

(c) $a^{-1}b \in K$.

(d) $a \equiv b \pmod{K}$.

(e) $b \in aK$.

(f) $aK \cap bK \neq \emptyset$.

(g) $aK = bK$.

(h) $a \in bK$.

(i) $b \equiv a \pmod{K}$.

(j) $b^{-1}a \in K$.

(k) $b^{-1}a = j$ *for some* $j \in K$.

(l) $a = bj$ *for some* $j \in K$.

Proof. (a) $\iff$ (b) : Multiply with a^{-1} from the left and use the Cancellation Law 1.4.3.

(b) $\iff$ (c) : Obvious.

(c) $\iff$ (d) : Follows from the definition of $' \equiv \pmod{K}'$.

(a) $\iff$ (e) : Note that $b = ak$ for some $k \in K$ if and only if $b \in \{ak \mid k \in K\}$, that is if and only if $b \in aK$.

So (a)-(e) are equivalent statements. Let $[a]$ be the equivalence class of $' \equiv \pmod{K}'$ containing a. So $[a] = \{b \in G \mid a \equiv b \pmod{K}\}$. Since (d) and (e) are equivalent, we conclude that $[a] = \{b \in G \mid b \in aK\} = aK$. Thus $[a] = aK$

Therefore Theorem A.1.3 implies that (d)-(k) are equivalent. In particular, (g) is equivalent to (a)-(c). Since the statement (g) is symmetric in a and b we conclude that (g) is also equivalent to (j)-(l). □

Proposition 1.7.7. *Let K be a subgroup of the group G.*

(a) Let $T \in G/K$ and $a \in G$. Then $a \in T$ if and only if $T = aK$.

(b) G is the disjoint union of its cosets, that is every element of G lies in a unique coset of K.

(c) Let $T \in G/K$ and $a \in T$. Then the map $\delta : K \to T, k \to ak$ is a bijection. In particular, $|T| = |K|$.

Proof. (a) Since $T \in G/K$, $T = bK$ for some $b \in G$. Since $a = ae$, $a \in aK$. Conversely if $a \in T$ then $a \in aK \cap T$ and $aK \cap bK \neq \emptyset$. Thus by 1.7.6(f),(g), $aK = bK = T$.

(b) Let $a \in G$. Then by (a), aK is the unique coset of K containing a.

(c) Let $t \in T$. By (a) $T = aK = \{ak \mid k \in K\}$ and so $t = bk$ for some $k \in K$. Thus $\delta(k) = t$ and δ is onto.

Let $k, l \in K$ with $\delta(k) = \delta(l)$. Then $gk = gl$ and the Cancellation Law 1.4.3 implies that $k = l$. Thus δ is 1-1. So δ is a bijection and hence $|K| = |T|$. □

Example 1.7.8.

Let $G = \mathrm{Sym}(3)$ and $K = \{(1), (1,2)\}$. We have

$$(1) \circ K = \{(1) \circ k \mid k \in K\} = \{(1) \circ (1), (1) \circ (1,2)\} = \{(1), (1,2)\}.$$

So K is a coset of K containing $(1,2)$ and thus by 1.7.7(a) $(1,2)\circ K = K$. Just for fun we will verify this directly:

$$(1,2)\circ K = \{(1,2)\circ(1), (1,2)\circ(1,2)\} = \{(1,2),(1)\} = K.$$

Next we compute the coset of K with respect to $(2,3)$:

$$(2,3)\circ K = \{(2,3)\circ(1), (2,3)\circ(1,2)\} = \{(2,3),(1,3,2)\}.$$

and so by Proposition 1.7.7(a) also $(1,3,2)\circ K = \{\{(2,3),(1,3,2)\}$. Again we do a direct verification:

$$(1,3,2)\circ K = \{(1,3,2)\circ(1), (1,3,2)\circ(1,2)\} = \{(1,3,2),(2,3)\}.$$

The coset of K with respect to $(1,3)$ is

$$(1,3)\circ K = \{(1,3)\circ(1), (1,3)\circ(1,2)\} = \{(1,3),(1,2,3)\}$$

and so by Proposition 1.7.7(a) also $(1,2,3)\circ K = \{(1,3),(1,2,3)\}$. We verify

$$(1,2,3)\circ K = \{(1,2,3)\circ(1), (1,2,3)\circ(1,2)\} = \{(1,2,3),(1,3)\}$$

Thus G/K consists of the three cosets $\{(1,2),(1)\}$, $\{(2,3),(1,3,2)\}$ and $\{(1,2,3),(1,3)\}$. So indeed each of the cosets has size $|K| = 2$ and each element of $\mathrm{Sym}(3)$ lies in exactly one of the three cosets.

Theorem 1.7.9 (Lagrange)**.** *Let G be a finite group and K a subgroup of G. Then*

$$|G| = |K|\cdot|G/K|.$$

In particular, $|K|$ divides $|G|$.

Proof. By 1.7.7(b), G is the disjoint union of the cosets of K in G. Hence

$$|G| = \sum_{T\in G/K} |T|.$$

By 1.7.7(c), $|T| = |K|$ for all $T\in G/K$ and so

$$|G| = \sum_{T\in G/K} |T| = \sum_{T\in G/K} |K| = |K|\cdot|G/K|.$$

$\square$

Example 1.7.10.

(1) $|D_4| = 8$ and $|\mathrm{Sym}(4)| = 4! = 24$. Hence $|\mathrm{Sym}(4)/D_4| = 24/8 = 3$. So D_4 has three cosets in $\mathrm{Sym}(4)$.

(2) Let $H = \langle (1,2) \rangle \leq \mathrm{Sym}(3)$. Since $\mathrm{Sym}(3)$ has order 6 and H has order 2, $|\mathrm{Sym}(3)/H| = 3$.

(3) Since 5 does not divide 24, $\mathrm{Sym}(4)$ does not have subgroup of order 5.

Corollary 1.7.11. *Let G be a finite group.*

(a) If $a \in G$, then the order of a divides the order of G.

(b) If $|G| = n$, then $a^n = e$ for all $a \in G$.

Proof. (a) By Example 1.5.7(4), $|a| = |\langle a \rangle|$ and by Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$.

(b) Let $m = |a|$. By (a) $n = mk$ for some $k \in \mathbb{Z}$ and so $a^n = a^{mk} = (a^m)^k = e^k = e$. $\square$

Example 1.7.12.

Let $g \in \mathrm{Sym}(4)$. We compute the order of g depending on the cycle type of g. Let $\{a, b, c, d\} = \{1, 2, 3, 4\}$

(1) $g = (a)(b)(c)(d)$. Then $|g| = 1$.

(2) $g = (a, b)(c)(d)$. Then $g^2 = (a)(b)(c)(d)$ and so $|g| = 2$.

(3) $g = (a, b, c)(d)$. Then $g^2 = (a, c, b)(d)$ and $g^3 = (a)(b)(c)(d)$. Thus $|g| = 3$.

(4) $g = (a, b, c, d)$. Then $g^2 = (a, c)(b, d)$, $g^3 = (a, d, c, b)$ and $g^4 = (a)(b)(c)(d)$. Thus $|g| = 4$

(5) $g = (a, b)(c, d)$. Then $g^2 = (a)(b)(c)(d)$ and so $|g| = 2$

So the elements in $\mathrm{Sym}(4)$ have orders $1, 2, 3$ or 4. Note that each of these number is a divisor of $\mathrm{Sym}(4)$. Of course we already knew that this to be true by 1.7.11(a).

For each of the five cycle types in (1)-(5) we now compute how many elements in $\mathrm{Sym}(4)$ have that cycle type.

(1) There is one element of the form $(a)(b)(c)(d)$. (Any of the 24 choices for the tuple (a, b, c, d) give the same element of $\mathrm{Sym}(4)$, namely the identity.)

(2) There are four ways to express the element $(a, b)(c)(d)$, namely

$$(a, b)(c)(d) = (b, a)(c)(d) = (a, b)(d)(c) = (b, a)(d)(c).$$

So there are $\frac{24}{4} = 6$ elements in $\mathrm{Sym}(4)$ of the form $(a, b)(c)(d)$.

(3) There are 3 ways to express the element $(a, b, c)(d)$, namely

$$(a, b, c)(d) = (b, c, a)(d) = (c, a, b)(d).$$

So there are $\frac{24}{3} = 8$ elements in $\mathrm{Sym}(4)$ of the form $(a, b, c)(d)$.

(4) There are 4 ways to express the element (a, b, c, d), namely

$$(a, b, c, d) = (b, c, d, a) = (c, d, a, b) = (d, a, b, c).$$

So there are $\frac{24}{4} = 6$ elements in Sym(4) of the form (a, b, c, d).

(5) There are 8 ways to express the element $(a, b)(c, d)$, namely

$$\begin{aligned} (a,b)(c,d) &= (b,a)(c,d) = (a,b)(d,c) = (b,a)(d,c) \\ &= (c,d)(a,b) = (c,d)(b,a) = (d,c)(a,b) = (d,c)(b,a) . \end{aligned}$$

So there are $\frac{24}{8} = 3$ elements in Sym(4) of the form $(a, b)(c, d)$.

All together there are $1+6+8+6+3 = 24$ elements in Sym(4), just the way it should be.

Definition 1.7.13. *A group G is called* cyclic *if $G = \langle g \rangle$ for some $g \in G$.*

Lemma 1.7.14. *Let G be a group of finite order n.*

(a) Let $g \in G$. Then $G = \langle g \rangle$ if and only if $|g| = n$.

(b) G is cyclic if and only if G contains an element of order n.

Proof. (a) Let $g \in G$. Recall that by Example 1.5.7(4) , $|\langle g \rangle| = |g|$. Since G is finite, $G = \langle g \rangle$ if and only if $|G| = |\langle g \rangle|$. And so if and only if $n = |g|$.

(b) From (a) we conclude that there exists $g \in G$ with $|G| = \langle g \rangle$ if and only if there exists $g \in G$ with $|g| = n$. □

Corollary 1.7.15. *Any group of prime order is cyclic.*

Proof. Let G be group of order p, p a prime. Let $e \neq g \in G$. Then by 1.7.11(b) $|g|$ divides p. Since $g \neq e$, $|g| \neq 1$. Since p is a prime this implies $|g| = p$. So by 1.7.14(b), $G = \langle g \rangle$ and so g is cyclic. □

Example 1.7.16.

Let $G = \mathrm{GL}_2(\mathbb{Q})$, the group of invertible 2×2 matrices with coefficients in $\mathbb{Q}$ and let $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Then $g^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ for all $n \in \mathbb{Z}$ and so $\langle g \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\}$.

Thus $|g| = |\mathbb{Z}| = |\mathbb{Q}| = |G|$ (See section A.3 for a primer on cardinalities). Also $G \neq \langle g \rangle$. So we see that 1.7.14 is not true for infinite groups.

1.8 Normal Subgroups

Lemma 1.8.1. *Let G be a group, A, B, C subsets of G and $g, h \in G$. Then*

(a) $A(BC) = \{abc \mid a \in A, b \in B, c \in C\} = (AB)C$.

(b) $A(gh) = (Ag)h$, $(gB)h = g(Bh)$ *and* $(gh)C = g(hC)$.

(c) $Ae = A = Ae = (Ag)g^{-1} = g^{-1}(gA)$.

(d) $A = B$ *if and only if* $Ag = Bg$ *and if and only if* $gA = gB$.

(e) $A \subseteq B$ *if and only if* $Ag \subseteq Bg$ *and if and only if* $gA \subseteq gB$.

(f) If A is subgroup of G, then $AA = A$ and $A^{-1} = A$.

(g) $(AB)^{-1} = B^{-1}A^{-1}$.

(h) $(gB)^{-1} = B^{-1}g^{-1}$ *and* $(Ag)^{-1} = g^{-1}A^{-1}$.

Proof. (a)

$$\begin{array}{rcccccc} A(BC) & = & \{ad \mid a \in A, d \in BC\} & = & \{a(bc) \mid a \in A, b \in B, c \in C\} & & \\ & = & \{(ab)c \mid a \in A, b \in B, c \in C\} & = & \{fc \mid f \in AB, c \in C\} & = & (AB)C \ . \end{array}$$

(b) Observe first that

$$A\{g\} = \big\{ab \mid a \in A, b \in \{g\}\big\} = \big\{ag \mid a \in A\big\} = Ag,$$

and $\{g\}\{h\} = \{gh\}$. So the first statement in (b) follows from (a) applied with $B = \{g\}$ and $C = \{h\}$. The other two statements are proved similarly.

(c) $Ae = \{ae \mid a \in A\} = \{a \mid a \in A\} = A$. Similarly $Ae = A$. By (b) $(Ag)g^{-1} = A(gg^{-1}) = Ae = A$. Similarly $g(g^{-1}A) = A$.

(d) Clearly $A = B$ implies that $Ag = Bg$. If $Ag = Bg$, then by (b)

$$A = (Ag)g^{-1} = (Bg)g^{-1} = B.$$

So $A = B$ if and only if $Ag = Bg$ and (similarly) if and only if $gA = gB$.

(e) Suppose that $A \subseteq B$ and let $a \in A$. Then $a \in B$ and so $ag \in Bg$. Hence $Ag \subseteq Bg$. If $Ag \subseteq Bg$ we conclude that $(Ag)g^{-1} \subseteq (Bg)g^{-1}$ and by (c), $A \subseteq B$. Hence $A \subseteq B$ if and only if $Ag \subseteq Bg$. Similarly, $A \subseteq B$ if and only if $gA \subseteq gB$

(f) Since a subgroup is closed under multiplication, $ab \in A$ for all $a, b \in A$. So $AA \subseteq A$. Also $e \in A$ and so $A = eA \subseteq AA$. Thus $AA = A$.

Since A is closed under inverses, $A^{-1} = \{a^{-1} \mid a \in A\} \subseteq A$. Let $a \in A$, then $a^{-1} \in A$ and $a = (a^{-1})^{-1}$. So $a \in A^{-1}$ and $A \subseteq A^{-1}$. Thus $A = A^{-1}$.

$$(g)\qquad \begin{aligned}(AB)^{-1} &= \{d^{-1} \mid d \in AB\} &&= \{(ab)^{-1} \mid a \in A, b \in B\}\\ &= \{b^{-1}a^{-1} \mid a \in A, b \in B\} &&= \{cd \mid c \in B^{-1}, d \in A^{-1}\}\\ &= B^{-1}A^{-1}\end{aligned}$$

(h) By (g) applies with $A = \{g\}$:

$$(gB)^{-1} = \big(\{g\}B\big)^{-1} = B^{-1}\{g\}^{-1} = B^{-1}\{g^{-1}\} = B^{-1}g^{-1}$$

Similarly, $(Ag)^{-1} = g^{-1}A^{-1}$. □

Definition 1.8.2. *Let N be a subgroup of the group G. N is called a* normal *subgroup of G and we write $N \trianglelefteq G$ provided that*

$$gN = Ng$$

for all $g \in G$.

Example 1.8.3.

(1) $(1,3) \circ \{(1),(1,2)\} = \{(1,3),(1,2,3)\}$ and $\{1,(1,2)\} \circ (1,3) = \{(1,3),(1,3,2)\}$. So $\{(1),(1,2)\}$ is not a normal subgroup of $\mathrm{Sym}(3)$.

(2) Let $H = \langle(1,2,3)\rangle \leq \mathrm{Sym}(3)$. Then $H = \{(1),(1,2,3),(1,3,2)\}$. If $g \in H$ then $gH = H = Hg$. Now

$$(1,2) \circ H = \{(1,2),(2,3),(1,3)\} = \mathrm{Sym}(3) \setminus H$$

and

$$H \circ (1,2) = \{(1,2),(1,3),(2,3)\} = \mathrm{Sym}(3) \setminus H.$$

Indeed, $gH = \mathrm{Sym}(3) \setminus H = Hg$ for all $h \in \mathrm{Sym}(3) \setminus H$ and so H is a normal subgroup of $\mathrm{Sym}(3)$.

Definition 1.8.4. *A binary operation $*$ on I is called* commutative *if $a * b = b * a$ for all $a, b \in I$. A group is called* abelian *of its binary operation is commutative.*

Lemma 1.8.5. *Let G be an abelian group. Then $AB = BA$ for all subsets A, B of G. In particular, every subgroup of G is normal in G.*

Proof.

$$AB = \{ab \mid a \in A, b \in B\} = \{ba \mid a \in A, b \in B\} = BA$$

If N is a subgroup of G and $g \in G$, then $gN = Ng$ and so N is normal in G. $\square$

Lemma 1.8.6. *Let N be a subgroup of the group G. Then the following statements are equivalent:*

(a) N is normal in G.

(b) $aNa^{-1} = N$ for all $a \in G$.

(c) $aNa^{-1} \subseteq N$ for $a \in G$.

(d) $ana^{-1} \in N$ for all $a \in G$ and $n \in N$.

(e) Every right coset of N is a left coset of N.

Proof. (a) $\iff$ (b) :

$$\begin{array}{cccl} & N \trianglelefteq G & & \\ \iff & aN = Na \text{ for all } a \in G & - & \text{definition of normal} \\ \iff & (aN)a^{-1} = (Na)a^{-1} \text{ for all } a \in G & - & 1.8.1(d) \\ \iff & aNa^{-1} = N \text{ for all } a \in G & - & 1.8.1(a),(c) \end{array}$$

(b) $\iff$ (c) : Clearly (b) implies (c). Suppose (c) holds and let $a \in G$. From (c) applied with a^{-1} in place of a, $a^{-1}Na \subseteq N$. We compute

$$\begin{array}{cccl} & a^{-1}Na \subseteq N & & \\ \Longrightarrow & a(a^{-1}Na) \subseteq aN & - & 1.8.1(e) \\ \Longrightarrow & (a(a^{-1}N))a \subseteq aN & - & 1.8.1(a) \\ \Longrightarrow & Na \subseteq aN & - & 1.8.1(c) \\ \Longrightarrow & (Na)a^{-1} \subseteq (aN)a^{-1} & - & 1.8.1(d) \\ \Longrightarrow & N \subseteq aNa^{-1} & - & 1.8.1(a),(c) \end{array}$$

Thus

$$N \subseteq aNa^{-1}$$

for all $a \in G$. Together with (c) this gives $aNa^{-1} = N$ and so (c) implies (b).

(c) $\iff$ (d) : Since $aNa^{-1} = \{ana^{-1} \mid a \in N\}$, $aNa^{-1} \subseteq N$ if and only if $ana^{-1} \in N$ for all $m \in N$.

(a) $\iff$ (e) : Suppose (a) holds. Then $aN = Na$ and so every left coset is a right coset. Thus (a) implies (e).

Suppose (e) holds and let $a \in G$. Then aN is a left coset and so also a right coset. Since $a = ae \in aN$ we conclude that both Na and aN are right cosets containing a. So by 1.7.6 $Na = aN$. Thus N is normal in G and so (e) implies (a). □

Proposition 1.8.7 (Normal Subgroup Proposition)**.** *Let N be a subset of the group G. Then N is a normal subgroup of G if and only if*

(i) N is closed under multiplication, that is $ab \in N$ for all $a, b \in N$.

(ii) $e_G \in N$.

(iii) N is closed under inverses, that is $a^{-1} \in N$ for all $a \in N$.

(iv) N is invariant under conjugation, that is $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

Proof. By the Subgroup Proposition 1.5.3 N is a subgroup of G if and only if (i),(ii) and (iii) hold. By 1.8.6(d), N is normal in G if and only if N is a subgroup of G and (iv) holds. So N is normal subgroup if and only if (i)-(iv) hold. □

The phrase 'invariant under conjugation' comes from the fact for $a \in G$, then map

$$\mathrm{inn}_a : G \to G, g \to aga^{-1}$$

is called *conjugation* by a. Note that by Homework 3#2, inn_g is an isomorphism of G.

Corollary 1.8.8. *Let N be a normal subgroup of the group G, $a, b \in G$ and $T \in G/N$.*

(a) $(aN)(bN) = abN$.

(b) $(aN)^{-1} = a^{-1}N$.

(c) $NT = T$.

(d) $T^{-1} \in G/N$, $TT^{-1} = N$ and $T^{-1}T = N$.

Proof. (a) Since $N \trianglelefteq G$, $bN = Nb$. By 1.8.1 $NN = N$ and multiplication of subsets is associative, thus

$$(aN)(bN) = a(Nb)N = a(bN)N = ab(NN) = abN.$$

(b) By 1.8.1 $(aN)^{-1} = N^{-1}a^{-1} = Na^{-1} = a^{-1}N$.

(c) We may assume $T = aN$. Then

$$NT = N(aN) = (Na)N = (aN)N = a(NN) = aN = T.$$

(d) By (c), $T^{-1} = (aN)^{-1} = a^{-1}N$ and so $T^{-1} \in G/N$. Moreover,

$$TT^{-1} = (aN)(a^{-1}N) = (aNa^{-1})N \overset{1.8.6(\mathrm{b})}{=} NN \overset{1.8.1(\mathrm{f})}{=} N$$

and similarly $T^{-1}T = N$. □

Definition 1.8.9. *Let G be a group and $N \trianglelefteq G$. Then $*_{G/N}$ denotes the binary operation*

$$*_{G/N} : G/N \times G/N \to G/N, \quad (S,T) \to S * T$$

Note here that by 1.8.8(a), $S * T$ is a coset of N, whenever S and T are cosets of N. G/N is called the quotient group *of G with respect to N.*

Theorem 1.8.10. *Let G be a group and $N \trianglelefteq G$. Then $(G/N, *_{G/N})$ is group. The identity of G/N is*

$$e_{G/N} = N = eN,$$

and the inverse of $T = gN \in G/N$ with respect to $*_{G/N}$ is

$$(gN)^{-1} = T^{-1} = \{t^{-1} \mid t \in T\} = g^{-1}N.$$

Proof. By definition $*_{G/N}$ is a binary operation on G/N. By 1.8.1(a), $*_{G/N}$ is associative; by 1.8.8(c), N is an identity for $*_{G/N}$; and by 1.8.8(d), T^{-1} is an inverse of T. Finally by 1.8.8(b), if $T = gN$ then $T^{-1} = g^{-1}N$. □

Example 1.8.11.

(1) Let n be an integer. Then $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ is subgroup of $\mathbb{Z}$, with respect to addition. Since $\mathbb{Z}$ is abelian, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. So we obtain the quotient group $\mathbb{Z}/n\mathbb{Z}$. Of course this is nothing else as $\mathbb{Z}_n$, the integers modulo n, views as a group under addition.

(2) By 1.8.3(2) $\langle(1,2,3)\rangle$ is a normal subgroup of $\mathrm{Sym}(3)$. By Lagrange's Theorem $|\,\mathrm{Sym}(3)/\langle(1,2,3)\rangle|$ has order $\frac{6}{3} = 2$ and so $\mathrm{Sym}(3)/\langle(1,2,3)\rangle$ is a group of order 2.

$$\mathrm{Sym}(3)/\langle(1,2,3)\rangle = \left\{\, \{(1),(1,2,3),(1,3,2)\},\ \{(1,2),(1,3),(2,3)\} \,\right\}$$

The Multiplication Table is

$*$	$\{(1),(1,2,3),(1,3,2)\}$	$\{(1,2),(1,3),(2,3)\}$
$\{(1),(1,2,3),(1,3,2)\}$	$\{(1),(1,2,3),(1,3,2)\}$	$\{(1,2),(1,3),(2,3)$
$\{(1,2),(1,3),(2,3)\}$	$\{(1,2),(1,3),(2,3)\}$	$\{(1),(1,2,3),(1,3,2)\}$

Let $N = \langle(1,2,3)\rangle$. Then $\mathrm{Sym}(3)/N = \{(1)\circ N, (1,2)\circ N\}$ and we can rewrite the multiplication table as

$*$	$(1)\circ N$	$(1,2)\circ N$
$(1)\circ N$	$(1)\circ N$	$(1,2)\circ N$
$(1,2)\circ N$	$(1,2)\circ N$	$(1)\circ N$

(3) Let $N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. For example by Example 1.6.8 N is a subgroup of $\mathrm{Sym}(4)$. We will show that N is a normal subgroup. For this we first learn how to compute fgf^{-1} for $f, g \in \mathrm{Sym}(I)$. Let $(a_1, a_2, a_3, \ldots, a_n)$ be cycle of g. Then

$$\begin{aligned}
(fgf^{-1})(f(a_1)) &= f(g(a_1)) = f(a_2) \\
(fgf^{-1})(f(a_2)) &= f(g(a_2)) = f(a_3) \\
&\vdots \\
(fgf^{-1})(f(a_{n-1})) &= f(g(a_{n-1})) = f(a_n) \\
(fgf^{-1})(f(a_n)) &= f(g(a_n)) = f(a_1) \qquad .
\end{aligned}$$

Thus

$$\big(f(a_1), f(a_2), f(a_3), \ldots, f(a_n)\big)$$

is a cycle of fgf^{-1}. This allows as to compute fgf^{-1}. Suppose

$$g = (a_1, a_2, \ldots a_n)(b_1, b_2, b_3, \ldots b_m) \ldots$$

Then

$$fgf^{-1} = \big(f(a_1), f(a_2), \ldots f(a_n)\big)\big(f(b_1), f(b_2), f(b_3), \ldots f(b_m)\big) \ldots$$

For example, if $g = (1,3)(2,4)$ and $f = (1,4,3,2)$. Then

$$fgf^{-1} = \big(f(1), f(3)\big)\big(f(2), f(4)\big) = (4,2)(1,3),$$

and

$$(1,3,4) \circ (2,4,3) \circ (1,3,4)^{-1} = (2,1,4).$$

In particular we see that if g has cycles of length $\lambda_1, \lambda_2, \ldots, \lambda_k$ then also fgf^{-1} has cycles of length $\lambda_1, \lambda_2, \ldots, \lambda_k$.

We are now able to show that $N \trianglelefteq \mathrm{Sym}(4)$. For this let $g \in N$ and $f \in \mathrm{Sym}(4)$. By 1.8.6(d) we need to show that $fgf^{-1} \in N$. If $g = (1)$, then also $fgf^{-1} = (1) \in N$. Otherwise g has two cycles of length two and so also fgf^{-1} has two cycles of length 2. But any element with two cycles of length 2 is contained in N. So $fgf^{-1} \in N$ and $N \trianglelefteq \mathrm{Sym}(4)$. Since $|N| = 4$ and $|\mathrm{Sym}(4)| = 24$, $\mathrm{Sym}(4)/N$ is a group of order 6.

1.9 The Isomorphism Theorems

Definition 1.9.1. *Let $\phi : G \to H$ be a homomorphism of groups. Then*

$$\ker\phi := \{g \in G \mid \phi(g) = e_H\}.$$

$\ker\phi$ *is called the* kernel *of ϕ.*

Lemma 1.9.2. *Let $\phi : G \to H$ be a homomorphism of groups. Then $\ker\phi$ is a normal subgroup of G.*

Proof. We will verify the four conditions (i)-(iv) in the Normal Subgroup Proposition 1.8.7 Let $a, b \in \ker\phi$. Then

$$\phi(a) = e_H \text{ and } \phi(b) = e_H.$$

(i) $\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H$ and so $ab \in \ker\phi$.
(i) By 1.6.5(a), $\phi(e_G) = e_H$ and so $e_G \in \ker\phi$.
(iii) By 1.6.5(b), $\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H$ and so $a^{-1} \in \ker\phi$.
(iv) Let $d \in G$. Then

$$\phi(dad^{-1}) = \phi(d)\phi(a)\phi(d)^{-1} = \phi(d)e_H\phi(d)^{-1} = \phi(d)\phi(d)^{-1} = e_H$$

and so $dad^{-1} \in \ker\phi$.

By (i)-(iv) and 1.8.7 $\ker\phi$ is a normal subgroup of G. □

Lemma 1.9.3. *Let N be a normal subgroup of G and define*

$$\phi : G \to G/N, g \to gN.$$

Then ϕ is an onto group homomorphism with $\ker\phi = N$. ϕ is called the natural homomorphism *from G to G/N.*

Proof. Let $a, b \in G$. Then

$$\phi(ab) = abN \overset{1.8.8(a)}{=} (aN)(bN) = \phi(a)\phi(b),$$

and so ϕ is a homomorphism.

If $T \in G/N$, then $T = gN$ for some $g \in G$. Thus $\phi(g) = gN = T$ and ϕ is onto. Since $e_{G/N} = N$ the following statements are equivalent for $g \in G$

$$\begin{array}{rccr} & g \in \ker\phi & & \\ \iff & \phi(g) = e_{G/N} & - & \text{definition of } \ker\phi \\ \iff & gN = N & - & \text{definition of } \phi, 1.8.10 \\ \iff & g \in N & - & 1.7.7(a) \end{array}$$

So $\ker\phi = N$. □

Corollary 1.9.4. *Let N be a subset of the group G. Then N is a normal subgroup of G if and only if N is the kernel of a homomorphism.*

Proof. By 1.9.2 the kernel of a homomorphism is a normal subgroup; and by 1.9.3 any normal subgroup is the kernel of a homomorphism. □

Theorem 1.9.5 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism of groups. Then*

$$\overline{\phi} : G/\ker\phi \to \operatorname{Im}\phi, \quad g\ker\phi \to \phi(g)$$

is well-defined isomorphism of groups. In particular

$$G/\ker\phi \cong \operatorname{Im}\phi.$$

Proof. Put $N = \ker\phi$ and Let $a, b \in G$. Then

$$\begin{array}{rcll} & gN = hN & & \\ \Longleftrightarrow & g^{-1}h \in N & - & 1.7.6 \\ \Longleftrightarrow & \phi(g^{-1}h) = e_H & - & \text{Definition of } N = \ker\phi \\ \Longleftrightarrow & \phi(g)^{-1}\phi(h) = e_H & - & \phi \text{ is a homomorphism}, 1.6.5(b) \\ \Longleftrightarrow & \phi(h) = \phi(g) & - & \text{Multiplication with } \phi(g) \text{ from the left,} \\ & & & \quad \text{Cancellation law} \end{array}$$

So

$$(*) \qquad gN = hN \Longleftrightarrow \phi(g) = \phi(h).$$

Since $gN = hN$ implies $\phi(g) = \phi(h)$ we conclude that $\overline{\phi}$ is well-defined.
Let $S, T \in G/N$. Then there exists $g, h \in N$ with $S = gN$ and $T = hN$.
Suppose that $\overline{\phi}(T) = \overline{\phi}(S)$. Then

$$\phi(g) = \overline{\phi}(gN) = \overline{\phi}(S) = \overline{\phi}(T) = \overline{\phi}(hN) = \phi(h),$$

and so by (*) $gN = hN$. Thus $S = T$ and ϕ is 1-1.

Let $b \in \operatorname{Im}\phi$. Then there exists $a \in G$ with $b = \phi(a)$ and so $\overline{\phi}(aN) = \phi(a) = b$. Therefore $\overline{\phi}$ is onto.

Finally

$$\overline{\phi}(ST) = \overline{\phi}(gNhN) \overset{1.8.8(a)}{=} \overline{\phi}(ghN) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(gN)\overline{\phi}(hN) = \overline{\phi}(S)\overline{\phi}(T)$$

and so $\overline{\phi}$ is a homomorphism. We proved that $\overline{\phi}$ is a well-defined, 1-1 and onto homomorphism, that is a well-defined isomorphism. □

The First Isomorphism Theorem can be summarized in the following diagram:

$$\begin{tikzcd}
& & G \arrow[dddll, "\phi"'] \arrow[dddrr, "\pi"] & & \\
& & g \arrow[dl] \arrow[dr] & & \\
& \phi(g) & & g\ker\phi \arrow[ll, "\cong"'] & \\
\operatorname{Im}\phi & & & & G/\ker\phi \arrow[llll, "\overline{\phi}"']
\end{tikzcd}$$

Example 1.9.6.

Let G be a group and $g \in G$. Define

$$\phi : \mathbb{Z} \to G, m \to g^m.$$

By 1.6.4(1) ϕ is an homomorphism from $(\mathbb{Z}, +)$ to G. We have

$$\operatorname{Im}\phi = \{\phi(m) \mid m \in \mathbb{Z}\} = \{g^m \mid m \in \mathbb{Z}\} \overset{1.5.7(2)}{=} \langle g \rangle, \tag{1}$$

and

$$\ker\phi = \{m \in \mathbb{Z} \mid \phi(m) = e\} = \{m \in \mathbb{Z} \mid g^m = e\}. \tag{2}$$

If g has finite order, put $n = |g|$. Otherwise put $n = 0$. We claim that

$$\ker\phi = n\mathbb{Z}. \tag{3}$$

Suppose first that $n = 0$. Then $|g| = \infty$ and $g^m \neq e$ for all $m \in \mathbb{Z}^+$. Hence also $g^{-m} = (g^m)^{-1} \neq e$ and so $\ker\phi = \{0\} = 0\mathbb{Z} = n\mathbb{Z}$. So (3) holds in this case.

Suppose next that n is positive integer and let $m \in \mathbb{Z}$. By the Division Algorithm [Hung, Theorem 1.1], $m = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < m$. Thus

$$g^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

By definition of n, $g^s \neq e$ for all $0 < s < n$ and so $g^r = e$ if and only if $r = 0$. So $g^m = e$ if and only if $n \mid m$ and if and only if $m \in n\mathbb{Z}$. Hence (3) holds also in this case.

By the First Isomorphism Theorem

$$\mathbb{Z}/\ker\phi \cong \operatorname{Im}\phi$$

and so by (1) and (3).

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong \langle g \rangle.$$

In particular, if $G = \langle g \rangle$ is cyclic then $G \cong \mathbb{Z}_n$. So every cyclic group is isomorphic to $(\mathbb{Z}, +)$ (in the $n = 0$ case) or $(\mathbb{Z}_n, +), n > 0$.

Definition 1.9.7. *Let $*$ be a binary operation on the set A and $\Box$ a binary operation on the set B. Then $*\times\Box$ is the binary operation on $A\times B$ defined by*

$$*\times\Box : (A\times B)\times(A\times B)\to A\times B, \quad ((a,b),(c,d))\to(a*c, b\,\Box\, d)$$

$(A\times B,\ *\times\Box)$ is called the direct product *of $(A,*)$ and $(B,\Box)$.*

Lemma 1.9.8. *Let $(A,*)$ and $(B,\Box)$ be groups. Then*

(a) $(A\times B,\ *\times\Box)$ is a group.

(b) $e_{A\times B}=(e_A,e_B)$.

(c) $(a,b)^{-1}=(a^{-1},b^{-1})$.

(d) If A and B are abelian, so is $A\times B$.

Proof. Let $x,y,z\in A\times B$. Then $x=(a,b)$, $y=(c,d)$ and $z=(f,g)$ for some $a,c,f\in A$ and b,d,g in B. To improve readability we write $\triangle$ for $*\times\Box$. We compute

$$\begin{array}{rcccc} x\triangle(y\triangle z) & = & (a,b)\triangle\big((c,d)\triangle(f,g)\big) & = & (a,b)\triangle\big((c*f,d\,\Box\, g)\big) \\ = \ (a*(c*f),b\,\Box\,(d\,\Box\, g)) & = & ((a*c)*f,(b\,\Box\, d)\,\Box\, g) & = & (a*c,b\,\Box\, g)\triangle(f,g) \\ = \ \big((a,b)\triangle(c,d)\big)\triangle(f,g) & = & (x\triangle y)\triangle z. & & \end{array}$$

So $\triangle$ is associative.

$$x\triangle(e_A,e_B)=(a,b)\triangle(e_A,e_B)=(a*e_A,b\,\Box\, e_B)=(a,b)=x,$$

and similarly $(e_A,e_B)\triangle x=x$. So (e_A,e_B) is an identity for $\triangle$ in $A\times B$.

$$x\triangle(a^{-1},b^{-1})=(a,b)\triangle(a^{-1},b^{-1})=(a*a^{-1},b\,\Box\, b^{-1})=(e_A,e_B),$$

and similarly $(a^{-1},b^{-1})\,\Box\, x=(e_A,e_B)$. So (a^{-1},b^{-1}) is an inverse of x.

Hence $(G,\triangle)$ is a group and (a), (b) and (c) hold.

(d) Suppose $*$ and $\Box$ are commutative. Then

$$x\triangle y=(a,b)\triangle(c,d)=(a*c,b\,\Box\, d)=(c*a,d\,\Box\, c)=(c,d)\triangle(a,b)=y\triangle x.$$

Hence $\triangle$ is commutative and $A\times B$ is a group. $\Box$

Example 1.9.9.

Let A and B be groups and define

$$\pi : A\times B\to B,(a,b)\to b.$$

Then

$$\pi\big((a,b)(c,d)\big) = \pi(ac,bd) = bd = \pi(a,b)\pi(c,d)$$

and so π is an homomorphism. Let $b \in B$. Then $\pi(e_A, b) = b$ and so π is onto. Let $(a,b) \in A \times B$. Then $\pi(a,b) = e_B$ if and only $b = e_B$ and so $\ker \pi = A \times \{e_B\}$. In particular, $A \times \{e_B\}$ is a normal subgroup of $A \times B$ and by the First Isomorphism Theorem 1.9.5

$$A \times B/A \times \{e_B\} \cong B.$$

Lemma 1.9.10. *Let G be a group, H a subgroup of G and $T \subseteq H$.*

(a) T is a subgroup of G if and only if T is a subgroup of H.

(b) If $T \trianglelefteq G$, then $T \trianglelefteq H$.

(c) If $\alpha : G \to F$ is a homomorphism of groups, then $\alpha_H : H \to F, h \to \alpha(h)$ is also a homomorphism of groups. Moreover, $\ker \alpha_H = H \cap \ker \alpha$ *and if α is 1-1 so is α_H.*

Proof. (a) This follows easily from the Subgroup Proposition 1.5.3.

(b) Thus follows easily from the Normal Subgroup Proposition 1.8.7.

(c) Let $a, b \in H$. Then $\alpha_H(ab) = \alpha(ab) = \alpha(a)\alpha(b) = \alpha_H(a)\alpha_H(b)$ and so α_H is a homomorphism. Let $g \in G$ then

$$\begin{aligned} & g \in \ker \alpha_H \\ \iff\ & g \in H \text{ and } \alpha_H(h) = e_F \\ \iff\ & g \in H \text{ and } \alpha(h) = e_F \\ \iff\ & g \in H \text{ and } g \in \ker \alpha \\ \iff\ & g \in H \cap \ker \alpha \end{aligned}$$

So $\ker \alpha_H = H \cap \ker \alpha$.

Suppose α is 1-1. If $\alpha_H(a) = \alpha_H(b)$, then $\alpha(a) = \alpha(b)$ and so $a = b$. Thus α is 1-1. □

Theorem 1.9.11 (Second Isomorphism Theorem)**.** *Let G be a group, N a normal subgroup of G and A a subgroup of G. Then $A \cap N$ is a normal subgroups of A, AN is a subgroup of G, N is a normal subgroup of AN and the map*

$$A/A \cap N \to AN/N, \quad a(A \cap N) \to aN$$

is a well-defined isomorphism. In particular,

$$A/A \cap N \cong AN/N.$$

Proof. Let $a \in A$, then $aN = Na \subseteq NA$ and so $AN \subseteq NA$. So by Homework 4#4 AN is a subgroup of G. Since $N \trianglelefteq G$ 1.9.10(b) implies that $N \trianglelefteq AN$. By 1.9.3 $\pi : G \to G/N, g \to gN$ is a homomorphism with $\ker \pi = N$. Hence by 1.9.10(c) also the restriction $\pi_A : A \to G/N, a \to aN$ of π to A is a homomorphism with

$$\ker \pi_A = A \cap \ker \pi = A \cap N \tag{1}$$

Hence by 1.9.2 $A \cap N$ is a normal subgroup of G. We have

$$\begin{aligned} \operatorname{Im} \pi_A &= \{\pi_A(a) \mid a \in A\} = \{aN \mid a \in H\} \\ &= \{anN \mid a \in A, n \in N\} = \{dN \mid d \in AN\} = AN/N \end{aligned} \tag{2}$$

By the First Isomorphism Theorem 1.9.5 we now conclude that

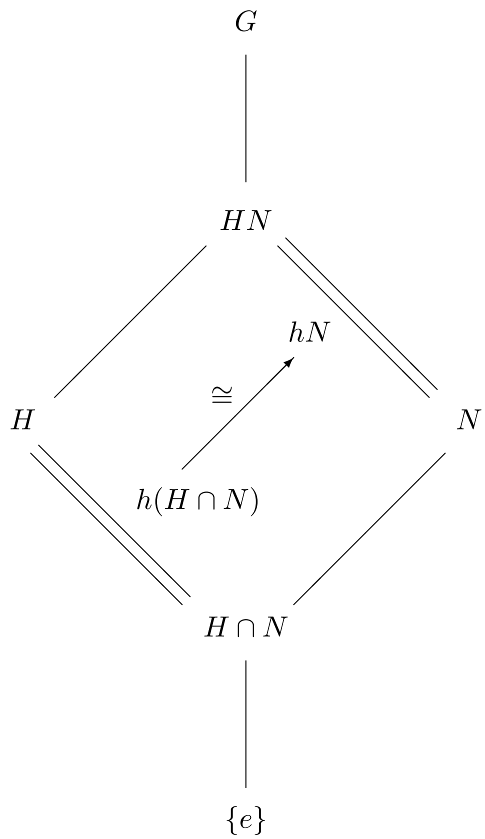
$$\overline{\pi_A} : \quad A/\ker \pi_A \to \operatorname{Im} \pi_A, \quad a \ker \pi_A \to \pi_A(a)$$

is a well-defined isomorphism. Thus by (1) and (2)

$$\overline{\pi_A} : \quad A/A \cap N \to AN/N, \quad a(A \cap N) \to aN$$

is a well-defined isomorphism. □

The Second Isomorphism Theorem can be summarized in the following diagram.



Example 1.9.12.

Let $H = \mathrm{Sym}(3)$ and view H has a subgroup of $G = \mathrm{Sym}(4)$. So $H = \{f \in \mathrm{Sym}(4) \mid f(4) = 4\}$. Put

$$N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

By 1.8.11(3) N is a normal subgroup of G and G/N is a group of order six. Observe that the only element in N which fixes 4 is (1). Thus $H \cap N = 1$. So the Second Isomorphism Theorem 1.9.11 implies that

$$H \cong H/\{(1)\} = H/H \cap N \cong HN/N.$$

In particular $|HN/N| = |H| = 6$. Since HN/N is a subset of G/N and $|G/N| = 6$ we conclude that $G/N = HN/N$. Thus $H \cong G/N$ and so

$$\mathrm{Sym}(3) \cong \mathrm{Sym}(4)/\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Lemma 1.9.13. *Let $\phi : G \to H$ be a homomorphism of groups.*

(a) If $A \leq G$ then $\phi(A)$ is a subgroup of H, where $\phi(A) = \{\phi(a) \mid a \in A\}$.

(b) If $A \trianglelefteq G$ and ϕ is onto, $\phi(A) \trianglelefteq H$.

(c) If $B \leq H$, then $\phi^{-1}(B)$ is a subgroup of G, where $\phi^{-1}(B) := \{a \in A \mid \phi(a) \in A\}$

(d) If $B \trianglelefteq H$, then $\phi^{-1}(B) \trianglelefteq G$.

Proof. (a) $\phi(A) = \{\phi(a) \mid a \in A\} = \{\phi_A(a) \mid a \in A\} = \operatorname{Im} \phi_A$. By 1.9.10(c) ϕ_A is a homomorphism and so by 1.6.5(c), $\operatorname{Im} \phi \leq H$. Hence $\phi(A) \leq H$.

(b) By (a) $\phi(A) \leq H$. Hence by 1.8.6(d) it suffices to show that $\phi(A)$ is invariant under conjugation. Let $b \in \phi(A)$ and $h \in H$. Then $b = \phi(a)$ for some $a \in A$ and since ϕ is onto, $h = \phi(g)$ for some $g \in G$. Thus

$$hbh^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi(aga^{-1}). \tag{1}$$

Since $A \trianglelefteq G$, 1.8.6(d) implies $aga^{-1} \in A$. So by (1), $hbh^{-1} \in \phi(A)$. Thus $\phi(A)$ is invariant under conjugation and $\phi(A) \trianglelefteq G$.

(c) We will use the Subgroup Proposition. Let $x, y \in \phi^{-1}(B)$. Then

$$\phi(x) \in B \text{ and } \phi(y) \in B. \tag{2}$$

Since $\phi(xy) = \phi(x)\phi(y)$ and B is closed under multiplication we conclude from (2) that $\phi(xy) \in B$. Hence $xy \in \phi^{-1}(B)$ and $\phi^{-1}(B)$ is closed under multiplication.

By 1.6.5(a) $\phi(e_G) = e_H$ and by the Subgroup Proposition, $e_H \in H$. Thus $\phi(e_G) \in H$ and $e_G \in \phi^{-1}(B)$.

By 1.6.5(b) $\phi(x^{-1}) = \phi(x)^{-1}$. Since B is closed under inverses, (2) implies $\phi(x)^{-1} \in B$. Thus $\phi(x^{-1}) \in B$ and $x^{-1} \in \phi^{-1}(B)$. Hence $\phi^{-1}(B)$ is closed under inverses.

We verified the three conditions of the Subgroup Proposition and so $\phi^{-1}(B) \leq G$.

(d) By (c), $\phi^{-1}(B) \leq G$. Let $x \in \phi^{-1}(B)$ and $g \in G$. Then

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1}. \tag{3}$$

Since $\phi(x) \in B$ and B is invariant under conjugation we have $\phi(g)\phi(x)\phi(g)^{-1} \in B$. Hence by (3) $gxg^{-1} \in \phi^{-1}(B)$ and by 1.8.6(d), $\phi^{-1}(B) \trianglelefteq G$. □

Theorem 1.9.14 (Correspondence Theorem)**.** *Let N be a normal subgroup of the group G. Put*

$$S(G,N) = \{H \mid N \leq H \leq G\} \text{ and } S(G/N) = \{F \mid F \leq G/N\}.$$

Let

$$\pi : G \to G/N, \quad g \to gN$$

be the natural homomorphism.

(a) Let $N \leq K \leq G$. Then $\pi(K) = K/N$.

(b) Let $F \leq G/N$. Then $\pi^{-1}(F) = \bigcup_{T \in F} T$.

(c) Let $N \leq K \leq G$ and $g \in G$. Then $g \in K$ if and only if $gN \in K/N$.

(d) The map

$$\beta : \quad \mathcal{S}(G, N) \to \mathcal{S}(G/N), \quad K \to K/N$$

is a well-defined bijection with inverse

$$\alpha : \quad \mathcal{S}(G/N) \to \mathcal{S}(G, N), \quad F \to \pi^{-1}(F).$$

In other words:

(a) If $N \leq K \leq G$, then K/N is a subgroup of G/N.

(b) For each subgroup F of G/N there exists a unique subgroup K of G with $N \leq K$ and $F = K/N$. Moreover, $K = \pi^{-1}(F)$.

(e) Let $N \leq K \leq G$. Then $K \trianglelefteq G$ if and only if $K/N \trianglelefteq G/N$.

(f) Let $N \leq H \leq G$ and $N \leq K \leq G$. Then $H \subseteq K$ if and only if $H/N \subseteq K/N$.

(g) **(Third Isomorphism Theorem)** *Let $N \leq H \trianglelefteq G$. Then the map*

$$\rho : \quad G/H \to (G/N)\big/(H/N), \quad gH \to (gN) * (H/N)$$

is a well-defined isomorphism.

Proof. (a) $\pi(K) = \{\pi(k) \mid k \in K\} = \{kN \mid k \in N\} = K/N$.

(b) Let $g \in G$. Then

$$\begin{array}{rcll}
 & g \in \pi^{-1}(F) & & \\
\iff & \pi(g) \in F & - & \text{definition of } \pi^{-1}(F) \\
\iff & gN \in F & - & \text{definition of } \pi \\
\iff & gN = T \text{ for some } T \in F & & \\
\iff & g \in T \text{ for some } T \in F & - & T \in G/N, 1.7.7\text{(a)} \\
\iff & g \in \bigcup_{T \in F} T & - & \text{definition of union}
\end{array}$$

(c) If $g \in K$ then clearly $gN \in K/N$. If $gN \in K/N$ then $gN = kN$ for some $k \in K$ and so $g \in gN = kN \subseteq K$. So $g \in K$ if and only if $gN \in K/N$.

(d) Let $N \leq H \leq G$ and $F \leq G/N$. By (a) $H/N = \pi(H)$ and so by 1.9.13(a) H/N is a subgroup of N. Hence β is well-defined. By 1.9.13(a) $\pi^{-1}(F) \leq G$. Also if

$n \in N$, then $\pi(n) = nN = N = e_{G/N} \in F$ and so $n \in \pi^{-1}(N)$. Thus $N \leq \pi^{-1}(N)$ and $\pi^{-1}(N) \in \mathcal{S}(G, N)$. This shows that α is well defined. We compute

$$\begin{aligned}\alpha(\beta(H)) &= \pi^{-1}(H/N) = \{g \in G \mid \pi(g) \in H/N\} \\ &= \{g \in G \mid gN \in H/N\} \overset{\text{(e)}}{=} \{g \in G \mid g \in H\} = H\end{aligned}$$

Since π onto, A.2.5 implies $\pi(\pi^{-1}(F)) = F$ and so $\beta(\alpha(F)) = F$. Hence α is an inverse of β and by A.2.6(c), β is a bijection.

(e) Suppose that $K \trianglelefteq N$. Then since π is onto, 1.9.13(b) implies $K/N = \pi(K) \trianglelefteq N$. Suppose that $K/N \trianglelefteq G/N$. By (f) $\pi^{-1}(K/N) = K$ and so by 1.9.13(d) $K \trianglelefteq N$.

(f) Let $h \in H$. By (c) $h \in K$ if and only if $hN \in K/N$ and so $H \subseteq K$ if and only if $H/N \subseteq K/N$.

(g) Let

$$\eta : \quad G/N \to G/N\big/H/N, \quad T \to T * (H/N)$$

be the natural homomorphism. Consider the composition:

$$\eta \circ \pi : \quad G \to G/N\Big/H/N, \quad g \to (gN) * (H/N).$$

Since η and π are homomorphism, also $\eta \circ \pi$ is homomorphism (see Homework 3#7). Since both η and π are onto, $\eta \circ \pi$ is onto (see A.2.3 b). So

$$\operatorname{Im} \eta \circ \pi = G/N\Big/H/N. \tag{1}$$

We now compute $\ker(\eta \circ \pi)$:

$$\begin{array}{rccl} & g \in \ker(\eta \circ \pi) & & \\ \iff & (\eta \circ \pi)(g) = e_{(G/N)/(H/N)} & - & \text{Definition of } \ker(\eta \circ \pi) \\ \iff & \eta(\pi(g)) = e_{(G/N)/(H/N)} & - & \text{Definition of } \circ \\ \iff & \pi(g) \in \ker \eta & - & \text{Definition of } \ker \eta \\ \iff & \pi(g) \in H/N & - & 1.9.3 \\ \iff & gN \in H/N & - & \text{Definition of } \pi \\ \iff & g \in H & - & (c) \end{array}$$

Thus

$$\ker(\eta \circ \pi) = H. \tag{2}$$

By the First Isomorphism Theorem 1.9.5

$$\rho : \quad G/\ker(\eta\circ\pi) \to \mathrm{Im}(\eta\circ\pi), \quad g\ker(\eta\circ\pi) \to (\eta\circ\pi)(g)$$

is a well defined isomorphism. Thus by (1) and (2)

$$\rho : G/H \to (G/N)\Big/(H/N), \quad gH \to (gN) * (H/N).$$

is a well-defined isomorphism.

□

Example 1.9.15.

In this example we compute the subgroups of $(\mathbb{Z}, +)$ and then use 1.9.14 to compute the subgroups of $\mathbb{Z}_n$.

Let H be an additive subgroup of $\mathbb{Z}$. We claim that

$$H = m\mathbb{Z} \text{ for some m } \in \mathbb{N}. \tag{1}$$

Observe that $0 \in H$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. So suppose that $H \neq \{0\}$. Then there exists $0 \neq i \in H$. Since H is closed under inverse, $-i \in H$ and so H contains a positive integer. Let m be the smallest positive integer contained in H. Then $m\mathbb{Z} = \langle m\rangle \leq H$. Let $h \in H$. Then $h = qm + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Then $r = h - qn \in H$. Since m is the smallest positive integer contained in H, r is not positive. Thus $r = 0$ and $h = qm \in m\mathbb{Z}$. So $H = m\mathbb{Z}$. Thus (1) is proved.

Let n be a positive integer. We will now use 1.9.14 to determine the subgroups of $\mathbb{Z}/n\mathbb{Z}$. Let F be a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Then by 1.9.14(d), $F = H/n\mathbb{Z}$ for some subgroup H of $\mathbb{Z}$ with $n\mathbb{Z} \leq H$. From (1), $H = m\mathbb{Z}$ for some $m \in \mathbb{N}$. Since $n \in n\mathbb{Z} \leq H = m\mathbb{Z}$ we get $m \neq 0$ and $m \mid n$. Thus

$$F = m\mathbb{Z}/nZ \text{ for some } m \in \mathbb{Z}^+ \text{ with } m \mid n. \tag{2}$$

For example the subgroups of $\mathbb{Z}/12\mathbb{Z}$ are

$$1\mathbb{Z}/12\mathbb{Z}, \quad 2\mathbb{Z}/12\mathbb{Z}, \quad 3\mathbb{Z}/12\mathbb{Z}, \quad 4\mathbb{Z}/12\mathbb{Z}, \quad 6\mathbb{Z}/12\mathbb{Z}, \quad 12\mathbb{Z}/12\mathbb{Z}. \tag{3}$$

By the Third Isomorphism Theorem

$$\mathbb{Z}/n\mathbb{Z}\Big/m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m, \tag{4}$$

and so $\left|\mathbb{Z}/n\mathbb{Z}\big/m\mathbb{Z}/n\mathbb{Z}\right| = \left|\mathbb{Z}/m\mathbb{Z}\right| = m$. Also $|\mathbb{Z}/n\mathbb{Z}| = n$. By Lagrange Theorem applied to the subgroup $m\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$,

$$\left|\mathbb{Z}/n\mathbb{Z}\right| = \left|\mathbb{Z}/n\mathbb{Z}\middle/ m\mathbb{Z}/n\mathbb{Z}\right| \cdot \left|m\mathbb{Z}/n\mathbb{Z}\right|$$

and so

$$n = m \cdot |m\mathbb{Z}/n\mathbb{Z}|.$$

Thus

$$|m\mathbb{Z}/n\mathbb{Z}| = \frac{n}{m}.$$

Observe that $m\mathbb{Z}/n\mathbb{Z}$ is generated by $m + n\mathbb{Z}$. So $m\mathbb{Z}/n\mathbb{Z}$ is cyclic and so by 1.9.6

(5) $$m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{\frac{n}{m}}.$$

So the groups in (3) are isomorphic to

(6) $$\mathbb{Z}_{12}, \quad \mathbb{Z}_6, \quad \mathbb{Z}_4, \quad \mathbb{Z}_3, \quad \mathbb{Z}_2, \quad \mathbb{Z}_1,$$

and by (4) their quotient groups are isomorphic to

(7) $$\mathbb{Z}_1, \quad \mathbb{Z}_2, \quad \mathbb{Z}_3, \quad \mathbb{Z}_4, \quad \mathbb{Z}_6, \quad \mathbb{Z}_{12}.$$

Example 1.9.16.

In this example we compute the subgroups of Sym(3) and then use 1.9.14 to compute some subgroups of Sym(4).

Let $K \leq \mathrm{Sym}(3)$. Then by Lagrange theorem $|K|\big|\,|\mathrm{Sym}(3)| = 6$ and so $|K| = 1, 2, 3$ or 6. If $|K| = 1$ them $K = \{(1)\}$.

If $|K| = 2$, then by 1.7.15 K is cyclic and so by 1.7.14(a), $K = \langle g \rangle$ for some $g \in K$. The elements of order 2 in Sym(3) are $(1,2), (1,3)$ and $(2,3)$. So K is one $\langle (1,2) \rangle$, $\langle (1,3) \rangle$ and $\langle (2,3) \rangle$.

Similarly if $|K| = 3$ we see $K = \langle g \rangle$ for some $g \in K$ with $|g| = 3$. The elements of order three in Sym(3) are $(1,2,3)$ and $(1,3,2)$. Also $\langle (1,2,3) \rangle = \{1, (1,2,3), (1,3,2)\} = \langle (1,3,2) \rangle$ and so $K = \langle (1,2,3) \rangle$.

If $|K| = 6$ then $K = \mathrm{Sym}(3)$. So the subgroups of Sym(3) are

(1) $$\{1\}, \quad \langle (1,2) \rangle, \quad \langle (1,3) \rangle, \quad \langle (2,3) \rangle, \quad \langle (1,2,3) \rangle, \quad \mathrm{Sym}(3).$$

Let $N = \langle (1,2)(3,4), (1,3)(2,4) \rangle$ and $H = \{f \in \mathrm{Sym}(4) \mid f(4) = 4\} \cong \mathrm{Sym}(3)$. By Example 1.9.12 $N \trianglelefteq \mathrm{Sym}(3)$ and the map $\phi : H \to \mathrm{Sym}(4)/N, h \to hN$ is an isomorphism. We can obtain the subgroups of G/N by computing $\phi(K)$ for each subgroups K of H:

$$\begin{aligned}
\phi(\{1\}) &= \{(1)N\} \\
&= \Big\{\{(1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}\Big\} \\
\phi(\langle(1,2)\rangle) &= \{(1)N,(1,2)N\} \\
&= \Big\{\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}, \\
&\qquad \{(1,2),(3,4),(1,3,2,4),(1,4,2,3)\}\Big\} \\
\phi(\langle(1,3)\rangle) &= \{(1)N,(1,3)N\} \\
&= \Big\{\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}, \\
&\qquad \{(1,3),(1,2,3,4),(2,4),(1,4,3,2)\}\Big\} \\
\phi(\langle(2,3)\rangle) &= \{(1)N,(2,3)N\} \\
&= \Big\{\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}, \\
&\qquad \{(2,3),(1,3,4,2),(1,2,4,3)),(1,4))\}\Big\} \\
\phi(\langle(1,2,3)\rangle) &= \{(1)N,(1,2,3),(1,3,2)N\} \\
&= \Big\{\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}, \\
&\qquad \{(1,2,3),(1,3,4),(2,4,3),(1,4,2)\}, \\
&\qquad\qquad \{(1,3,2),(2,3,4),(1,2,4),(1,4,3)\}\Big\} \\
\phi(H) &= \mathrm{Sym}(4)/N
\end{aligned}$$

By 1.9.14 taking the unions over the sets of cosets in (7) gives us the subgroups of Sym(4) containing N:

(3)

$$\begin{aligned}
N = {}& \{(1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \\
X_1 = {}& \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,2),(3,4),(1,3,2,4),(1,4,2,3)\} \\
D_4 = {}& \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,3),(1,2,3,4),(2,4),(1,4,3,2)\} \\
X_2 = {}& \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(2,3),(1,3,4,2),(1,2,4,3)),(1,4)) \\
\mathrm{Alt}(4) := {}& \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,2,3),(1,3,4), \\
& (2,4,3),(1,4,2)(1,3,2),(2,3,4),(1,2,4),(1,4,3)\} \\
& \mathrm{Sym}(4)
\end{aligned}$$

By Example 1.8.3, $\langle(1,2)\rangle$ is not normal in Sym(3), while $\langle(1,2,3)\rangle$ is normal. Similarly neither $\langle(1,3)\rangle$ nor $\langle(2,3)\rangle$ is normal in Sym(3). Thus the normal subgroups of Sym(3) are

$$\{(1)\}, \quad \mathrm{Alt}(3) := \langle (1,2,3) \rangle, \quad \mathrm{Sym}(3). \tag{10}$$

So by 1.9.14 the normal subgroups of Sym(4) containing N are

$$N, \quad \mathrm{Alt}(4), \quad \mathrm{Sym}(4). \tag{11}$$

Chapter 2

Group Actions and Sylow's Theorem

2.1 Group Action

Definition 2.1.1. *Let G be group and I a set. An* action *of G on I is a function*

$$\diamond : \quad G \times I \to I \quad (g, i) \to (g \diamond i)$$

such that

(act:i) $e \diamond i = i$ *for all* $i \in I$.

(act:ii) $g \diamond (h \diamond i) = (g * h) \diamond i$ *for all* $g, h \in G$, $i \in I$.

*The pair $(I, \diamond)$ is called a G-*set. *We also say that G acts on I via $\diamond$. Abusing notations we often just say that I is a G-set. Also we often just write gi for $g \diamond i$.*

Example 2.1.2.

(1) Let $(G, *)$ be a group. We claim that $*$ is an action of G on G. Indeed since e is an identity for $*$, we have $e * g = g$ for all $g \in G$ and so (act:i) holds. Since $*$ is associative, $a * (b * g) = (a * b) * g$ for all $a, b, g \in G$. So also (act ii) holds. This action is called the action of G on G by left-multiplication.

(2) $\mathrm{Sym}(I)$ acts on I via $f \diamond i = f(i)$ for all $f \in \mathrm{Sym}(I)$ and $i \in I$. Indeed, $\mathrm{id}_I \diamond i = \mathrm{id}_I(i) = i$ and so (act:i) holds. Moreover, $f \diamond (g \diamond i) = f(g(i)) = (f \circ g)(i)$.

(3) Let $\mathbb{F}$ be a field. Recall that $GL_2(\mathbb{F})$ is the group of invertible 2×2 matrices with coefficients in $\mathbb{F}$. Define

$$\begin{aligned}\diamond: \qquad & GL_2(\mathbb{F}) \times \mathbb{F}^2 \to \mathbb{F}^2\\ & (A, v) \to Av\\ & \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \to \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}\end{aligned}$$

We claim that $\diamond$ is an action of $GL_2(\mathbb{F})$ on $\mathbb{F}^2$. Recall that the identity element in $GL_2(\mathbb{F})$ is the identity matrix $\begin{pmatrix} 1_\mathbb{F} & 0_\mathbb{F} \\ 0_\mathbb{F} & 1_\mathbb{F} \end{pmatrix}$. Since

$$\begin{pmatrix} 1_\mathbb{F} & 0_\mathbb{F} \\ 0_\mathbb{F} & 1_\mathbb{F} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1_\mathbb{F}x + 0_\mathbb{F}y \\ 0_\mathbb{F}x + 1_\mathbb{F}y \end{pmatrix} = \begin{pmatrix} x + 0_\mathbb{F} \\ 0_\mathbb{F} + y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix},$$

we conclude that (act:i) holds. Since matrix multiplication is associative, $A(Bv) = (AB)v$ for all $A, B \in GL_2(\mathbb{F})$ and $v \in \mathbb{F}^2$. Hence (act:ii) holds.

The next lemma shows that an action of G on I is basically the same as an homomorphism from G to $\mathrm{Sym}(I)$.

Lemma 2.1.3. *Let G be a group and I a set.*

(a) Suppose $\diamond$ is an action of G on I. For $a \in G$ define

$$f_a: \quad I \to I, \quad i \to a \diamond i.$$

Then $f_a \in \mathrm{Sym}(I)$ and the map

$$\Phi_\diamond: \quad G \to \mathrm{Sym}(I), \quad a \to f_a$$

is a homomorphism. $\Phi_\diamond$ is called the homomorphism associated to the action of *G on I.*

(b) Let $\Phi : G \to \mathrm{Sym}(I)$ be homomorphisms of groups. Define

$$\diamond : G \times I \to I, (g, i) \to \Phi(g)(i).$$

Then $\diamond$ is an action of G on I.

Proof. (a) Observe first that $f_e(i) = ei = i$ for all $i \in I$ and so

$$f_e = \mathrm{id}_I \tag{1}$$

Let $a, b \in I$ then

$$f_{ab}(i) = (ab)i = a(bi) = f_a(f_b(i)) = (f_a \circ f_b)(i)$$

and so

$$f_{ab} = f_a \circ f_b. \tag{2}$$

From (2) applied to $b = a^{-1}$ we have

$$f_a \circ f_{a^{-1}} \overset{(2)}{=} f_{aa^{-1}} = f_e \overset{(1)}{=} \mathrm{id}_I.$$

and similarly $f_{a^{-1}} \circ f_a = \mathrm{id}_I$. So by A.2.6(c), f_a is a bijection. Thus $f_a \in \mathrm{Sym}(I)$. Now

$$\Phi_\diamond(ab) = f_{ab} \overset{(2)}{=} f_a \circ f_b = \Phi_\diamond(a) \circ \Phi_\diamond(b)$$

and so $\Phi_\diamond$ is a homomorphism.

(b) By 1.6.5(a), $\Phi(e) = e_{\mathrm{Sym}(I)} = \mathrm{id}_I$. Thus

$$e \diamond i = \Phi(e)(i) = \mathrm{id}_I(i) = i$$

for all $i \in I$. So (act:i) holds.

Let $a, b \in G$. Then

$$(ab) \diamond i = \Phi(ab)(i) \overset{\Phi\ \mathrm{hom}}{=} (\Phi(a) \circ \Phi(b)(i) = \Phi(a)(\Phi(b)(i)) = a \diamond (b \diamond i).$$

Thus (act:ii) holds and $\diamond$ is an action for G on I. □

Example 2.1.4.

(1) We will compute the homomorphism Φ associated the action of a group G on itself by left-multiplication (see Example 2.1.2(1)). For this let $a \in G$. Then for each $g \in G$, $f_a(g) = ag$ and $\Phi(a) = f_a$. So Φ is the homomorphism used in the proof of Cayley's Theorem 1.6.7.

(2) We will compute the homomorphism Φ associated to the action of a $\mathrm{Sym}(I)$ on I (see Example 2.1.2(2)). Let $a \in \mathrm{Sym}(i)$. Then for all $i \in I$,

$$f_a(i) = a \diamond i = a(i).$$

So $f_a = a$ and thus $\Phi(a) = a$. Hence $\Phi = \mathrm{id}_{\mathrm{Sym}(I)}$.

Lemma 2.1.5. *Let G be a group and H a subgroups of G. Define*

$$\diamond_{G/H}: \quad G \times G/H \to G/H, \quad (g, T) \to gT$$

Then $\diamond_{G/H}$ is well-defined action of G on G/H. This action is called the action of G on G/H by left multiplication.

Proof. Let $a \in G$ and $T \in G/H$. Then $T = tH$ for some $t \in G$. We have

$$aT = atH = (at)H \in G/H,$$

and so $\diamond_{G/H}$ is well defined. By 1.8.1(c) $eT = T$ and hence (act:i) holds.

Let $a, b \in G$. Then $(ab)T = a(bT)$ by 1.8.1(a) and so also (act:ii) holds. □

Example 2.1.6.

Let $G = \mathrm{Sym}(4)$ and $H = D_4$. We will investigate the action of G on G/D_4 by left multiplication. Put

$$a = D_4, \quad b = (1,2)D_4, \quad \text{and} \quad c = (1,4)D_4.$$

Since $(1,2) \notin D_4$, $a \neq b$. Since $(1,4) \notin D_4$, $a \neq c$ and since $(1,2)^{-1} \circ (1,4) = (1,2) \circ (1,4) = (1,4,2) \notin D_4$, $b \neq c$. By Lagrange's Theorem $|G/H| = \frac{|G|}{|H|} = \frac{24}{3} = 3$. Hence

$$G/H = \{a, b, c\}.$$

We now compute how $(1,2), (1,3)$ and $(1,4)$ act on G/H. We start with $(1,2)$:

$$(1,2)a = (1,2)D_4 = b, \tag{1.1}$$

$$(1,2)b = (1,2)(1,2)D_4 = D_4 = b, \tag{1.2}$$

and

$$(1,2)c = (1,2)(1,4)D_4 = (1,4,2)D_4.$$

Is $(1,4,2)D_4$ equal to a, b or c? Since the map $f_{(1,2)} : G/H \to G/H, T \to (1,2)T$ is a bijection we must have

$$(1,2)c = c. \tag{1.3}$$

So $(1,4,2)D_4 = (1,4)D_4$. Thus can also be verified directly: $(1,4,2)^{-1}(1,4) = (1,2,4)(1,4) = (2,4) \in D_4$ and so $(1,4)D_4 = (1,4,2)D_4$.

Let Φ be the homomorphism from G to $\mathrm{Sym}(G/H)$ associated to the action of G on $G/H = \{a, b, c\}$. From (1.1),(1.2) and (1.3):

$$\Phi((1,2)) = f_{(1,2)} = (a, b). \tag{1}$$

Next we consider $(1,3)$:

$$(1,3)a = (1,3)D_4 = D_4 = a. \tag{2.1}$$

From

$$(1,3)b = (1,3)(1,2)D_4 = (1,2,3)D_4,$$

and

$$(1,2,3)^{-1}(1,4) = (1,3,2)(1,4) = (1,4,3,2) \in D_4$$

we have

$$(1,3)b = c. \tag{2.2}$$

$$(1,3)c = (1,3)(1,3)b = (1)b = b. \tag{2.3}$$

From (2.1),(2.2) and (2,3)

$$\Phi((1,3)) = f_{(1,3)} = (b,c). \tag{2}$$

$$(1,4)a = (1,4)D_4 = c, \tag{3.1}$$

$$(1,4)c = (1,4)(1,4)D_4 = (1)D_4 = D_4 = a, \tag{3.2}$$

and so since $f_{(1,4)}$ is a bijection

$$(1,4)b = b. \tag{3.3}$$

From (3.1),(3.2) and (3.3):

$$\Phi((1,4)) = f_{(1,4)} = (a,c). \tag{3}$$

Since $(1,2)(1,3) = (1,3,2)$ and Φ is a homomorphism, we conclude that

$$\Phi((1,3,2)) = \Phi((1,2))\Phi((1,3)) = (a,b)(b,c) = (a,b,c), \tag{4}$$

and

$$\Phi((1,2,3)) = \Phi((1,3,2)^{-1}) = \Phi((1,3,2))^{-1} = (a,b,c)^{-1} = (a,c,b). \tag{5}$$

Clearly

$$(6) \qquad \Phi((1)) = (a).$$

From (1)-(6), Φ is onto and so $G/\ker\Phi \cong \mathrm{Sym}(3)$.

What is $\ker\phi$?

Recall that in example 1.8.11(3) we learned how to compute $f\circ g\circ f^{-1}$ for permutations f and g. We have

$$(1,3)^{-1}\circ(1,2)\circ(1,3) = (3,2) = (2,3).$$

Since Φ is a homomorphism this implies

$$\begin{array}{rclclcl} \Phi((2,3)) & = & \Phi\big((1,3)^{-1}\circ(1,2)\circ(1,3)\big) & = & \Phi((1,3))^{-1}\circ\Phi((1,2))\circ\Phi((1,3)) \\ & = & (b,c)^{-1}\circ(a,b)\circ(b,c)^{-1} & = & (a,c) & = & \Phi((1,4)) \end{array}$$

Thus

$$\Phi((1,4)(2,3)) = \Phi((1,4))\Phi((2,3)) = (a,c)(a,c) = (a)$$

and so $(1,4)(2,3)\in\ker\Phi$. Since $\ker\Phi$ is a normal subgroup of G, this implies that also $(1,2)^{-1}\circ(1,4)(2,3)\circ(1,2)\in\ker\Phi$ and $(1,3)^{-1}\circ(1,4)(2,3)\circ(1,3)\in\ker\Phi$.

So

$$N := \{(1),(1,4)(2,3),(2,4)(1,3),(3,4)(2,1)\}\subseteq\ker\Phi.$$

By Lagrange's $|\ker\Phi| = \frac{|G|}{|\mathrm{Sym}(3)|} = \frac{24}{6} = 4$ and so $\ker\Phi = N$. Thus $\mathrm{Sym}(4)/N\cong \mathrm{Sym}(3)$. Of course we already proved this once before in Example 1.9.12.

Lemma 2.1.7 (Cancellation Law for Action)**.** *Let G be a group acting on the set I, $a\in G$ and $i,j\in H$. Then*

(a) $a^{-1}(ai) = i$.

(b) $i = j \iff ai = aj$.

(c) $j = ai \iff i = a^{-1}j$.

Proof. (a) $a^{-1}(ai) \overset{\text{act ii}}{=} (a^{-1}a)i \overset{\text{Def } a^{-1}}{=} ei \overset{\text{act i}}{=} i$.

(b) Clearly if $i=j$, then $ai=aj$. Suppose $ai=aj$. Then then $a^{-1}(ai) = a^{-1}(aj)$ and so by (a), $i=j$.

(c)

$$\begin{array}{rccl} & j = ai & & \\ \iff & a^{-1}j = a^{-1}(ai) & - & (b) \\ \iff & a^{-1}j = i & - & (a) \end{array}$$

□

Definition 2.1.8. *Let G be a group and $(I, \diamond)$ a G-set.*

(a) The relation $\equiv_\diamond \pmod{G}$ on I is defined by $i \equiv_\diamond j \pmod{G}$ if there exists $g \in G$ with $gi = j$.

(b) $G \diamond i := \{g \diamond i \mid g \in G\}$. $G \diamond i$ is called the orbit *of G on I (with respect to $\diamond$) containing i. We often write Gi for $G \diamond i$.*

Example 2.1.9.

(1) Let G be a group and H a subgroup of G. Then H acts on G by left multiplication. Let $g \in G$. Then

$$H \diamond g = \{h \diamond g \mid h \in H\} = \{hg \mid h \in H\} = Hg$$

So the orbits of H on G with respect to left multiplication are the right cosets of H.

(2) Let I be a set and let $\diamond$ be the natural action of $\mathrm{Sym}(I)$ on I, see Example 2.1.2(2). Let $i \in I$

$$\mathrm{Sym}(I) \diamond i = \{f \diamond i \mid f \in \mathrm{Sym}(I)\} = \{f(i) \mid f \in \mathrm{Sym}(I)\}.$$

Let $j \in I$, then there exists $f \in \mathrm{Sym}(I)$ with $f(i) = j$, for example $f = (i, j)$. So $j \in \mathrm{Sym}(I) \diamond i$ and thus $\mathrm{Sym}(I) \diamond i = I$. Hence I is the only orbit of $\mathrm{Sym}(I)$ on I.

(3) Let $N = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. By Example 1.8.11(3), N is a normal subgroup of G. Hence by Homework 6#3

$$\diamond : \quad \mathrm{Sym}(4) \times N \to N, (g, n) \to gng^{-1}$$

is an action of $\mathrm{Sym}(4)$ on N. Let $n \in N$, then

$$\mathrm{Sym}(4) \diamond n = \{g \diamond n \mid g \in \mathrm{Sym}(4)\} = \{gng^{-1} \mid \mathrm{Sym}(4)\}.$$

Consider $n = e$. Then $geg^{-1} = e$ and so

$$\mathrm{Sym}(4) \diamond e = \{e\}.$$

Consider $n = (1,2)(3,4)$. Then $gng^{-1} \neq e$ and $gng^{-1} \in N$. We compute

$$\begin{aligned}
(1) \circ (1,2)(3,4) \circ (1)^{-1} &= (1,2)(3,4), \\
(1,3) \circ (1,2)(3,4) \circ (1,3)^{-1} &= (1,4)(2,3), \\
(1,4) \circ (1,2)(3,4) \circ (1,4)^{-1} &= (1,3)(2,4).
\end{aligned}$$

Thus

$$\mathrm{Sym}(4) \diamond (1,2)(3,4) = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Lemma 2.1.10. *Let G be a group acting in the set I. Then $'\equiv \pmod G'$ is an equivalence relation on I. The equivalence class of $'\equiv \pmod G'$ containing $i \in I$ is Gi.*

Proof. Let $i, j, k \in I$. From $ei = i$ we conclude that $i \equiv i \pmod G$ and $'\equiv \pmod G'$ is reflexive.

If $i \equiv j \pmod G$ then $j = gi$ for some $g \in G$ and so

$$g^{-1}j = g^{-1}(gi) = (g^{-i}g)i = ei = i.$$

Thus $j \equiv i \pmod G$ and $'\equiv \pmod G'$ is symmetric.

If $i \equiv j \pmod G$ and $j \equiv k \pmod G$, then $j = gi$ and $k = hj$ for some $g, h \in G$. Thus

$$(hg)i = h(gi) = hj = k,$$

and so $i \equiv k \pmod G$. Thus $'\equiv \pmod G'$ is transitive . It follows that $'\equiv \pmod G'$ is an equivalence relation.

Let $[i]$ be the equivalence class of $'\equiv \pmod G'$ containing i. Then

$$[i] = \{j \in J \mid i \equiv j \pmod G\} = \{j \in G \mid j = gi \text{ for some } g \in G\} = \{gi \mid g \in G\} = Gi$$

□

Proposition 2.1.11. *Let G be a group acting on the set I and $i, j \in G$. Then following are equivalent.*

(a) $j = gi$ *for some* $g \in G$.

(b) $i \equiv j \pmod G$

(c) $j \in Gi$.

(d) $Gi \cap Gj \neq \emptyset$

(e) $Gi = Gj$

(f) $i \in Gj$.

(g) $j \equiv i \pmod G$.

(h) $i = hj$ *for some* $h \in G$

In particular, I is the disjoint union of the orbits for G on I.

Proof. By definition of $i \equiv j \pmod G$, (a) and (b) are equivalent, and also (g) and (h) are equivalent. By 2.1.10, Gi is the equivalence class containing i. So by A.1.3 (b)-(h) are equivalent. □

Definition 2.1.12. *Let G be a group acting on the set I. We say that G acts* transitively *on I if for all $i, j \in G$ there exists $g \in G$ with $gi = j$.*

Corollary 2.1.13. *Let G be group acting on the non-empty set I. Then the following are equivalent*

(a) G *acts transitively on* I.

(b) $I = Gi$ *for all* $i \in I$.

(c) $I = Gi$ *for some* $i \in I$.

(d) I *is an orbit for* G *on* I.

(e) G *has exactly one orbit on* I.

(f) $Gi = Gj$ *for all* $i, j \in G$.

(g) $i \equiv j \pmod G$ *for all* $i, j \in G$.

Proof. (a) $\Longrightarrow$ (b): Let $i, j \in I$. Since G is transitive $j = gi$ for some $g \in G$. Thus $j \in Gi$ and so $Gi = I$.

(b) $\Longrightarrow$ (c): Since I is not empty, there exists $i \in I$. So by (b), $G = Gi$.

(c) $\Longrightarrow$ (d): By definition, Gi is an orbit. So (c) implies (d).

(d) $\Longrightarrow$ (e): Let O be any orbit for G on I. So O and I both are orbits for G on I and $O \cap I = O \neq \emptyset$. Thus $O = I$ and I is the only orbit for G on I.

(e) $\Longrightarrow$ (f): Both Gi and Gj are orbits for G on I and so equal by assumption.

(f) $\Longrightarrow$ (g): Let $i, j \in I$. By assumption $Gi = Gj$ and so by 2.1.11 $i \equiv j \pmod G$.

(g) $\Longrightarrow$ (a): Let $i, j \in I$. Then $i \equiv j \pmod G$, that is $j = gi$ for some $g \in G$. So G is transitive on I. $\square$

Definition 2.1.14. *(a) Let* G *be a group and* $(I, \diamond)$ *and* $(J, \square)$ *be* G*-sets. A function* $f : I \to J$ *is called* G-homomorphism *if*

$$f(a \diamond i) = a \,\square\, f(i)$$

for all $a \in G$ *and* i. *A* G-isomorphism *is bijective* G*-homomorphism. We say that* I *and* H *are* G*-isomorphic and write*

$$I \cong_G J$$

if there exists an G*-isomorphism from* I *to* J.

(b) Let I *be a* G *set and* $J \subseteq I$. *Then*

$$\operatorname{Stab}^{\diamond}_G(J) = \{g \in G \mid gj = j \text{ for all } j \in J\}$$

and for $i \in I$

$$\operatorname{Stab}^{\diamond}_G(i) = \{g \in G \mid gi = i\}$$

$\operatorname{Stab}^{\diamond}_G(i)$ *is called the* stabilizer *of* i *in* G *with respect to* $\diamond$.

Example 2.1.15.

Recall that by 2.1.2(2), $\mathrm{Sym}(n)$ acts on $\{1,2,3,\ldots,n\}$ via $f \diamond i = f(i)$. We have

$$\mathrm{Stab}^{\diamond}_{\mathrm{Sym}(3)}(1)\} = \{f \in \mathrm{Sym}(3) \mid f(1) = 1\} = \{(1),(2,3)\}$$

and

$$\mathrm{Stab}^{\diamond}_{\mathrm{Sym}(5)}(\{2,3\}) = \{f \in \mathrm{Sym}(5) \mid f(2) = 2 \text{ and } f(3) = 3\} \cong \mathrm{Sym}(\{1,4,5\}) \cong \mathrm{Sym}(3).$$

Theorem 2.1.16 (Isomorphism Theorem for G-sets)**.** *Let G be a group and $(I,\diamond)$ a G-set. Let $i \in I$ and put $H = \mathrm{Stab}_G(i)$. Then*

$$\phi: \quad G/H \to Gi, \quad aH \to ai$$

is a well-defined G-isomorphism.

In particular

$$G/H \cong_G Gi, \quad |Gi| = |G/\mathrm{Stab}_G(i)| \quad \textit{and} \quad |Gi| \textit{ divides } |G|$$

Proof. Let a,b in G. Then

$$\begin{array}{rcll} & ai = bi & & \\ \Longleftrightarrow & a^{-1}(ai) = a^{-1}(bi) & - & 2.1.7(c) \\ \Longleftrightarrow & i = (a^{-1}b)i & - & 2.1.7(a), (\text{act ii}) \\ \Longleftrightarrow & a^{-1}b \in H & - & H = \mathrm{Stab}(i), \text{ Definition of Stab} \\ \Longleftrightarrow & aH = bH & - & 1.7.6(c), (g) \end{array}$$

So $ai = bi$ if and only if $aH = bH$. The backward direction of this statement means that ϕ is well defined, and the forward direction that ϕ is 1-1. Let $j \in Gi$. Then $j = gi$ for some $g \in G$ and so $\phi(gH) = gi = j$. Thus ϕ is onto. Since

$$\phi(a(bH) = \phi((ab)H) = (ab)i = a(bi) = a\phi(bH)$$

ϕ is a G-homomorphism. □

Example 2.1.17.

By 2.1.9(2), $\mathrm{Sym}(n)$ acts transitively on $\{1,2,\ldots,n\}$. Thus $\mathrm{Sym}(n) \diamond n = \{1,2,\ldots n\}$. Set $H := \mathrm{Stab}^{\diamond}_{\mathrm{Sym}(n)}(n)$. Then

$$H = \{f \in \mathrm{Sym}(n) \mid f(n) = n\} \cong \mathrm{Sym}(n-1).$$

Then by 2.1.16

$$\operatorname{Sym}(n)/H \cong \{1,2,3\ldots,n\} \text{ as } \operatorname{Sym}(n)\text{-sets}$$

Note here that $|\operatorname{Sym}(n)/H| = \frac{n!}{(n-1)!} = n = |\{1,2,3,\ldots,n\}|$.

Theorem 2.1.18 (Orbit Equation)**.** *Let G be a group acting on a finite set I. Let $I_k, 1 \le k \le n$ be the distinct orbits for G on I. For each $1 \le k \le n$ let i_k be an element of I_k. Then*

$$|I| = \sum_{i=1}^{n} |I_k| = \sum_{i=1}^{n} |G/\operatorname{Stab}_G(i_k)|.$$

Proof. By 2.1.11 I is the disjoint union of the I_k's. Hence

$$|I| = \sum_{k=1}^{n} |I_k|. \tag{1}$$

By 2.1.11 $I_k = Gi_k$ and so 2.1.16 implies

$$|I_k| = |G/\operatorname{Stab}_G(i_k)| \text{ for all } 1 \le k \le n. \tag{2}$$

Substituting (2) into (1) gives the theorem. □

Example 2.1.19.

Define

$$H := \big\{ f \in \operatorname{Sym}(5) \big| f(\{1,2\}) = \{1,2\} \big\}.$$

So an elements of H can permute the two elements of $\{1,2\}$ and the three elements of $\{3,4,5\}$. Thus

$$H \cong \operatorname{Sym}(\{1,2\}) \times \operatorname{Sym}(\{3,4,5\}).$$

For example $(1,2)$, $(3,4)$, and $(1,2)(3,5,4)$ are elements of H, but $(1,3)(2,5)$ is not.

What are the orbits of H on $\{1,2,3,4,5\}$? If $f \in H$, then $f(1)$ is 1 or 2. So $H \diamond 1 = \{1,2\}$. $f(3)$ can be $3, 4$ or 5 and so $H \diamond 3 = \{3,4,5\}$. So the orbits are

$$\{1,2\} \text{ and } \{3,4,5\}.$$

Next we compute the stabilizers of 1 and 3 in H.

Let $f \in H$. Then $f \in \operatorname{Stab}_H(1)$ if and only if $f(1) = 1$. Since f permutes $\{1,2\}$ we also must have $f(2) = 2$, but f can permute $\{3,4,5\}$ arbitrarily. It follows that

$$\operatorname{Stab}_H(1) \cong \operatorname{Sym}(\{3,4,5\}).$$

$f \in \operatorname{Stab}_H(3)$ if and only if $f(3) = 3$. f can permute $\{1,2\}$ and $\{4,5\}$ arbitrarily. Thus

$$\operatorname{Stab}_H(3) \cong \operatorname{Sym}(\{1,2\}) \times \operatorname{Sym}(\{4,5\}).$$

The Orbit Equation 2.1.18 now implies that

$$|H/\operatorname{Stab}_H(1)| + |H/\operatorname{Stab}_H(3)| = |\{1,2,3,4,5\}|.$$

Observe that $|H| = 2! \cdot 3! = 12$, $|\operatorname{Stab}_H(1)| = 3! = 6$ and $|\operatorname{Stab}_H(3)| = 2! \cdot 2! = 4$. So

$$\frac{12}{6} + \frac{12}{4} = 5$$

and

$$2 + 3 = 5.$$

2.2 Sylow's Theorem

Definition 2.2.1. *Let p be a prime and G a group. Then G is a* p-group *if $|G| = p^k$ for some $k \in \mathbb{N}$.*

Example 2.2.2.

$|\mathbb{Z}_1| = 1 = p^0$. So $\mathbb{Z}_1$ is a p-group for every prime p.
$|\mathbb{Z}_2| = 2$. So $\mathbb{Z}_2$ is a 2-group.
$\mathbb{Z}_3$ is a 3-group.
$\mathbb{Z}_4$ is a 2-group.
$\mathbb{Z}_5$ is a 5-group.
$\mathbb{Z}_6$ is not a p-group for any prime p.
$\mathbb{Z}_7$ is a 7-group.
$\mathbb{Z}_8$ is a 2-group.
$\mathbb{Z}_9$ is a 3-group.
$\mathbb{Z}_{10}$ is a not a p-group for any prime p.

Definition 2.2.3. *Let G be a finite group and p a prime. A* p-subgroup *of G is a subgroup of G which is a p-group. A* Sylow p-subgroup *of G is a maximal p-subgroup of G, that is S is a Sylow p-subgroup of G provided that*

(i) S is a p-subgroup of G.

(ii) If P is a p-subgroup of G with $S \leq P$, then $S = P$.

$\mathrm{Syl}_p(G)$ *denotes the set of Sylow p-subgroups of G.*

Lemma 2.2.4. *Let G be a finite group, p a prime and let $|G| = p^k l$ with $k \in \mathbb{N}$, $l \in \mathbb{Z}^+$ and $p \nmid l$.*

(a) If P is a p-subgroup of G, then $|P| \leq p^k$.

(b) If $S \leq G$ with $|S| = p^k$, then S is a Sylow p-subgroup of G.

Proof. (a) Since P is a p-group, $|P| = p^n$ for some $n \in \mathbb{N}$. By Lagrange's Theorem, $|P|$ divides $|G|$ and so p^n divides $p^k l$. Since $p \nmid l$ we conclude that $n \leq k$ and so $|P| = p^n \leq p^k$.

(b) Since $|S| = p^k$ and $S \leq G$, S is a p-subgroup of G. Suppose that $S \leq P$ for some p-subgroup P of G. By (a) $|P| \leq p^k = |S|$. Since $P \subseteq S$ this implies $P = S$ and so S is a Sylow p-subgroup of G. □

Example 2.2.5.

(a) $|\mathrm{Sym}(3)| = 3! = 6 = 2 \cdot 3$. $\langle(1,2)\rangle$ has order 2 and so by 2.2.4(b), $\langle(1,2)\rangle$is a Sylow 2-subgroup of Sym(3).

$\langle(1,2,3)\rangle$ has order 3 and so is a Sylow 3-subgroup of Sym(3).

(b) $|\mathrm{Sym}(4)| = 4! = 24 = 2^3 \cdot 3$. D_4 is a subgroup of order eight of Sym(4) and so D_4 is a Sylow 2-subgroup of Sym(4).

$\langle(1,2,3)\rangle$ is a Sylow 3-subgroup of Sym(4).

(c) $|\mathrm{Sym}(5)| = 5! = 5 \cdot 24 = 2^3 \cdot 3 \cdot 5$. So D_4 is a Sylow 2-subgroup of Sym(5), $\langle(1,2,3)\rangle$ is a Sylow 3-subgroup of Sym(5) and $\langle(1,2,3,4,5)\rangle$ is a Sylow 5-subgroup of Sym(5).

(d) $|\mathrm{Sym}(6)| = 6! = 6 \cdot 5! = 2^4 \cdot 3^2 \cdot 5$. $D_4 \times \langle(5,6)\rangle$ is a subgroup of order 16 of Sym(6) and so is a Sylow 2-subgroup of Sym(6).

$\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$ is a group of order 9, and so is a Sylow 3-subgroup of Sym(6).

$\langle(1,2,3,4,5)\rangle$ is a Sylow 5-subgroup of Sym(6).

Definition 2.2.6. *Let G be a group acting on a set I. Let $i \in I$. Then i is called a* fixed-point *of G on I provided that $gi = i$ for all $g \in G$.* $\mathrm{Fix}_I(G)$ *is the set of all fixed-points for G on I. So*

$$\mathrm{Fix}_I(G) = \{i \in I \mid gi = i \text{ for all } g \in G\}.$$

Lemma 2.2.7 (Fixed-Point Formula)**.** *Let p be a prime and P a p-group acting on finite set I. Then*

$$|I| \equiv |\mathrm{Fix}_I(P)| \pmod{p}.$$

In particular, if $p \nmid |I|$, then P has a fixed-point on I.

Proof. Let $I_1, I_2, \ldots, I_n$ be the orbits of P on I and choose notation such that

$$|I_l| = 1 \text{ for } 1 \leq l \leq m \text{ and } |I_l| > 1 \text{ for } m < l \leq n. \tag{1}$$

Let $i \in I$ and pick $1 \leq l \leq n$ with $i \in I_l$. By 2.1.11

$$I_l = Gi. \tag{2}$$

We have

$$\begin{aligned}
& i \in \mathrm{Fix}_I(P) & & \\
\iff & gi = i \text{ for all } g \in G & - & \text{ Definition of } \mathrm{Fix}_I(P) \\
\iff & Gi = \{i\} & - & \text{ Definition of } Gi \\
\iff & |Gi| = 1 & - & \text{ since } i \in Gi \\
\iff & |I_l| = 1 & - & \text{ (2)} \\
\iff & l \leq m & - & \text{ (1)}
\end{aligned} \tag{3}$$

Thus

$$\mathrm{Fix}_I(P) = \bigcup_{l=1}^{m} I_l. \tag{4}$$

Let $m < l \leq n$. By 2.1.16 $|I_l|$ divides $|P|$. Since $|P|$ is a power of p, we conclude that $|I_l|$ is a power of p. Since $|I_l| \neq 1$ we get $p \big| |I_l|$ and so

$$|I_l| \equiv 0 \pmod p \text{for all } m < l \leq n. \tag{5}$$

We compute

$$|I| \overset{2.1.18}{=} \sum_{l=1}^{n} |I_l| = \sum_{l=1}^{m} |I_l| + \sum_{l=m+1}^{n} |I_l| \overset{(4)}{=} |\mathrm{Fix}_I(P)| + \sum_{l=m+1}^{n} |I_l|,$$

and so by (5)

$$|I| \equiv |\mathrm{Fix}_I(P)| \pmod p.$$

□

Example 2.2.8.

Let $P = \langle (1,2,3),(4,5,6)\rangle$ viewed as subgroup of Sym(8). Then P has order 9 and so P is a 3-group. The orbits of P on $I := \{1,2,3,\ldots,8\}$ are $\{1,2,3\}$, $\{4,5,6\}$, $\{7\},\{8\}$. The fixed-points of P on I are 7 and 8. So $|\operatorname{Fix}_I(P)| = 2$, $|I| = 8$ and $8 \equiv 2 \pmod 3$, as predicted by 2.2.7.

Definition 2.2.9. *Let G be a group and $(I,\diamond)$ a G-set.*

(a) $\mathcal{P}(I)$ is the sets of all subsets of $\mathcal{I}$. $\mathcal{P}(I)$ is called the power set *of I.*

(b) For $a \in G$ and $J \subseteq I$ put $a \diamond J = \{a \diamond j \mid j \in J\}$.

(c) $\diamond_{\mathcal{P}}$ denotes the function

$$\diamond_{\mathcal{P}}: \quad G \times \mathcal{P}(I) \to \mathcal{P}(I), \quad (a,J) \to a \diamond J$$

*(d) Let J be a subset of I and $H \le G$. Then J is called H-*invariant *if*

$$hj \in J$$

for all $h \in H, j \in J$.

(e) Let $H \le G$ and J be a H-invariant. Then $\diamond_{H,J}$ denotes the function

$$\diamond_{H,J}: \quad H \times J \to J, \quad (h,j) \to h \diamond j$$

Lemma 2.2.10. *Let G be a group and $(I,\diamond)$ a G-set.*

(a) $\diamond_{\mathcal{P}}$ is an action of G on $\mathcal{P}(I)$.

(b) Let $H \le G$ and J be a H-invariant subset of I. Then $\diamond_{H,J}$ is an action of H on J.

Proof. (a) Let $a,b \in J$ and J a subset I.

$$eJ = \{ej \mid j \in J\} = \{j \mid j \in J\} = J$$

and

$$a(bJ) = a\{bj \mid j \in J\} = \{a(bj) \mid j \in J\} = \{(ab)j \mid j \in J\} = (ab)J.$$

Thus $\diamond_{\mathcal{P}}$ fulfills both axioms of an action.

(b) By 1.5.3 $e_H = e_G$ and so $e_H j = e_G j = j$ for all $j \in J$. Clearly $(ab)j = a(bj)$ for all $a,b \in H$ and $j \in J$ and so (b) holds. □

Definition 2.2.11. *Let A and B be subsets of the group G. We say that A is* conjugate *to B in G if there exists $g \in G$ with $A = gBg^{-1}$.*

Lemma 2.2.12. *Let G be a group, H a subgroup of G and $a \in G$.*

(a) aHa^{-1} is a subgroup of G isomorphic to H. So conjugate subgroups of G are isomorphic.

(b) If H is a p-subgroup of G for some prime p, so is aHa^{-1}.

Proof. (a) By Homework 3#2 $\phi : G \to G, g \to aga^{-1}$ is an isomorphism. Thus by 1.9.10(c) the restriction $\phi_H : H \to G, h \to aha^{-1}$ is homomorphism. Since ϕ is 1-1, so is ϕ_H. Thus by 1.6.5(d), $H \cong \operatorname{Im} \phi_H$. Since

$$\operatorname{Im} \phi_H = \{\phi_H(h) \mid h \in H\} = \{aha^{-1} \mid h \in H\} = aHa^{-1}$$

we get $H \cong aHa^{-1}$.

(b) By (a) $|H| = |aHa^{-1}|$. So if $|H|$ is a power of p also $|aHa^{-1}|$ is a power of p. □

Lemma 2.2.13. *Let G be a finite group and p a prime. Then*

$$\diamond : \quad G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G), \quad (g, P) \to gPg^{-1}$$

is a well-defined action of G on $\mathrm{Syl}_p(G)$. This action is called the action of G on $\mathrm{Syl}_p(G)$ by conjugation.

Proof. By Homework 6#3 G acts on G by conjugation. So by 2.2.10(a), G acts on $\mathcal{P}(G)$ by conjugation. Hence by 2.2.10(b) it suffices to show that $\mathrm{Syl}_p(G)$ invariant under G with respect to conjugation. That is we need to show that if S is a Sylow p-subgroup of G and $g \in G$, then also gSg^{-1} is a Sylow p-subgroup of G. By 2.2.12(b) gSg^{-1} is a p-subgroup of G.

Let P be a p-subgroup of G with $gSg^{-1} \leq P$. Then by 1.8.1(e) $S \leq g^{-1}Pg$. By 2.2.12(b) $g^{-1}Pg$ is a p-subgroup of G and since S is a Sylow p-subgroup we conclude $S = g^{-1}Pg$. Thus by 1.8.1(d) also $gSg^{-1} = P$. Hence gSg^{-1} is a Sylow p-subgroup of G. □

Lemma 2.2.14 (Order Formula)**.** *Let A and B be subgroups of the group G.*

(a) Put $AB/B = \{gB \mid g \in AB\}$. The map

$$\phi : \quad A/A \cap B \to AB/B, \quad a(A \cap B) \to aB$$

is a well-defined bijection.

(b) If A and B are finite, then

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Proof. (a) Let $a, d \in A$. Then by 1.5.3 $a^{-1}d \in A$. We have

$$\begin{array}{rcll} & aB = dB & & \\ \iff & a^{-1}d \in B & - & 1.7.6 \\ \iff & a^{-1}d \in A \cap B & - & \text{since } a^{-1}d \in A \\ \iff & a(A \cap B) = d(A \cap B) & - & 1.7.6 \end{array}$$

This shows that ϕ is well-defined and 1-1. Let $T \in AB/B$. Then $T = gB$ for some $g \in AB$. By definition of AB, $g = ab$ for some $a \in A, b \in B$. Since $bB = B$ we have

$$T = abB = aB \tag{1}$$

So $\phi(a(A \cap B)) = aB$ and ϕ is onto.

(b) Let $T \in AB/B$. By (1) $T = aB \subseteq AB$. So $\bigcup_{T \in AB/B} T \subseteq AB$. If $g \in AB$, then $g \in gB \subseteq_{T \in AB/B} T$. Hence

$$\bigcup_{T \in AB/B} T = AB. \tag{2}$$

By 1.7.6

$$\text{distinct cosets are disjoint,} \tag{3}$$

and by 1.7.7(c)

$$|T| = |B| \text{ for all } B \in AB/B. \tag{4}$$

Thus

$$|AB| \overset{(2),(3)}{=} \sum_{T \in AB/B} |T| \overset{(4)}{=} \sum_{T \in AB/B} |B| = |AB/B| \cdot |B| \overset{(a)}{=} |A/A \cap B| \cdot |B|.$$

Lagrange's Theorem gives $|A/A \cap B| = \frac{|A|}{|A \cap B|}$ and so

$$|AB| = \frac{|A|}{|A \cap B|} \cdot |B| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

□

Theorem 2.2.15. *Let G be a finite group and p a prime.*

(a) (Second Sylow Theorem) *G acts transitively on $\mathrm{Syl}_p(G)$ by conjugation, that is any two Sylow p-subgroups of G are conjugate in G and so if S and T are Sylow p-subgroups of G, then $S = gTg^{-1}$ for some $g \in G$.*

(b) (Third Sylow Theorem) *The number of Sylow p-subgroups of G divides $|G|$ and is congruent to 1 modulo p.*

Proof. By 2.2.13 G acts on $\mathrm{Syl}_p(G)$ by conjugation. Let I be an orbit for G on $\mathrm{Syl}_p(G)$ and $P \in I$. Then P is a Sylow p-subgroup of G. We will first show that

$$(1) \qquad P \text{ has a unique fixed-point on } \mathrm{Syl}_p(G), \text{ namely } P.$$

Let $Q \in \mathrm{Syl}_p(G)$. Then P fixes Q (with respect to the action by conjugation) if and only if $aQa^{-1} = Q$ for all $a \in P$. Clearly $aPa^{-1} = P$ for all $a \in P$ and so P is a fixed-point for P on $\mathrm{Syl}_p(G)$. Now let Q be any fixed-point for P on $\mathrm{Syl}_p(G)$. Then $aQa^{-1} = Q$ for all $a \in P$ and so by 1.8.1 $aQ = Qa$. Thus

$$PQ = \{ab \mid a \in P, b \in Q\} = \bigcup \{a \in P\}\{ab \mid b \in Q\} = \bigcup_{a \in P} aQ = \bigcup_{a \in P} Qa = QP.$$

Thus by Homework 4#4 PQ is a subgroup of G. By 2.2.14(b),

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}.$$

Since P and Q are p-groups, we conclude that $|P|$ and $|Q|$ are powers of p. Hence also $|PQ|$ is a power of p. Thus PQ is a p-subgroup of G. Since $P \leq PQ$ and P is a maximal p-subgroup of G, $P = PQ$. Similarly, since $Q \leq PQ$ and Q is a maximal p-subgroup of G, $Q = PQ$. Thus $P = Q$ and (1) is proved.

$$(2) \qquad |I| \equiv 1 \pmod p.$$

By (1) $\mathrm{Fix}_I(P) = \{P\}$. Hence $|\mathrm{Fix}_I(P)| = 1$. By 2.2.7 $|I| \equiv |\mathrm{Fix}_I(P)| \pmod p$ and so (2) holds.

$$(3) \qquad I \text{ is the unique orbit for } G \text{ on } \mathrm{Syl}_p(G).$$

Suppose this is false and let J be an orbit for G on $\mathrm{Syl}_p(G)$ distinct from I. Then by (2) applied to J,

$$(*) \qquad |J| \equiv 1 \pmod p.$$

On the other hand, $P \notin J$ and so by (1), $\mathrm{Fix}_J(P) = \emptyset$. Hence $|\mathrm{Fix}_J(P) = 0$ and by 2.2.7 $|J| \equiv 0 \pmod p$, a contradiction to (*).

Thus (3) holds.

By (3) and 2.1.13(e),(a) G acts transitively on $\mathrm{Syl}_p(G)$. Hence the Second Sylow Theorem holds. Moreover, $\mathrm{Syl}_p(G) = I$ and so by 2.1.16 $|I|$ divides $|G|$ and by (2) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$. □

Lemma 2.2.16. *Let I be a set. Then* $\mathrm{Sym}(n)$ *acts on* I^n *via*

$$f \diamond (i_1, i_2, \ldots i_n) = (i_{f^{-1}(1)}, i_{f^{-1}(2)}, \ldots, i_{f^{-1}(n)}).$$

So if $i = (i_1, i_2, \ldots, i_n) \in I^n$ *and* $j = f \diamond i = (j_1, j_2, \ldots, j_n)$ *then* $j_{f(l)} = i_l$.

Proof. Before we start we the proof a couple of examples: $(1,2,3) \diamond (x,y,z) = (z,x,t)$ and $(1,3)(2,5) \diamond (a,b,c,d,e) = (c,e,a,d,b)$.

Clearly $(1) \diamond i = i$ for all $i \in I^n$. So (act i) holds.

Let $a, b \in \mathrm{Sym}(n)$ and $i \in I$. Put $j = b \diamond i$ and $k = a \diamond (b \diamond i) = a \diamond j$. Then $k_{a(l)} = j_l$ and so also $k_{a(b(l))} = j_{b(l)} = i_l$. Hence $k_{(ab)(l)} = i_l$ and so $k = (ab) \circ i$. Thus (act ii) holds and $\diamond$ is an action of $\mathrm{Sym}(n)$ on I^n. □

Theorem 2.2.17 (Cauchy's Theorem)**.** *Let G be a finite group and p a prime dividing the order of G. Then G has an element of order p.*

Proof. Let $\diamond$ be the action of $\mathrm{Sym}(p)$ on G^p given in 2.2.16. Let $h = (1,2,3,\ldots,p) \in \mathrm{Sym}(p)$ and $H = \langle h \rangle$. Then H is a subgroup of order p of $\mathrm{Sym}(p)$. Observe that

$$h \diamond (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

and inductively,

(1) $$h^i \diamond (g_1, g_2, \ldots, g_p) = (g_{i+1}, g_{i+2}, \ldots, g_p, g_1, \ldots, g_i) \text{ for all } 0 \le i < p$$

Hence h fixes $(g_1, g_2, \ldots, g_p)$ if and only if $g_1 = g_2, \ldots, g_{p-1} = g_p, g_p = g_1$ and so

(2) $$\mathrm{Fix}_{G^p}(h) = \{(g, g, \ldots, g) \mid g \in G\}.$$

Put

$$J := \{(g_1, g_2, \ldots g_p) \in G^p \mid g_1 g_2 \ldots g_p = e\}.$$

If $g_1 = g_2 = \ldots = g_p$, then $g_1 g_2 \ldots g_p = g_1^p$ and so by (2):

(3) $$\mathrm{Fix}_J(H) = \{(g, g, \ldots, g) \mid g \in G, g^p = e\}$$

In particular $(e, \ldots, e) \in \mathrm{Fix}_J(H)$ and so

(4) $$|\mathrm{Fix}_J(H)| \ge 1.$$

In view of (3) our is now to show that $\mathrm{Fix}_J(H) > 1$. For this we will use the Fixed-Point-Formula 2.2.7 for H on acting on J. But we first must make sure that H acts on J. By 2.2.10(b), we need to verify that J is H-invariant. Let $(g_1, g_2, \ldots g_p) \in J$. Then

$$g_1 g_2 \dots g_p = e.$$

Multiplying with g_1^{-1} from the left and g_1 from the right gives

$$g_2 g_3 \dots g_p g_1 = e,$$

and so

$$(g_2, g_3, \dots, g_p, g_1) \in J.$$

An easy induction proof shows that

$$(g_{i+1}, g_{i+2}, \dots, g_p, g_1, \dots, g_i) \in J \text{ for all } 1 \leq i < p.$$

Hence by (1) $h^i \diamond (g_1, \dots g_p) \in J$ for all $1 \leq i < p$. Since $H = \{h^i \mid 0 \leq i < p\}$ we conclude that J is an H-invariant subset of G^n. Thus by 2.2.10(b), H acts on J and so by 2.2.7

$$|J| \equiv |\operatorname{Fix}_J(H)| \pmod{p}. \tag{5}$$

Note that $|J| = |G|^{p-1}$. Indeed we can choose $g_1, g_2, \dots, g_{p-1}$ freely and then g_p is uniquely determined as $g_p = (g_1 \dots g_p)^{-1}$. Since p divides $|G|$ we conclude that $p \mid |J|$ and so by (5)

$$p \big| |\operatorname{Fix}_J(H)|. \tag{6}$$

From (4) and (6) $|\operatorname{Fix}_J(H)| \geq p$. So by (3) there exists $g \in G$ with $g \neq e$ and $g^p = e$. Thus $|g| \big| p$. Since $g \neq e$ and p is a prime, $|g| = p$ and so Cauchy's Theorem holds. □

Proposition 2.2.18. *Let G be a finite group and p a prime. Then any p-subgroup of G is contained in a Sylow p-subgroup of G. In particular, G has a Sylow p-subgroup.*

Proof. Let P be a p-subgroup and choose a p-subgroup S of G of maximal order with respect to $P \leq S$. If Q is a p-subgroup of G with $S \leq Q$, then also $P \leq Q$ and so by maximality of $|S|$, $|Q| \leq |S|$. Since $S \leq Q$ we get $|S| = |Q|$ and $S = Q$. So S is a Sylow p-subgroup of G.

In particular, the p-subgroup $\{e\}$ of G is contained in a Sylow p-subgroup of G and so G has Sylow p-subgroup.

Comment:This should have been proved right after Example 2.2.5, since the existence of Sylow subgroups has been used various times □

Theorem 2.2.19 (First Sylow Theorem)**.** *Let G be a finite group, p a prime and $S \in \mathrm{Syl}_p(G)$. Let $|G| = p^k l$ with $k \in \mathbb{N}$, $l \in \mathbb{Z}^+$ and $p \nmid l$ (p^k is called the p-part of $|G|$). Then $|S| = p^k$. In particular,*

$$\mathrm{Syl}_p(G) = \{P \leq G \big| |P| = p^k\}$$

and G has a subgroup of order p^k.

Proof. The proof that $|S| = p^k$ is by complete induction on k. If $k = 0$, then by 2.2.4 $|S| \leq p^k = 1$ and so $|S| = 1$. Assume now $k > 0$ and that the theorem is true for all finite groups whose order has p-part smaller than p^k.

Since $k > 0$, $p \big| |G|$. So by Cauchy's Theorem G has a subgroup P of order p. By 2.2.18 P is contained in a Sylow p-subgroup T of G. Then $|T| > 1$. By the Second Sylow Theorem, S is conjugate to T and so by 2.2.12 $S \cong T$ and $|S| = |T|$. Thus

$$|S| > 1. \tag{1}$$

Let N be the stabilizer of S with respect to the action of G on $\mathrm{Syl}_p(G)$ by conjugation. So

$$N = \{g \in G \mid gSg^{-1} = S\}.$$

Clearly $S \leq N$ and by 1.8.6(c), $S \trianglelefteq N$. By the Second Sylow Theorem, $\mathrm{Syl}_p(G) = \{gSg_{-1} \mid g \in G\}$ and so by 2.1.16

$$|G/N| = |\,\mathrm{Syl}_p(G)|.$$

The Third Sylow Theorem implies

$$|G/N| \equiv 1 \pmod p.$$

Thus $p \nmid |G/N|$. By Lagrange's theorem, $p^k l = |G| = |G/N| \cdot |N|$. We conclude that

$$|N| = p^k m$$

for some $m \in \mathbb{Z}^+$ with $p \nmid m$. Let $|S| = p^n$. Then by Lagrange's theorem

$$|N/S| = \frac{|N|}{|S|} = p^{k-n}m.$$

Let R be a Sylow p-subgroup of N/S. By (1) $n \neq 0$. So $k - n < k$ and by the induction assumption

$$|R| = p^{k-n}.$$

By 1.9.14(g), there exists a subgroup U of N with $S \leq U$ and $U/S = R$. By Lagrange's Theorem

$$|U| = |U/S| \cdot |S| = |R| \cdot |S| = p^{k-n}p^n = p^k.$$

So U is a p-group and since $S \leq U$ and S is a maximal p-subgroup, $S = U$. Thus $|S| = p^k$.

We proved that any p-Sylow subgroup of G has order p^k. Conversely by 2.2.4 any subgroups of order p^k is a Sylow p-subgroup and so

$$\mathrm{Syl}_p(G) = \{P \leq G \big| |P| = p^k.\}$$

□

Example 2.2.20.

(1) The subgroups of order 2 in $\mathrm{Syl}_2(\mathrm{Sym}(3))$ are $\langle(1,2)\rangle, \langle(1,3)\rangle$ and $\langle(2,3)\rangle$ and so by the First Sylow Theorem

$$\mathrm{Syl}_2(\mathrm{Sym}(3)) = \{\langle(1,2)\rangle, \langle(1,3)\rangle\langle(2,3)\rangle\}.$$

(2) Let S be a Sylow 5-subgroup of $\mathrm{Sym}(5)$. Since $|\mathrm{Sym}(5)| = 5! = 2^3 \cdot 3 \cdot 5$, $|H|$ has order 5. Let $1 \neq h \in H$. Then h is a five cycle and so $h = (v, w, x, y, z)$. There are 120 choices for the tuple (v, w, x, y, x). But any of the five cyclic permutations:

$$(v, w, x, y, x), (w, x, y, z, v), (x, y, z, v, w), (y, z, v, w, x), (z, v, w, x, y)$$

is also equal to h. Hence there are $\frac{120}{5} = 24$ elements of order five in $\mathrm{Sym}(5)$. Since $H = \langle h \rangle$ any of the four elements of order five in H uniquely determine H. Thus there are $\frac{24}{4} = 6$ Sylow 5-subgroups in G. Note here that $6 \equiv 1 \pmod 5$ in accordance with the Third Sylow Theorems.

(3) Let G be any group of order 120 and s_5 the number of 5-Sylow subgroups of G. The Third Sylow Theorem says that $s_5 \mid 120$ and $s_5 \equiv 1 \pmod 5$. So $5 \nmid s_5$ and since $120 = 5 \cdot 24$ we conclude that $s_5 \mid 24$. The number less or equal to 24 and congruent to 1 modulo 5 are $1, 6, 11, 16$ and 21. Of these only 1 and 6 divide 24. So $s_5 = 1$ or 6.

Lemma 2.2.21. *Let G be a finite group and p a prime. Let S be a Sylow p-subgroup of G. Then S is normal in G if and only if S is the only Sylow p-subgroup of G.*

Proof. By the Second Sylow Theorem

$$\mathrm{Syl}_p(G) = \{gSg^{-1} \mid g \in G\}.$$

So $\mathrm{Syl}_p(G) = \{S\}$ if and only if $S = gSg^{-1}$ for all g in G and so by 1.8.6(b) if and only if S is normal in G. □

Lemma 2.2.22. *Let $\phi : A \to B$ be a homomorphism of groups. Then ϕ is 1-1 if and only of* $\ker \phi = \{e_A\}$.

Proof. Let $a, b \in A$. Then

$$\begin{array}{rcll} & \phi(a) = \phi(b) & & \\ \iff & \phi(a)^{-1}\phi(b) = e_B & & \\ \iff & \phi(a^{-1}b) = e_B & - & 1.6.5 \\ \iff & a^{-1}b \in \ker\phi & - & \text{definition of } \ker\phi \\ \iff & b = ak \text{ for some } k \in \ker\phi & - & 1.7.6(c)(a) \end{array}$$

So $\phi(a) = \phi(b)$ implies $a = b$ if and only if e_A is the only element in $\ker\phi$. $\square$

Example 2.2.23.

(1) $\langle(1,2,3)\rangle$ is the only Sylow 3-subgroup of Sym(3) and so by 2.2.21 $\langle(1,2,3)\rangle \trianglelefteq \mathrm{Sym}(3)$.

(2) Sym(3) has three Sylow 2-subgroups, and by 2.2.21 $\langle(1,2)\rangle \ntrianglelefteq \mathrm{Sym}(3)$.

(3) A group G is called simple if $\{e\}$ and G are the only normal subgroups of G. Let G be a simple group of order 168. We will show that G is isomorphic to a subgroup of Sym(8). Let s_7 be the number of Sylow 7-subgroups of G and let S be a Sylow 7-subgroup of G. By the First Sylow Theorem, $|S| = 7$ and so $S \neq \{e\}$ and $S \neq G$. Since G is simple, $S \ntrianglelefteq G$ and so by 2.2.21 $s_7 \neq 1$. Since $|G| = 168 = 7 \cdot 24$, the Third Sylow Theorem implies that $s_7 \equiv 1 \pmod 7$ and $s_7 \mid 24$. The numbers which are less or equal to 24 and are 1 modulo 7 are $1, 8, 15$ and 22. Of these only 1 and 8 divide 24. As $s_7 \neq 1$ we have $s_7 = 8$.

   Let $\phi : G \to \mathrm{Sym}(\mathrm{Syl}_7(G))$ be the homomorphism associated to the action of G on $\mathrm{Syl}_7(G)$ by conjugation (see 2.1.3(a)). So for g in G we have $\phi(g)(S) = gSg^{-1}$.

   Suppose that $\ker\phi = G$. Then $\phi(g) = \mathrm{id}_{\mathrm{Sym}_7(G)}$ for all $g \in G$ and so

$$S = \phi(g)(S) = gSg^{-1}$$

   for all $g \in G$. Thus by 1.8.6(b), $S \trianglelefteq G$, a contradiction since G is simple.

   Hence $\ker\phi \neq G$. Since G is simple, $\ker\phi = \{e\}$. Thus by 2.2.22 ϕ is 1-1 and so by 1.6.5(d),

$$G \cong \mathrm{Im}\,\phi \tag{1}$$

   and $\mathrm{Im}\,\phi$ is a subgroup of $\mathrm{Sym}(\mathrm{Syl}_7(G))$. Since $|\,\mathrm{Syl}_7(G)| = n_7 = 8$ we conclude from Homework 3#5 that there exists an isomorphism,

$$\alpha : \mathrm{Sym}(\mathrm{Syl}_7(G)) \to \mathrm{Sym}(8).$$

   By 1.9.10(c) $\alpha\,|_{\mathrm{Im}\,\phi}$ is 1-1 and so by 1.6.5(d)

$$\mathrm{Im}\,\phi \cong \alpha(\mathrm{Im}\,\phi) \tag{2}$$

and $\alpha(\operatorname{Im}\phi)$ is a subgroup of Sym(8). From (1),(2) and Homework 6#5,

$$G \cong \alpha(\operatorname{Im}\phi)$$

and so G is isomorphic to a subgroup of Sym(8).

Lemma 2.2.24. *Let G be a group and A, B normal subgroups of G with $A \cap B = \{e\}$. Then AB is a subgroup of G, $ab = ba$ for all $a \in A, b \in B$ and the map*

$$\phi : A \times B \to AB, (a, b) \to ab$$

is an isomorphism of groups. In particular,

$$AB \cong A \times B.$$

Proof. Let $a \in A$ and $b \in B$. Since $B \trianglelefteq G$, $aba^{-1} \in B$ and since B is closed under multiplication,

$$aba^{-1}b^{-1} \in B. \tag{1}$$

Similarly $ba^{-1}b^{-1} \in A$ and

$$aba^{-1}b^{-1} \in A. \tag{2}$$

By assumption $A \cap B = \{e\}$ and so by (1) and (2), $aba^{-1}b^{-1} = e$. Multiplication with ba from the right gives

$$ab = ba. \tag{3}$$

From (3) we get $AB = BA$ and thus by Homework 4#4 AB is a subgroup of G.

Let $x \in AB$. Then $x = ab$ for some $a \in A, b \in B$. Hence $x = \phi\big((a, b)\big)$ and so ϕ is onto. Let $c \in A$ and $d \in B$

Suppose that $\phi\big((a, b)\big) = \phi\big((c, d)\big)$. Then $ab = cd$ and so $c^{-1}a = db^{-1}$. Since $c^{-1}a \in A$ and $db^{-1} \in B$ we get $c^{-1}a = db^{-1} \in A$. So $A \cap B = \{e\}$ implies $ca^{-1} = e = db^{-1}$. Thus $a = c$, $b = d$ and $(a, b) = (c, d)$. Therefore ϕ is 1-1.

$$\phi\big((a, b)(c, d)\big) = \phi\big((ac, bd)\big) = (ac)(bd) = a(cb)d \overset{(3)}{=} a(bc)d = (ab)(bd) = \phi\big((a, b)\big)\phi\big((c, d)\big).$$

So ϕ is a homomorphism and the lemma is proved. $\square$

Lemma 2.2.25. *Let A be finite abelian groups. Let $p_1, p_2, \dots p_n$ be the distinct prime divisor of $|A|$ (and so $|A| = p_1^{m_1}\phi_2 m_2 \dots p_n^{m_k}$ for some positive integers m_i). Then for each $1 \leq i \leq n$, G has a unique Sylow p_i-subgroup A_i and*

$$A \cong A_1 \times A_2 \times \dots \times A_n.$$

Proof. Let A_i be a Sylow p_i-subgroup of G. By 1.8.5 subgroups of abelian groups are normal. So $A_i \trianglelefteq G$. So by 2.2.21 A_i is the unique Sylow p_i-subgroup of G. By the First Sylow Theorem we have

$$|A_i| = p_i^{m_i}. \tag{1}$$

Put $D_1 = A_1$ and inductively $D_{k+1} := D_k A_{k+1}$. We will show by induction on k that

$$D_k \text{ is a subgroup of } A \text{ of order } p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}, \tag{2}$$

and

$$D_k \cong A_1 \times A_2 \times \dots \times A_k. \tag{3}$$

By (1) $D_1 = A_1$ has order $p_1^{m_1}$. Also $D_1 = A_1 \cong A_1$ and so (2) and (3) hold for $k = 1$. So suppose that (2) and (3) hold for k. We will show that (2) and (3) also holds for $k+1$.

By (2) D_k has order $p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$. By (1) A_{k+1} has order $p_{k+1}^{m_{k_1}}$. Thus $|D_k|$ and $|A_{k+1}|$ are relatively prime. Hence by Homework 4#3 $D_k \cap A_{k+1} = \{e\}$. Since A is abelian, D_k and A_{k+1} are normal subgroups of A (see 1.8.5) and so by 2.2.24 $D_{k+1} = D_k A_{k+1}$ is a subgroup of A and

$$D_{k+1} \cong D_k \times A_{k+1}. \tag{4}$$

Thus

$$|\,\mathrm{D}_{k+1}\,| = |D_k| \cdot |A_{k+1}| \overset{(1),(2)}{=} p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \cdot p_{k+1}^{m_{k+1}}.$$

and

$$D_{k+1} \overset{(4)}{\cong} D_k \times A_{k+1} \overset{(3)}{\cong} (A_1 \dots A_2 \times \dots A_k) \times A_{k+1}.$$

So (2) and (3) holds for $k+1$. Thus (2) and (3) hold for all $1 \leq i \leq n$.

By (2) applied to $k = n$ we get $|D_n| = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} = |A|$. Hence $A = D_n$. Thus (3) applied with $n = k$ gives

$$A = D_n \cong A_1 \times A_2 \times \dots \times A_n.$$

$\square$

Example 2.2.26.

Let n be positive integer and let

$$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \tag{1}$$

where the $p_1, \dots, p_k$ are distinct positive primes and $m_1, \dots, m_k$ are positive integers. Put $q_i = \frac{n}{p_i^{m_i}}$ and $A_i = q_i\mathbb{Z}/n\mathbb{Z}$. Then A_i is a subgroup of $\mathbb{Z}_n$ and by Example 1.9.14(5)

$$A_i \cong \mathbb{Z}_{\frac{n}{q_i}} = \mathbb{Z}_{p_i^{m_i}} \tag{2}$$

Thus by (1) and 2.2.4 A_i is a Sylow p_i-subgroup of $\mathbb{Z}_n$. So by 2.2.25

$$\mathbb{Z}_n \cong A_1 \times A_2 \times \dots \times A_k.$$

Hence (2) implies

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1}^{m_1} \times \mathbb{Z}_{p_2}^{m_2} \times \dots \times \mathbb{Z}_{p_k}^{m_k}. \tag{3}$$

For example

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3,$$

$$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5,$$

and

$$\mathbb{Z}_{168} \cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7.$$

Chapter 3

Field Extensions

3.1 Vector Spaces

Definition 3.1.1. *Let $\mathbb{K}$ be a field. A* vector space *over $\mathbb{K}$ (or a $\mathbb{K}$-space) is a tuple $(V, +, \diamond)$ such that*

(i) $(V, +)$ *is an abelian group.*

(ii) $\diamond : \mathbb{K} \times V \to V$ *is a function called* scalar multiplication .

(iii) $a \diamond (v + w) = (a \diamond v) + (a \diamond w)$ *for all* $a \in \mathbb{K}, v, w \in V$.

(iv) $(a + b) \diamond v = (a \diamond v) + (b \diamond v)$ *for all* $a, b \in \mathbb{K}, v \in V$.

(v) $(ab) \diamond v = a \diamond (b \diamond v)$ *for all* $a, b \in \mathbb{K}, v \in V$.

(vi) $1_{\mathbb{K}} \diamond v = v$ *for all* $v \in V$

The elements of a vector space are called vectors*. The usually just write kv for $k \diamond v$.*

Example 3.1.2.

Let $\mathbb{K}$ be a field.

(1) $\mathbb{Z}_1 = \{0\}$ is a $\mathbb{K}$-space via $f \diamond 0 = 0$ for all $k \in \mathbb{K}$.

(2) Let $n \in \mathbb{N}$. Then $\mathbb{K}^n$ is an $\mathbb{K}$-space via $k \diamond (a_1, \ldots, a_n) = (ka_1, \ldots, ka_n)$ for all $k, a_1, \ldots, a_n \in \mathbb{K}$.

(3) The ring $\mathbb{K}[x]$ of polynomials with coefficients in $\mathbb{K}$ is a $\mathbb{K}$-space via

$$k \diamond (a_0 + a_1 x + \ldots a_n x^n) = (ka_0) + (ka_1)x + \ldots (ka_n x^n)$$

for all $k, a_0, \ldots, a_n \in \mathbb{K}$.

Definition 3.1.3. *Let $\mathbb{K}$ be a field and V and $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \dots, v_n) \in V^n$ be a list of vectors in V.*

(a) $\mathcal{L}$ is called $\mathbb{K}$-linearly independent *if*

$$a_1v_1 + av_2 + \dots av_n = 0_V$$

for some $a_1, a_2, \dots, a_n \in \mathbb{K}$ implies $a_1 = a_2 = \dots = a_n = 0_{\mathbb{K}}$.

(b) Let $(a_1, a_2 \dots, a_n) \in \mathbb{K}^n$. Then $a_1v_1 + a_2v_2 + \dots + a_nv_n$ is called a $\mathbb{K}$-linear combination *of $\mathcal{L}$.*

$$\mathrm{Span}_{\mathbb{K}}(\mathcal{L}) = \{a_1v_1 + a_2v_2 + \dots a_nv_n \mid (a_1, \dots, a_n) \in \mathbb{K}^n\}$$

is called the $\mathbb{K}$-span *of $\mathcal{L}$. So $\mathrm{Span}_{\mathbb{K}}(\mathcal{L})$ consists of all the $\mathbb{K}$-linear combination of $\mathcal{L}$. We consider 0_V to be a linear combination of the empty list $()$ and so $\mathrm{Span}_{\mathbb{K}}\big(()\big) = \{0_V\}$.*

(c) We say that $\mathcal{L}$ spans *V, if $V = \mathrm{Span}_{\mathbb{K}}(\mathcal{L})$, that is if every vector in V is a linear combination of $\mathcal{L}$.*

(d) We say that $\mathcal{L}$ is a basis *of V if $\mathcal{L}$ is linearly independent and spans V.*

(e) We say that $\mathcal{L}$ is a linearly dependent *if it's not linearly independent, that is, if there exist $k_1, \dots, k_n \in \mathbb{K}$, not all zero such that*

$$k_1v_1 + kv_2 + \dots kv_n = 0_V.$$

Example 3.1.4. *(1) Put $e_i = (0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}) \in \mathbb{K}^n$ where the $1_{\mathbb{K}}$ is in the i-position. Then $(e_1, e_2, \dots, e_n)$ is a basis for $\mathbb{K}^n$, called the* standard basis *of $\mathbb{K}^n$.*

(2) $(1_{\mathbb{K}}, x, x^2, \dots x^n)$ is a basis for $\mathbb{K}_n[x]$, where $\mathbb{K}_n[x]$ is set of all polynomials with coefficients in $\mathbb{K}$ and degree at most n.

(3) The empty list $()$ is basis for $\mathbb{Z}_1$.

Lemma 3.1.5. *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $\mathcal{L} = (v_1, \dots, v_n)$ a list of vectors in V. Then $\mathcal{L}$ is a basis for V if and only if for each $v \in V$ there exists uniquely determined $k_1, \dots, k_n \in \mathbb{K}$ with*

$$v = \sum_{i=1}^{m} k_iv_i.$$

Proof. $\Longrightarrow$ Suppose that $\mathcal{L}$ is a basis. Then $\mathcal{L}$ spans v and so for each $v \in V$ there exist $k_1, \dots, k_n$ with

$$v = \sum_{i=1}^{m} k_iv_i.$$

Suppose that also $l_1, \dots, l_n \in \mathbb{K}$ with

$$v = \sum_{i=1}^{m} l_iv_i.$$

Then

$$\sum_{i=1}^{m}(k_i - l_i)v_i = \sum_{i=1}^{m} k_i v_i - \sum_{i=1}^{m} l_i v_i = 0_V.$$

Since $\mathcal{L}$ is linearly independent we conclude that $k_i - l_i = 0_{\mathbb{K}}$ and so $k_i = l_i$ for all $1 \leq i \leq n$. So the k_i's are unique.

$\Longleftarrow$: Suppose each v in V is a unique linear combination of $\mathcal{L}$. Then clearly $\mathcal{L}$ spans V. Let $k_1, \ldots, k_n \in \mathbb{K}$ with

$$\sum_{i=1}^{m} k_i v_i = 0_V$$

Since also

$$\sum_{i=1}^{m} 0_{\mathbb{K}} v_i = 0_V$$

the uniqueness assumption gives $k_1 = k_2 = \ldots = k_n = 0_{\mathbb{K}}$. Hence $\mathcal{L}$ is linearly independent and thus a basis for V. □

Lemma 3.1.6. *Let $\mathbb{K}$ be field and V a $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \ldots, v_n)$ be a list of vectors in V. Suppose the exists $1 \leq i \leq n$ such that v_i is linear combination of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. Then $\mathcal{L}$ is linearly dependent.*

Proof. By assumption,

$$v_i = k_1 v_1 + \ldots + k_{i-1} v_{i-1} + k_{i+1} v_{i+1} + \ldots + k_n v_n$$

for some $k_j \in \mathbb{K}$. Thus

$$k_1 v_1 + \ldots + k_{i-1} v_{i-1} + (-1_{\mathbb{K}}) v_i + k_{i+1} v_{i+1} + \ldots + k_n v_n = 0_V$$

and $\mathcal{L}$ is linearly dependent. □

Lemma 3.1.7. *Let $\mathbb{K}$ be field, V an $\mathbb{K}$-space and $\mathcal{L} = (v_1, v_2, \ldots v_n)$ a finite list of vectors in V. Then the following three statements are equivalent:*

(a) $\mathcal{L}$ is basis for V.

(b) $\mathcal{L}$ is a minimal spanning list, that is $\mathcal{L}$ spans V but for all $1 \leq i \leq n$,

$$(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$$

does not span V.

(c) $\mathcal{L}$ is maximal linearly independent list, that is $\mathcal{L}$ is linearly independent, but for all $v \in V$, $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent.

Proof. (a) $\Longrightarrow$ (b): Since $\mathcal{L}$ is basis, it spans V. Since $\mathcal{L}$ is linearly independent 3.1.6 implies that v_i is not in the span of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ and so $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ does not span V.

(a) $\Longrightarrow$ (c): Let $v \in V$. Since $\mathcal{L}$ spans V, v is a linear combination of $\mathcal{L}$ and so by 3.1.6 $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent.

(b) $\Longrightarrow$ (a): By assumption, $\mathcal{L}$ spans V so we only need to show that $\mathcal{L}$ is linearly independent. Suppose not. Then $\sum_{i=1}^n k_i v_i = 0_V$ for some $k_1, k_2, \ldots, k_n \in \mathbb{K}$, not all $0_{\mathbb{K}}$. Relabeling we may assume $k_1 \neq 0_{\mathbb{K}}$. Thus

$$v_1 = -k_1^{-1}(\sum_{i=2}^{n} k_i v_i).$$

Let $v \in V$. Then $v = \sum_{i=1}^n a_i v_i$ for some $a_i \in \mathbb{K}$ and so

$$v = a_1 \left(-k_1^{-1}(\sum_{i=2}^{n} a_i v_i) \right) + \sum_{i=2}^{n} a_i v_i = \sum_{i=2}^{n} (a_i - k_1^{-1} a_i) v_i.$$

Thus $(v_2, \ldots, v_n)$ spans V, contrary to the assumptions.

(c) $\Longrightarrow$ (a): By assumption $\mathcal{L}$ is linear independent, so we only need to show that $\mathcal{L}$ spans V. Let $v \in V$. By assumption $(v_1, \ldots, v_n, v)$ is linearly dependent and so

$$\left(\sum_{i=1}^{n} a_i v_i \right) + av = 0_V$$

for some $a_1, a_2, \ldots, a_n, a$ in $\mathbb{K}$ not all $0_{\mathbb{K}}$. If $a = 0_{\mathbb{K}}$, then since $\mathcal{L}$ is linearly independent, $a_i = 0_{\mathbb{K}}$ for all $1 \leq i \leq n$, contrary to the assumption. Thus $a \neq 0$ and

$$v = \sum_{i=1}^{n} (-a^{-1} a_i) v_i.$$

So $\mathcal{L}$ spans V. $\square$

Definition 3.1.8. *Let* $\mathbb{K}$ *be a field and* V *and* W $\mathbb{K}$*-spaces. A* $\mathbb{K}$-linear map from V to W is function

$$f : V \to W$$

such that

(a) $f(u+v) = f(u) + f(v)$ for all $u, v \in W$

(b) $f(kv) = kf(v)$ for all $k \in \mathbb{K}$ and $v \in V$.

A $\mathbb{K}$-linear map is called a $\mathbb{K}$-*isomorphism* if it's 1-1 and onto.

We say that V and W are $\mathbb{K}$-isomorphic and write $V \cong_{\mathbb{K}} W$ if there exists a $\mathbb{K}$-isomorphism from V to W.

Example 3.1.9.

(1) The map $\mathbb{K}^2 \to \mathbb{K}, (a, b) \to a$ is $\mathbb{K}$-linear.

(2) The map $\mathbb{K}^3 \to \mathbb{K}^2$, $(a, b, c) \to (a + 2b, b - c)$ is $\mathbb{K}$-linear.

(3) We claim that the map $f : \mathbb{K} \to \mathbb{K}, k \to k^2$ is $\mathbb{K}$-linear if and only if $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$.

Indeed, if $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$, then $k = k^2$ for all $k \in \mathbb{K}$ and so f is $\mathbb{K}$-linear.

Conversely, suppose f is $\mathbb{K}$-linear. Then for all $k \in \mathbb{K}$,

$$k^2 = f(k) = f(k \cdot 1_{\mathbb{K}}) = kf(1_{\mathbb{K}}) = k1_{\mathbb{K}}^2 = k$$

So $0_{\mathbb{K}} = k^2 - k = k(k - 1_{\mathbb{K}})$. Since $\mathbb{K}$ is a field and hence an integral domain we conclude that $k = 0_{\mathbb{K}}$ or $k = 1_{\mathbb{K}}$. Hence $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\kappa}\}$.

(4) For $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{K}[x]$ define

$$f' = \sum_{i=1}^{n} i f_i x^{i-1}.$$

Then

$$D : \mathbb{K}[x] \to \mathbb{K}[x], f \to f'$$

is a $\mathbb{K}$-linear map.

Lemma 3.1.10. *Let $\mathbb{K}$ be a field and V and W be $\mathbb{K}$-spaces. Suppose that $(v_1, v_2, \ldots, v_n)$ is basis of V and let $w_1, w_2, \ldots w_n \in W$. Then*

(a) There exists a unique $\mathbb{K}$-linear map $f : V \to W$ with $f(v_i) = w_i$ for each $1 \leq i \leq n$.

(b) $f(\sum_{i=1}^{n} k_i v_i) = \sum_{i=1}^{n} k_i w_i$. for all $k_1, \ldots, k_n \in \mathbb{K}$.

(c) f is 1-1 if and only if $(w_1, w_2, \ldots, w_n)$ is linearly independent.

(d) f is onto if and only if $(w_1, w_2, \ldots, w_n)$ spans W.

(e) f is an isomorphism if and only if $(w_1, w_2, \ldots, w_n)$ is a basis for W.

Proof. (a) and (b): If $f : V \to W$ is $\mathbb{K}$-linear with $f(v_i) = w_i$, then

$$f\left(\sum_{i=1}^{n} a_i v_i\right) = \sum_{i=1}^{n} a_i f(v_i) = \sum_{i=1}^{n} a_i w_i. \tag{1}$$

So (b) holds. Moreover, since $(v_1, \ldots v_n)$ spans V, each v in V is of the form $\sum_{i=1} a_i v_i$ and so by (1), $f(v)$ is uniquely determined. So f is unique.

It remains to show the existence of f. Since $(v_1, \ldots, v_n)$ is a basis for V, any $v \in V$ can by uniquely written as $v = \sum_{i=1} a_i v_i$. So we obtain a well-defined function

$$f: \quad V \to W, \quad \sum_{i=1}^{n} a_i v_i \to \sum_{i=1}^{n} a_i w_i.$$

It is now readily verified that f is $\mathbb{K}$-linear and $f(v_i) = w_i$. So f exists.

(c) From (b)

$$\ker f = \{v \in V \mid f(v) = 0_W\} = \left\{ \sum_{i=1}^{n} k_i v_i \,\middle|\, \sum_{i=1}^{n} k_i w_i = 0_W \right\}. \tag{2}$$

Hence

$$\begin{array}{clcl}
 & f \text{ is 1-1} & & \\
\iff & \ker f = \{0_V\} & - & 2.2.22 \\
\iff & \{\sum_{i=1}^{n} k_i v_i \mid \sum_{i=1}^{n} k_i w_i = 0_W\} = \{0_V\} & - & (2) \\
\iff & \{(k_1, k_2, \ldots, k_n) \in \mathbb{K}^n \mid \sum_{i=1}^{n} k_i w_i = 0_W\} = \{(0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}})\} & - & (v_1, \ldots, v_n) \text{ is linearly indep.} \\
\iff & (w_1, \ldots, w_n) \text{ is linearly indep.} & - & \text{definition of linearly indep.}
\end{array}$$

So (c) holds.

(d)

$$\operatorname{Im} f = \{f(v) \mid v \in V\} = \left\{ \sum_{i=1}^{n} a_i w_i \,\middle|\, a_1, \ldots a_n \in \mathbb{K} \right\} = \operatorname{Span}(w_1, w_2, \ldots, w_n).$$

f is onto if and only if $\operatorname{Im} f = W$ and so if and only if $(w_1, \ldots, w_n)$ spans W.

(e) follows from (c) and (d). □

Corollary 3.1.11. *Let $\mathbb{K}$ be a field and W a $\mathbb{K}$-space with basis $(w_1, w_2 \ldots, w_n)$. Then the map*

$$f : \mathbb{K}^n \to W, (a_1, \ldots a_n) \to \sum_{i=1}^{n} a_i w_i$$

is a $\mathbb{K}$-isomorphism. In particular,

$$W \cong_{\mathbb{K}} \mathbb{K}^n.$$

Proof. By Example 3.1.4(1), $(e_1, e_2, \ldots, e_n)$ is basis for $\mathbb{K}^n$. Also $f(e_i) = w_i$ and so by 3.1.10(e), f is an isomorphism. □

Definition 3.1.12. *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $W \subseteq V$. Then W is called a* $\mathbb{K}$-subspace *of V provided that* *(i)* $0_V \in W$.

(ii) $v + w \in W$ *for all* $v, w \in W$.

(iii) $kw \in W$ *for all* $k \in \mathbb{K}$, $w \in W$.

Proposition 3.1.13 (Subspace Proposition)**.** *Let* $\mathbb{K}$ *be a field,* V *a* $\mathbb{K}$*-space and* W *an* $\mathbb{K}$*-subspace of* V.

(a) Let $v \in V$ *and* $k \in \mathbb{K}$. *Then* $0_{\mathbb{K}} v = v$, $(-1_{\mathbb{K}})v = -v$ *and* $k 0_V = 0_V$.

(b) W *is a subgroup of* V *with respect to addition.*

(c) W *together with the restriction of the addition and scalar multiplication to* W *is a well-defined* $\mathbb{K}$*-space.*

Proof. (a) I will just write 1 for $1_{\mathbb{K}}$ and 0 for $0_{\mathbb{K}}$. Then

$$0 \diamond v + 0_V = 0 \diamond v = (0 + 0) \diamond v = (0 \diamond v) + (0 \diamond v).$$

So by the Cancellation Law 1.4.3, $0 \diamond v = 0_V$.

Hence

$$0_V = 0 \diamond v = (1 + (-1)) \diamond v = (1 \diamond v) + (-1) \diamond v = v + (-1) \diamond v.$$

So by 1.4.4(c), $(-1) \diamond v = -v$.

$$0_V + k \diamond 0_V = k \diamond 0_V = k \diamond (0_V + 0_V) = k \diamond 0_V + k \diamond 0_V$$

and so by the Cancellation Law 1.4.3, $k \diamond 0_V = 0_V$.

(b) By definition of a $\mathbb{K}$-subspace, W is closed under addition and $0_V \in W$. Let $w \in W$. Since W is closed under scalar multiplication, $(-1) \diamond v \in W$. So by (a), $-v \in W$. Hence W is closed under additive inverses. So by the Subgroup Proposition 1.5.3, W is a subgroup of V with respect to addition.

(c) Using (b) this is readily verified and the details are left to the reader. □

Proposition 3.1.14 (Quotient Space Proposition)**.** *Let* $\mathbb{K}$ *be field,* V *a* $\mathbb{K}$*-space and* W *a* $\mathbb{K}$*-subspace of* V.

(a) $V/W := \{v + W \mid v \in V\}$ *together with the addition*

$$+_{V/W} : \quad V/W \times V/W \to V/W, (u + V, v + W) \to (u + v) + W$$

and scalar multiplication

$$\diamond_{V/W} : \quad \mathbb{K} \times V/W \to V/W, (k, v + W) \to kv + W$$

is a well-defined vector space.

(b) The map $\phi : V \to V/W, v + W$ is an onto and $\mathbb{K}$-linear. Moreover, $\ker\phi = W$.

Proof. (a) By Theorem 1.8.10 $(V/W, +_{V/W})$ is a well defined group. We have

$$(u + W) + (v + W) = (u + v) + W = (v + u) + W = (v + W) + (v + W)$$

and so $(V/W, +_{V/W})$ is an abelian group. Thus Axiom (i) of a vector space holds.

Let $k \in V$ and $u, v \in V$ with $u + W = v + W$. Then $u - v \in W$ and since W is a subspace, $k(u-v) \in W$. Thus $ku-kv \in W$ and $ku+W = kv+W$. So $\diamond_{V/W}$ is well-defined and Axiom (ii) of a vector space holds. The remaining four axioms (iii)-(vi) are readily verified.

(b) By 1.9.3 ϕ is an homomorphism of abelian groups and $\ker\phi = W$. Let $k \in \mathbb{K}$ and $v \in V$. Then

$$\phi(kv) = kv + W = k(v + W),$$

and so ϕ is a $\mathbb{K}$-linear map. $\square$

Lemma 3.1.15. *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space, W a subspace of V. Suppose that $(w_1, \ldots, w_l)$ be a basis for W and let $(v_1, \ldots, v_l)$ be a list of vectors in V. Then the following are equivalent*

(a) $(w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_l)$ is a basis for V.

(b) $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a basis for V/W.

Proof. Put $\mathcal{B} = (w_1, w_2, \ldots, w_k, v_1, v_2, \ldots v_l)$.

(a) $\Longrightarrow$ (b): Suppose that $\mathcal{B}$ is a basis for V. Let $T \in V/W$. Then $T = v + W$ for some $v \in V$. Since $\mathcal{B}$ is spanning list for V there exist $a_1, \ldots, a_k$, $b_1, \ldots b_k \in \mathbb{K}$ with

$$v = \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j.$$

Since $\sum_{i=1}^{k} a_i w_i \in W$ we conclude that

$$T = v + W = \left(\sum_{i=1}^{k} b_i v_i\right) + W = \sum_{i=1}^{k} b_i(v_i + W).$$

Therefore $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a spanning set for V/W.

Now suppose that $b_1, \ldots b_l \in \mathbb{K}$ with

$$\sum_{j=1}^{l} b_i(v_i + W) = 0_{V/W}.$$

Then $(\sum_{j=1}^{l} b_i v_i) + W = W$ and $\sum_{j=1}^{l} b_i v_i \in W$. Since $(w_1, w_2, \ldots, w_k)$ spans W there exist $a_1, a_2 \ldots, a_k \in \mathbb{K}$ with

$$\sum_{j=1}^{l} b_i v_i = \sum_{i=1}^{k} a_i w_i,$$

and so

$$\sum_{i=1}^{k} (-a_i) w_i + \sum_{j=1}^{l} b_j v_j = 0_V.$$

Since $\mathcal{B}$ is linearly independent, we conclude that $-a_1 = -a_2 = \ldots = -a_k = b_1 = b_2 = \ldots = b_l = 0_{\mathbb{K}}$. Thus $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is linearly independent and so a basis for V/W.

(b) $\Longrightarrow$ (a): Suppose $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is a basis for W. Let $v \in V$. Then $v + W = \sum_{j=1}^{l} b_i(v_i + W)$ for some $b_1, \ldots b_l \in \mathbb{K}$. Thus

$$v - \sum_{i=1}^{l} b_i v_i \in W,$$

and so

$$v - \sum_{i=1}^{l} b_i v_i = \sum_{i=1}^{k} a_i w_i$$

for some $a_1, \ldots, a_k \in \mathbb{K}$. Thus

$$v = \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j,$$

and $\mathcal{B}$ is a spanning list.

Now let $a_1, \ldots, a_k$, $b_1, \ldots b_k \in \mathbb{K}$ with

$$(*) \qquad \sum_{i=1}^{k} a_i w_i + \sum_{j=1}^{l} b_j v_j = 0_V.$$

Since $\sum_{i=1}^{k} a_i w_i \in W$, this implies

$$\sum_{j=1}^{l} b_j (v_j + W) = 0_{V/W}.$$

Since $(v_1 + W, v_2 + W, \ldots, v_l + W)$ is linearly independent, $b_1 = b_2 = \ldots = b_l = 0$. Thus by (*)

$$\sum_{i=1}^{k} a_i w_i = 0_V,$$

and since $(w_1, \ldots, w_k)$ is linearly independent, $a_1 = \ldots = a_k = 0_{\mathbb{K}}$.

Hence $\mathcal{B}$ is linearly independent and so a basis. $\square$

Lemma 3.1.16. *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space and $(v_1, \ldots, v_n)$ and $(w_1, \ldots w_m)$ be bases for V. Then $n = m$.*

Proof. The proof is by induction on $\min(n, m)$. If $n = 0$ or $m = 0$, then $V = \{0_V\}$. So V contains no non-zero vectors and $n = m = 0$.

Suppose now that $1 \leq n \leq m$. Put $W = \mathrm{Span}(w_1)$. Clearly $(v_1 + W, \ldots, v_n + W)$ is a spanning list for V/W. Relabeling the $v_i's$ we may assume that $(v_1 + W, \ldots, v_k + W)$ is a minimal spanning sublist of $(v_1 + W, \ldots, v_n + W)$. So by 3.1.7(a), $(v_1 + W, \ldots, v_k + W)$ is a basis for V/W.

By 3.1.7(b), $(w_1, v_1, \ldots, v_n)$ is linearly dependent and so not a basis for V. w_1 is basis for W and so by 3.1.15 $(v_1 + W, \ldots, v_n + W)$ is not basis for V/W. Hence $k \neq n$ and so $k < n$. So by induction any basis for V/W has size k. Since w_1 is a basis for W and $(w_1, \ldots, w_n)$ is a basis for V, 3.1.15 implies that $(w_2 + W, \ldots, w_m + W)$ is a basis for V/W. Hence $k = m - 1$ and so $m = k + 1 \leq n \leq m$. Thus $n = m$. $\square$

Definition 3.1.17. *A vector space V over the field $\mathbb{K}$ is called* finite dimensional *if V has a finite basis $(v_1, \ldots, v_n)$. n is called the* dimension *of $\mathbb{K}$ and is denoted by $\dim_{\mathbb{K}} V$. (Note that this is well-defined by 3.1.16).*

Lemma 3.1.18. *Let $\mathbb{K}$ be a field and V an $\mathbb{K}$-space with a finite spanning list $\mathcal{L} = (v_1, v_2, \ldots, v_n)$. Then some sublist of $\mathcal{L}$ is a basis for V. In particular, V is finite dimensional and $\dim_{\mathbb{K}} V \leq n$.*

Proof. Let $\mathcal{B}$ be spanning sublist of $\mathcal{L}$ of minimal length. Then by 3.1.7(b) $\mathcal{B}$ is basis for V. $\square$

The next lemma is the analogue of Lagrange's Theorem for vector spaces:

Theorem 3.1.19 (Dimension Formula)**.** *Let V be a vector space over the field $\mathbb{K}$. Let W be an $\mathbb{K}$-subspace of V. Then V is finite dimensional if and only if both W and V/W are finite dimensional. Moreover, if this is the case, then*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

Proof. Suppose first that V and V/W are finite dimensional. Let $(w_1, w_2 \ldots w_k)$ be basis for W and $(v_1 + W, \ldots v_l + W)$ a basis for V/W.

Then by 3.1.15 $(w_1, \ldots, w_l, v_1, \ldots, v_l)$ is basis for V. Thus

$$(*) \qquad V \text{is finite dimensional and } \dim_{\mathbb{K}} V = k + l = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

Suppose next that V is finite dimensional and let $(z_1, \ldots, z_n)$ be a basis for V. Then $(z_1 + W, z_2 + W, \ldots, z_n + W)$ is a spanning list for V/W. So by 3.1.18

(**) $$V/W \text{ is finite dimensional.}$$

It remains to show that W is finite dimensional. This will be done by induction on $\dim_{\mathbb{K}} V$. If $\dim_{\mathbb{K}} V = 0$, then $W = \{0_V\}$ and so finite dimensional. Inductively assume that all subspaces of vector spaces of dimension $n-1$ are finite dimensional. We may assume that $W \neq \{0_V\}$ and so there exists $0_V \neq w \in W$. Put $Z = \mathrm{Span}(w)$. Then $\dim_{\mathbb{K}} Z = 1$ and by (**) (applied to Z in place of W) V/Z is finite dimensional. Thus by (*),applied to Z in place of W, $\dim V/Z = \dim V - 1$. Since W/Z is a subspace of V/Z, we conclude from the induction assumption that W/Z is finite dimensional. Since also Z is finite dimensional we conclude from (*) (applied with W and Z in place of V and W) that W is finite dimensional. □

Corollary 3.1.20. *Let V be a finite dimensional vector space over the field $\mathbb{K}$ and $\mathcal{L}$ a linearly independent list of vectors in V. Then $\mathcal{L}$ is contained in a basis of V and so*

$$|\mathcal{L}| \leq \dim_{\mathbb{K}} V.$$

Proof. Let $W = \mathrm{Span}(\mathcal{L})$. Then $\mathcal{L}$ is a basis for W. By 3.1.19 V/W is finite dimensional and so has a basis $(v_1, v_2, \ldots v_l)$. Hence by 3.1.15 $(w_1, \ldots, w_k, v_1, \ldots v_l)$ is a basis for V, where $(w_1, \ldots w_k) = \mathcal{L}$. □

3.2 Simple Field Extensions

Definition 3.2.1. *Let $\mathbb{K}$ be a field and $\mathbb{F}$ a subset of $\mathbb{K}$. $\mathbb{F}$ is a called a* subfield *of $\mathbb{K}$ provided that*

(i) $a + b \in \mathbb{F}$ *for all* $a, b \in \mathbb{F}$.

(ii) $0_{\mathbb{K}} \in \mathbb{F}$.

(iii) $-a \in \mathbb{F}$ *for all* $a \in \mathbb{F}$.

(iv) $ab \in \mathbb{F}$ *for all* $a, b \in \mathbb{F}$.

(v) $1_{\mathbb{K}} \in \mathbb{F}$.

(vi) $a^{-1} \in \mathbb{F}$ *for all* $a \in \mathbb{F}$ *with* $a \neq 0_{\mathbb{K}}$.

If $\mathbb{F}$ is a subfield of $\mathbb{K}$ we also say that $\mathbb{K}$ is an extension field *of $\mathbb{F}$ and that $\mathbb{K} : \mathbb{F}$ is a field extension.*

Note that (i), (ii) and (iii) just say that $\mathbb{F}$ is subgroup of $\mathbb{K}$ with respect to addition and (iv),(v),(vi) say that $\mathbb{F} \setminus \{0_{\mathbb{K}}\}$ is a subgroup of $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$ with respect to multiplication.

Example 3.2.2.

$\mathbb{R} : \mathbb{Q}$ and $\mathbb{C} : \mathbb{R}$ are field extensions.

Lemma 3.2.3. *Let $\mathbb{K} : \mathbb{F}$ be a field extension. Then $\mathbb{K}$ is vector space over $\mathbb{F}$, where the scalar multiplication is given by*

$$\mathbb{F} \times \mathbb{K} \to \mathbb{K}, (f, k) \to fk$$

Proof. Using the axioms of a field it is easy to verify the axioms of a vector space. □

Definition 3.2.4. *A field extension $\mathbb{K} : \mathbb{F}$ is called* finite *if $\mathbb{K}$ is a finite dimensional $\mathbb{F}$-space..* $\dim_{\mathbb{F}} \mathbb{K}$ *is called the* degree *of the extension $\mathbb{K} : \mathbb{F}$.*

Example 3.2.5.

$(1, i)$ is an $\mathbb{R}$-basis for $\mathbb{C}$ and so $\mathbb{C} : \mathbb{R}$ is a finite field extension of degree 2. $\mathbb{R} : \mathbb{Q}$ is not finite. Indeed, by 3.1.11 every finite dimensional vector space over $\mathbb{Q}$ is isomorphic to $\mathbb{Q}^n$ for some $n \in \mathbb{N}$ and so by A.3.9 is countable. Since by A.3.8, $\mathbb{R}$ is not countable, $\mathbb{R}$ is not finite dimensional over $\mathbb{Q}$.

Lemma 3.2.6. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and V a $\mathbb{K}$-space. Then with respect to the restriction of the scalar multiplication to $\mathbb{F}$, V is an $\mathbb{F}$-space. If V is finite dimensional over $\mathbb{K}$ and $\mathbb{K} : \mathbb{F}$ is finite, then V is finite dimensional over $\mathbb{F}$ and*

$$\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} V.$$

Proof. It is readily verified that V is indeed on $\mathbb{F}$-space. Suppose now that V is finite dimensional over $\mathbb{K}$ and that $\mathbb{K} : \mathbb{F}$ is finite. Then there exist a $\mathbb{K}$-basis $(v_1, \ldots, v_n)$ for V and an $\mathbb{F}$-basis $(k_1, \ldots, k_m)$ for $\mathbb{K}$. We will show that

$$\mathcal{B} := (k_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq n)$$

is an $\mathbb{F}$-basis for V.

To show that $\mathcal{B}$ spans V over $\mathbb{F}$, let $v \in V$. Then since $(v_1, \ldots, v_n)$ spans V over $\mathbb{K}$ there exists $l_1, \ldots, l_n \in \mathbb{K}$ with

$$v = \sum_{j=1}^{n} l_j v_j. \tag{1}$$

Let $1 \leq j \leq n$. Since $(k_1, \ldots, k_m)$ spans $\mathbb{K}$ over $\mathbb{F}$ there exists $a_{1j}, \ldots a_{mj} \in \mathbb{F}$ with

$$l_i = \sum_{i=1}^{m} a_{ij} k_i. \tag{2}$$

Substituting (2) into (1) gives

$$v = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} k_i \right) v_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} k_i v_j.$$

Thus $\mathcal{B}$ spans V.

To show that $\mathcal{B}$ is linearly independent over $\mathbb{F}$, let $a_{ij} \in \mathbb{F}$ for $1 \leq i \leq m$ and $i \leq j \leq n$ with

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} k_i v_j = 0_V.$$

Then also

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} k_i \right) v_j = 0_V.$$

Since $\sum_{i=1}^{m} a_{ij} k_i \in \mathbb{K}$ and $(v_1, \ldots, v_n)$ is linearly independent over $\mathbb{K}$ we conclude that for all $1 \leq j \leq n$:

$$\sum_{i=1}^{m} a_{ij} k_i = 0_{\mathbb{K}}.$$

Since $(k_1, k_2, \ldots, k_m)$ is linearly independent over $\mathbb{F}$ this implies $a_{ij} = 0_{\mathbb{F}}$ for all $1 \leq i \leq m$ and all $1 \leq j \leq m$. Thus $\mathcal{B}$ is a basis for V over $\mathbb{F}$, V is finite dimensional over $\mathbb{F}$ and

$$\dim_{\mathbb{F}} V = mn = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} V.$$

□

Corollary 3.2.7. *Let $\mathbb{E} : \mathbb{K}$ and $\mathbb{K} : \mathbb{F}$ be finite field extensions. Then also $\mathbb{E} : \mathbb{F}$ is a finite field extension and*

$$\dim_{\mathbb{F}} \mathbb{E} = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} \mathbb{E}.$$

Proof. By 3.2.3 $\mathbb{E}$ is a $\mathbb{K}$-space. So the corollary follows from 3.2.6 applied with $V = \mathbb{E}$. □

Before proceeding we recall some definitions from ring theory. Let R be a ring and I a subset of R. Then I is an *ideal* in R if I is an additive subgroup of R and $ri \in I$ and $ir \in I$ for all $r \in R$ and $i \in I$. Let $a \in R$. Then (a) denotes ideal in R generated by R, that the intersection of all ideals of R containing a. If R is a commutative ring with identity, then $(a) = Ra = \{ra \mid r \in R\}$.

Lemma 3.2.8. *Let $\mathbb{F}$ be a field and I a non-zero ideal in $\mathbb{F}[x]$.*

(a) There exists a unique monic polynomial $p \in \mathbb{F}[x]$ with $I = \mathbb{F}[x]p = (p)$.

(b) $F[x]/I$ is an integral domain if and only if p is irreducible and if and only if $F[x]/I$ is field.

Proof. (a) We will first show the existence of p. Since $I \neq \{0_{\mathbb{F}}\}$ there exists $q \in I$ with $q \neq 0_{\mathbb{F}}$. Choose such a q with $\deg q$ minimal. Let $p := \text{lead}(q)^{-1} \cdot q$. Then p is monic, $\deg p = \deg q$ and since I is an ideal $p \in I$. Let $g \in \mathbb{F}[x]$. By the Remainder Theorem [Hung, Theorem 4.4], $g = tp + r$ where $t, r \in \mathbb{F}[x]$ with $\deg r < \deg p$. Since I is an ideal, $tp \in I$ and so $g \in I$ if and only if $g - tp \in I$ and so if and only if $r \in I$. Since $\deg r < \deg p = \deg q$, the minimal choice of $\deg q$ shows that $r \in I$ if and only if $r = 0_{\mathbb{F}}$. So $g \in I$ if and only if $r = 0_{\mathbb{F}}$ and if and only if $q \in (p) = \mathbb{F}[x]p$. Therefore $I = (p)$.

Suppose that also $\tilde{p} \in \mathbb{F}[x]$ is monic with $I = (\tilde{p})$. Then $\tilde{p} \in (\tilde{p}) = (p) = \mathbb{F}[x]p$ and so $p \mid \tilde{p}$. Similarly $p \mid \tilde{p}$. Since p and $\tilde{p}$ are monic, [Hung, Exercise 4.2 4(b)] gives $p = \tilde{p}$. So p is unique.

(b) This is [Hung, Theorem 5.10]. □

Definition 3.2.9. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$.*

(a) $\mathbb{F}[a] = \{f(a) \mid f \in \mathbb{F}[x]\}$.

(b) If there exists a non-zero $f \in F[x]$ with $f(a) = 0_{\mathbb{F}}$ then a is called algebraic *over $\mathbb{F}$. Otherwise a is called transcendental over $\mathbb{F}$.*

Example 3.2.10.

$\sqrt(2)$ is the a root of $x^2 - 2$ and so $\sqrt(2)$ is algebraic over $\mathbb{Q}$.

i is a root of $x^2 + 1$ so i is algebraic over $\mathbb{Q}$

π is not the root of any non-zero polynomial with rational coefficients. So π is transcendental. The proof of this fact is highly non-trivial and beyond the scope of this lecture notes. For a proof see Appendix 1 in [Lang].

Lemma 3.2.11. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$.*

(a) The map $\phi_a : \mathbb{F}[x] \to \mathbb{K}, f \to f(a)$ is a ring homomorphism.

(b) $\operatorname{Im} \phi_a = \mathbb{F}[a]$ *is a subring of* $\mathbb{K}$.

(c) ϕ_a is 1-1 if and only if $\ker \phi_a = \{0_{\mathbb{F}}\}$ *and if and only if a is transcendental.*

Proof. (a) This is readily verified. See for example Theorem $4.13\frac{1}{2}$ in my Lecture notes for MTH 310, Fall 05 [310].

(b) $\operatorname{Im} \phi_a = \{\phi_a(f) \mid f \in \mathbb{F}[x]\} = \{f(a) \mid f \in \mathbb{F}[x]\} = \mathbb{F}[a]$. By Corollary 3.13 in Hungerford [Hung] the image of a homomorphism is a subring and so $\mathbb{F}[a]$ is a subring of $\mathbb{K}$.

(c) By 2.2.22 ϕ_a is 1-1 if and only if $\ker \phi_a = \{0_{\mathbb{F}}\}$. Now

$$\ker \phi_a = \{f \in \mathbb{F}[x] \mid \phi_a(f) = 0_{\mathbb{K}}\} = \{f \in \mathbb{F}[x] \mid f(a) = 0_{\mathbb{K}}\},$$

and so $\ker \phi_a = \{0_{\mathbb{F}}\}$ if and only if there does not exist a non-zero polynomial f with $f(a) = 0_{\mathbb{K}}$, that is if and only if a is transcendental. □

Theorem 3.2.12. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$. Suppose that a is transcendental over $\mathbb{F}$. Then*

(a) $\tilde{\phi}_a : \mathbb{F}[x] \to \mathbb{F}[a], f \to f(a)$ *is an isomorphism of rings.*

(b) For all $n \in \mathbb{N}$, $(1, a, a^2, \dots, a^n)$ is linearly independent over $\mathbb{F}$.

(c) $\mathbb{F}[a]$ is not finite dimensional over $\mathbb{F}$ and $\mathbb{K} : \mathbb{F}$ is not finite.

(d) $a^{-1} \notin \mathbb{F}[a]$ and $\mathbb{F}[a]$ is not a subfield of $\mathbb{K}$.

Proof. (a) Since a is transcendental, $f(a) \neq 0_{\mathbb{F}}$ for all non-zero $f \in \mathbb{F}[x]$. So $\ker \phi_a = \{0_{\mathbb{F}}\}$ and by 2.2.22 ϕ_a is 1-1. So $\mathbb{F}[x] \cong \operatorname{Im} \phi_a$ as a ring. But $\operatorname{Im} \phi_a = \mathbb{F}[a]$ and so $F[x] \cong \mathbb{F}[a]$.

(b) Let $b_0, b_1, \dots, b_n \in \mathbb{F}$ with $\sum_{i=0}^n b_i a^i = 0_{\mathbb{F}}$. Then $f(a) = 0_{\mathbb{F}}$ where $f = \sum_{i=0}^n b_i x^i$. Since a is transcendental $f = 0_{\mathbb{F}}$ and so $b_0 = b_1 = \dots = b_n = 0_{\mathbb{F}}$. Thus $(1_{\mathbb{F}}, a, \dots, a^n)$ is linearly independent over $\mathbb{F}$.

(c) Suppose $\mathbb{F}[a]$ is finite dimensional over $\mathbb{F}$ and put $n = \dim_{\mathbb{F}} \mathbb{F}[a]$. Then by (b) $(1, a, a^2, \dots, a^n)$ is linearly independent over $\mathbb{F}$. This list has length $n + 1$ and so by 3.1.20

$$n + 1 \leq \dim_F \mathbb{F}[a] = n,$$

a contradiction.

So $\mathbb{F}[a]$ is not finite dimensional over $\mathbb{F}$. Suppose $\mathbb{K} : \mathbb{F}$ is finite, then by 3.1.19 also $\mathbb{F}[a]$ is finite dimensional over $\mathbb{F}$, a contradiction.

(d) Suppose $a^{-1} \in \mathbb{F}[x]$. Then $a^{-1} = f(a)$ for some $f \in \mathbb{F}[x]$. Thus $af(a) - 1_{\mathbb{F}} = 0_{|}F$ and so a is root of the non-zero polynomial $xf - 1_{|}F$. But then a is algebraic, a contradiction. □

Theorem 3.2.13. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$. Suppose that a is algebraic over $\mathbb{F}$. Then*

(a) There exists a unique monic polynomial $p_a \in \mathbb{F}[x]$ with $\ker \phi_a = (p_a)$.

(b) $\overline{\phi}_a : \quad \mathbb{F}[x]/(p_a) \to \mathbb{F}[a], \quad f + (p_a) \to f(a)$ *is a well-defined isomorphism of rings.*

(c) p_a is irreducible.

(d) $\mathbb{F}[a]$ is a subfield of $\mathbb{K}$.

(e) Let Put $n = \deg p_a$. Then $(1, a, \dots, a^{n-1})$ is an $\mathbb{F}$-basis for $\mathbb{F}[a]$

(f) $\dim_{\mathbb{F}} \mathbb{F}[a] = \deg p_a$.

(g) Let $g \in \mathbb{F}[x]$. Then $g(a) = 0_{\mathbb{K}}$ if and only if $p_a \mid g$ in $\mathbb{F}[x]$.

Proof. (a) By 3.2.11(c), $\ker \phi_a \neq \{0_{\mathbb{F}}\}$. By 3.2.11(a) is a ring homomorphism and so by Theorem 6.10 in Hungerford [Hung], $\ker \phi_a$ is an ideal in $\mathbb{F}[x]$. Thus by 3.2.8, $\ker \phi_a = (p_a)$ for a unique monic polynomial $p_a \in \mathbb{F}[x]$.

(b): By definition of p_a, $\ker \phi_a = (p_a)$. By 3.2.11(a) ϕ_a is a ring homomorphism and so (b) follows from the First Isomorphism Theorem of Rings, [Hung, Theorem 6.13].

(c) and (d): Since $\mathbb{K}$ is an integral domain, $\mathbb{F}[a]$ is an integral domain. So by (b), $\mathbb{F}[x]/(p_a)$ is an integral domain. Hence by 3.2.8(b), p_a is irreducible and $\mathbb{F}[x]/(p_a)$ is a field. By (b) also $\mathbb{F}[a]$ is a field. So (c) and (d) hold.

(d) Let $T \in \mathbb{F}[x]/(p_a)$. By Corollary 5.5 in Hungerford there exists a unique polynomial $f \in \mathbb{F}[x]$ of degree less than n with $T = f + (p_a)$. Let $f = \sum_{i=0}^{n-1} f_i x^i$ with $f_i \in \mathbb{F}$. Then the f_i are unique in $\mathbb{F}$ with

$$T = \left(\sum_{i=0}^{n-1} f_i x^i\right) + (p_a) = \sum_{i=0}^{n-1} f_i(x^i + (p_a)).$$

Thus by 3.1.5

$$1 + (p_a), x + (p_a), \ldots, x^{n-1} + (p_a)$$

is a basis for $\mathbb{F}[x]/(p_a)$. Since $\overline{\phi}_a\big(x^i + (p_a)\big) = a^i$ we conclude from 3.1.10(e) that

$$(1, a, a^2, \ldots, a^{n-1})$$

is a basis for $\mathbb{F}[a]$.

(f) Follows from (e).

(g) $g(a) = 0_{\mathbb{K}}$ if and only if $\phi_a(a) = 0_{\mathbb{K}}$ if and only if $g \in \ker \phi_a$ if and only if $g \in (p_a)$ and if and only if $p_a \mid g$ in $\mathbb{F}[x]$. □

Definition 3.2.14. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and let $a \in \mathbb{F}$ be algebraic over $\mathbb{F}$. The unique monic polynomial $p_a \in \mathbb{F}[x]$ with $\ker \phi_a = (p_a)$ is called the* minimal polynomial *of a over $\mathbb{F}$.*

Lemma 3.2.15. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Let $p \in \mathbb{F}[x]$. Then $p = p_a$ if and only of p is monic, and irreducible and $p(a) = 0_{\mathbb{F}}$.*

Proof. $\Longleftarrow$: Suppose $p = p_a$. We have $p_a \in (p_a) = \ker \phi_a$ and so $p_a(a) = 0$. By definition p_a is monic and by 3.2.13(c), p_a is irreducible.

$\Longrightarrow$: Suppose p is monic and irreducible and $p(a) = 0$. Then $p \in \ker \phi_a =)p_a)$ and so $p_a \mid p$. Since p_a is not constant (since it has a as a root) and p is irreducible, $p = bp_a$ for some $b \in \mathbb{F}$. Since both p and p_a are monic we get $b = 1$ and so $p = p_a$. □

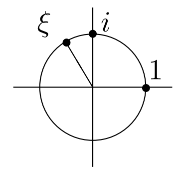
Example 3.2.16.

(1) It is easy to see that $x^3 - 2$ has no root in $\mathbb{Q}$. Since $x^3 - 2$ has degree 3, [Hung, Corollary 4.18] implies that $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. So 3.2.15 implies that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. Hence by 3.2.13(e)

$$\left(1, \sqrt[3]{2}, (\sqrt[3]{2})^2\right) = \left(1, \sqrt[3]{2}), \sqrt[3]{4}\right)$$

is a basis for $\mathbb{Q}[\sqrt[3]{2}]$. Thus

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$



(2) Let $\xi = e^{\frac{2\pi}{3}i} = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Then $\xi^3 = 1$ and ξ is a root of $x^3 - 1$. $x^3 - 1$ is not irreducible, since $(x^3 - 1) = (x-1)(x^2 + x + 1)$. So ξ is a root of $x^2 + x + 1$. $x^2 + x + 1$ does not have a root in $\mathbb{Q}$ and so is irreducible in $\mathbb{Q}[x]$. Hence the minimal polynomial of ξ is $x^2 + x + 1$. Thus

$$\mathbb{Q}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Q}\}.$$

Lemma 3.2.17. *(a) Let $\alpha : R \to S$ and $\beta : S \to T$ be ring isomorphisms. Then*

$$\beta \circ \alpha : R \to T, r \to \beta(\alpha(r))$$

and

$$\alpha^{-1} : S \to R, s \to \alpha^{-1}(s)$$

are ring isomorphism.

(b) Let R and S be rings, I an ideal in R and $\alpha : R \to S$ a ring isomorphism. Put $J = \alpha(I)$. Then

- *(a) J is an ideal in S.*
- *(b) $\beta : I \to J, \quad i \to \alpha(i)$ is a ring isomorphism.*
- *(c) $\gamma : R/I \to S/J, \quad r + I \to \alpha(i) + J$ is a well-defined ring isomorphism.*
- *(d) $\alpha\big((a)\big) = \big(\alpha(a)\big)$ for all $a \in R$. That is α maps to ideal in R generated by a to the ideal in S generated in $\alpha(a)$.*

(c) Let R and S be commutative rings with identities and $\sigma : R \to S$ a ring isomorphism. Then

$$R[x] \to S[x], \quad \sum_{i=1}^{n} f_i x^i \to \sum_{i=1}^{n} \sigma(i) x^i$$

is a ring isomorphism. In the following, we will denote this ring isomorphism also by σ. So if $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}[x]$, then $\sigma(f) = \sum_{i=0}^{n} \sigma(f_i) x^i$.

Proof. Readily verified. $\square$

Corollary 3.2.18. *Let $\sigma : \mathbb{K}_1 \to \mathbb{K}_2$ be a field isomorphism. For $i = 1, 2$ let $\mathbb{E}_i : \mathbb{K}_i$ be a field extension and suppose $a_i \in \mathbb{K}_i$ is algebraic over $\mathbb{K}_i$ with minimal polynomial p_i. Suppose that $\sigma(p_1) = p_2$. Then there exists a field isomorphism*

$$\check{\sigma} : \mathbb{K}_1[a_1] \to \mathbb{K}_2[a_2]$$

with

$$\rho(a_1) = a_2 \text{ and } \rho \mid_{\mathbb{K}_1} = \sigma$$

Proof. By 3.2.17(c) $\sigma : \mathbb{K}_1[x] \to \mathbb{K}_2[x], f \to \sigma(f)$ is a ring isomorphism. By 3.2.17(b:a) $\sigma((p_1)) = (\sigma(p_1)) = (p_2)$ and so by 3.2.17(b:c)

$$\mathbb{K}_1[x]/(p_1) \cong \mathbb{K}_2[x]/(p_2) \tag{1}$$

By 3.2.13(b)

$$\mathbb{K}_1[a_1] \cong \mathbb{K}_1[x]/(p_1) \text{ and } \mathbb{K}_1[a_1] \cong \mathbb{K}_2[x]/(p_2) \tag{2}$$

Composing the three isomorphism in (1) and (2) we obtain the isomorphism

$$\begin{array}{rcccccccc} \rho : & \mathbb{K}_1[x] & \to & \mathbb{K}_1[x]/(p_1) & \to & \mathbb{K}_2[x]/(p_2) & \to & \mathbb{K}_2[x] \\ & f(a_1) & \to & f + (p_1) & \to & \sigma(f) + (p_2) & \to & \sigma(f)(a_2) \end{array}$$

For $f = k \in \mathbb{K}_1$ (a constant polynomial) we have $\sigma(f) = \sigma(k)$, $f(a_1) = k$ and $\sigma(f)(a_2) = \sigma(k)$. So $\rho(k) = \sigma(k)$.

For $f = x$ we have $\sigma(x) = x$, $f(a_1) = a_1$ and $\sigma(x)(a_2) = a_2$. So $\rho(a_1) = a_2$. $\square$

3.3 Splitting Fields

Definition 3.3.1. *A field extension $\mathbb{K} : \mathbb{F}$ is called* algebraic *if each $k \in \mathbb{K}$ is algebraic over $\mathbb{F}$.*

Example 3.3.2.

$\mathbb{C} : \mathbb{R}$ is algebraic but $\mathbb{C} : \mathbb{Q}$ is not.

Lemma 3.3.3. *Any finite field extension is algebraic.*

Proof. Let $\mathbb{K} : \mathbb{F}$ be a finite field extension. Let $a \in \mathbb{K}$. Suppose that a is transcendental over $\mathbb{F}$. Then by 3.2.12(c), $\mathbb{K} : \mathbb{F}$ is not finite, a contradiction. $\square$

Definition 3.3.4. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a_1, a_2 \ldots, a_n \in \mathbb{K}$. Inductively, define $\mathbb{F}[a_1, \alpha_2, \ldots, a_k] := \mathbb{F}[a_1, a_2, \ldots, a_{k-1}][a_k]$.*

Definition 3.3.5. *Let $\mathbb{K} : \mathbb{F}$ be field extensions and $f \in \mathbb{F}[x]$. We say that f* splits *in $\mathbb{K}$ if there exists $a_1 \ldots a_n \in \mathbb{K}$ with*

(i) $f = \mathrm{lead}(f)(x - a_1)(x - a_2)\ldots(x - a_n)$.

We say that $\mathbb{K}$ is a splitting field *for f over $\mathbb{F}$ if f splits in $\mathbb{K}$ and*

(ii) $\mathbb{K} = \mathbb{F}[a_1, a_2, \ldots, a_n]$.

Proposition 3.3.6. *Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$. Then there exists a splitting field $\mathbb{K}$ for f over $\mathbb{F}$. Moreover, $\mathbb{K} : \mathbb{F}$ is finite of degree at most $n!$.*

Proof. The proof is by induction on $\deg f$. If $\deg f \leq 0$, then $f = \mathrm{lead}(f)$ and so $\mathbb{F}$ is a splitting field for f over $\mathbb{F}$. Now suppose that $\deg f = k + 1$ and that the proposition holds for all fields and all polynomials of degree k. Let p be an irreducible divisor of f and put $\mathbb{E} = \mathbb{F}[x]/(p)$. By 3.2.8 $\mathbb{E}$ is a field. We identify $a \in \mathbb{F}$ with $a + (p)$ in $\mathbb{E}$. So $\mathbb{F}$ is a subfield of $\mathbb{E}$. Put $b := x + (p) \in \mathbb{F}$. Then $\mathbb{E} = \mathbb{F}[b]$. Since $p \mid f$, $f \in (p)$ and so $f + (p) = (p) = 0_{\mathbb{E}}$. Hence

$$f(b) = f(x + (p)) = f(x) + (p) = f + (p) = (p) = 0_{\mathbb{E}},$$

and so b is a root of f in $\mathbb{E}$. By the Factor Theorem [Hung, 4.15] $f = (x - b) \cdot g$ for some $g \in \mathbb{E}[x]$ with $\deg g = k$. So by the induction assumption there exists a splitting field $\mathbb{K}$ for g over $\mathbb{E}$ with $\dim_{\mathbb{E}} \mathbb{K} \leq k!$. Hence exist $a_1, \ldots, a_k \in \mathbb{K}$ with

(i) $g = \mathrm{lead}(g)(x - a_1)(x - a_2)\ldots(x - a_k)$;

(ii) $\mathbb{K} = \mathbb{E}[a_1, a_2, \ldots, a_k]$; and

(iii) $\dim_{\mathbb{K}} \mathbb{E} \leq k!$

Since $\mathrm{lead}\, f = \mathrm{lead}\, g$, $f = (x - b) \cdot g$ and $\mathbb{E} = \mathbb{K}[b]$ we conclude that

(iv) $g = \mathrm{lead}(f)(x - b)(x - a_1)(x - a_2)\ldots(x - a_k)$, and

(v) $\mathbb{K} = \mathbb{F}[b][a_1, a_2, \ldots, a_b] = \mathbb{F}[b, a_1, \ldots, a_n]$.

Thus $\mathbb{K}$ is a splitting field for f over $\mathbb{F}$.
Note that $\dim_{\mathbb{K}} \mathbb{E} = \deg p \leq \deg f = k + 1$ and so by 3.2.7 and (iii)

$$\dim_{\mathbb{F}} \mathbb{K} = \dim_{\mathbb{K}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{K} \leq (k + 1) \cdot k! = (k + 1)!$$

So the theorem also holds for polynomials of degree $k + 1$ and, by the Principal of Mathematical Induction, for all polynomials. □

Theorem 3.3.7. *Suppose that*

(i) $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ *is an isomorphism of fields;*

(ii) For $i = 1$ *and* 2, $f_i \in \mathbb{F}[x]$ *and* $\mathbb{K}_i$ *a splitting field for* f_i *over* $\mathbb{F}_i$*; and*

(iii) $\sigma(f_1) = f_2$

Then there exists a field isomorphism

$$\check{\sigma} : \mathbb{K}_1 \to \mathbb{K}_2 \text{ with } \check{\sigma} \mid_{\mathbb{F}_1} = \sigma.$$

Suppose in addition that

(iv) For $i = 1$ *and* 2, p_i *is an irreducible factor of* f_i *in* $\mathbb{F}[x]$ *and* a_i *is a root of* p_i *in* $\mathbb{K}_i$*; and*

(v) $\sigma(p_1) = \sigma(p_2)$.

Then $\check{\sigma}$ *can be chosen such that*

$$\sigma(a_1) = a_2.$$

Proof. The proof is by induction on $\deg f$. If $\deg f \leq 0$, then $\mathbb{K}_1 = \mathbb{F}_1$ and $\mathbb{K}_2 = \mathbb{F}_2$ and so the theorem holds with $\sigma = \check{\sigma}$.

So suppose that $\deg f = k+1$ and that the lemma holds for all fields and all polynomials of degree k. If (iv) and (v) hold let p_i and a_i as there.

Otherwise let p_1 be any irreducible factor of f_1. Put $p_2 = \sigma(p_1)$. By 3.2.17(c), $\sigma : \mathbb{K}_1[x] \to \mathbb{K}_2[x]$ is a ring isomorphism. Thus p_2 is a irreducible factor of $\sigma(f_1) = f_2$. Since f_i splits over $\mathbb{K}$, there exists a root a_i for p_i in $\mathbb{K}_i$.

Put $\mathbb{E}_i = \mathbb{K}_i[a_i]$. By 3.2.18 there exists a field isomorphism $\rho : \mathbb{E}_1 \to \mathbb{E}_2$ with $\rho(a_1) = a_2$ and $\rho \mid_{\mathbb{F}_1} = \sigma$. By the factor theorem $f_i = (x - a_i) \cdot g_i$ for some $g_i \in \mathbb{E}_i[x]$. Since $\rho \mid_{\mathbb{F}_1} = \sigma$ and f_1 has coefficients in $\mathbb{F}_1$, $\rho(f_1) = \sigma(f_1) = f_2$. Thus

$$(x - a_2) \cdot g_2 = f_2 = \rho(f_1) = \rho\big((x - a_1) \cdot g_1\big) = big(x - \rho(a_2)\big) \cdot \rho(g_1) = (x - a_2) \cdot \rho(g_1),$$

and so by the Cancellation Law $g_2 = \rho(g_1)$. Since $\mathbb{K}_i$ is a splitting field for f_i over $\mathbb{K}_i$, $\mathbb{K}_i$ is also a splitting field for g_i over $\mathbb{E}_i$. So by the induction assumption there exists a field isomorphism $\check{\sigma} : \mathbb{K}_1 \to \mathbb{K}_2$ with $\check{\sigma} \mid_{\mathbb{E}_i} = \rho$. We have $\check{\sigma}(a_1) = \rho(a_1) = a_2$ and $\check{\sigma} \mid_{\mathbb{F}_1} = \rho \mid_{\mathbb{F}_1} = \sigma$.

Thus the Theorem holds for polynomials of degree $k + 1$ and so by induction for all polynomials. □

Example 3.3.8.

Note that $x^2+1=(x-i)(x-(-i))$ and $\mathbb{R}[i]=\mathbb{C}$. So $\mathbb{C}$ is a splitting field for x^2+1 over $\mathbb{R}$. We now apply 3.3.7 with

$$\mathbb{F}_1=\mathbb{F}_2=\mathbb{R},\quad \mathbb{K}_1=\mathbb{K}_2=\mathbb{C},\quad \sigma=\mathrm{id}_{\mathbb{R}},\quad f_1=p_1=f_2=p_2=x^2+1,\quad a_1=i,\quad a_2=-i.$$

We conclude that there exists a field isomorphism $\check{\sigma}:\mathbb{C}\to\mathbb{C}$ with

$$\check{\sigma}\mid_{\mathbb{R}}=\sigma=\mathrm{id}_{\mathbb{R}}$$

and

$$\check{\sigma}(i)=\check{\sigma}(a_1)=a_2=-i.$$

Let $a,b\in\mathbb{R}$. Then

$$\check{\sigma}(a+bi)=\check{\sigma}(a)+\check{\sigma}(b)\check{\sigma}(-i)=a+b(-i)=a-bi$$

This shows $\check{\sigma}$ is complex conjugation.

3.4 Separable Extension

Definition 3.4.1. *Let $\mathbb{K}:\mathbb{F}$ be a field extension.*

(a) Let $f\in\mathbb{F}[x]$. If f is irreducible, then f is called separable *over $\mathbb{F}$ provided that f does not have a double root in its splitting field over $\mathbb{F}$. In general, f is called separable over $\mathbb{F}$ provided that all irreducible factors of f in $\mathbb{F}[x]$ are separable over $\mathbb{F}$.*

(b) $a\in\mathbb{K}$ is called separable over $\mathbb{K}$ if a is algebraic over $\mathbb{F}$ and the minimal polynomial of a over $\mathbb{F}$ is separable over $\mathbb{F}$.

(c) $\mathbb{K}:\mathbb{F}$ is called separable over $\mathbb{F}$ if each $a\in\mathbb{K}$ is separable over $\mathbb{F}$.

Example 3.4.2.

Let $\mathbb{E}:\mathbb{Z}_2$ be a field extension and let $t\in\mathbb{E}$ be transcendental over $\mathbb{Z}_2$. Put

$$\mathbb{K}=\mathbb{Z}_2(t)=\{ab^{-1}\mid a,b\in\mathbb{Z}_2[t],b\neq 0_{\mathbb{Z}_2}\}$$

and

$$\mathbb{F}=\mathbb{Z}_2(t^2).$$

By Homework 11#2 $\mathbb{F}$ and $\mathbb{K}$ are subfields of $\mathbb{E}$. It is easy to see that $t\notin\mathbb{F}$. Since $-1_{\mathbb{Z}_2}=1_{\mathbb{Z}_2}$,

$$x^2-t^2=(x-t)(x+t)=(x-t)^2.$$

So t is a double root of $x^2 - t^2$. Since $t \notin \mathbb{F}$, $x^2 - t^2$ has no root in $\mathbb{F}$ and so by [Hung, Corollary 4.18] is irreducible in $\mathbb{F}[x]$. Hence by 3.2.15 $x^2 - t^2$ is the minimal polynomial of t over $\mathbb{F}$. Since t is a double root of $x^2 - t^2$, $x^2 - t^2$ is not separable. So also t is not separable over $\mathbb{F}$ and $\mathbb{K}$ is not separable over $\mathbb{F}$.

Lemma 3.4.3. *Let $\mathbb{K} : \mathbb{E}$ and $\mathbb{E} : \mathbb{F}$ be a field extensions.*

(a) Let $a \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then a is algebraic over $\mathbb{E}$. Moreover, if $p_a^{\mathbb{E}}$ is the minimal polynomial of a over $\mathbb{E}$, and $p_a^{\mathbb{F}}$ is the minimal polynomial of a over $\mathbb{F}$, then $p_a^{\mathbb{E}}$ divides $p_a^{\mathbb{F}}$ in $\mathbb{E}[x]$.

(b) If $f \in \mathbb{F}[x]$ is separable over $\mathbb{F}$, then f is separable over $\mathbb{E}$.

(c) If $a \in \mathbb{K}$ is separable over $\mathbb{F}$, then a is separable over $\mathbb{E}$.

(d) If $\mathbb{K} : \mathbb{F}$ is separable, then also $\mathbb{K} : \mathbb{E}$ and $\mathbb{E} : \mathbb{K}$ are separable.

Proof. (a) Since $p_a^{\mathbb{F}}(a) = 0_{\mathbb{F}}$ and $p_a^{\mathbb{E}} \in \mathbb{F}[x] \subseteq \mathbb{E}[x]$, a is algebraic over $\mathbb{E}$. Moreover,

$$p_a^{\mathbb{F}} \in \ker \phi_a^{\mathbb{E}} = \mathbb{E}[x] p_\alpha^{\mathbb{E}}$$

and so $p_a^{\mathbb{E}}$ divides $p_a^{\mathbb{F}}$ in $\mathbb{E}[x]$.

(b) Let $f \in \mathbb{F}[x]$ be separable over $\mathbb{F}$. Then $f = p_1 p_2 \ldots p_k$ for some irreducible $p_i \in \mathbb{F}[x]$. Moreover, $p_i = q_{i1} q_{i2} \ldots q_{il_i}$ for some irreducible $q_{ij} \in \mathbb{E}[x]$. Since f is separable, p_i has no double roots. Since q_{ij} divides p_i also q_{ij} has no double roots. Hence q_{ij} is separable over $\mathbb{E}$ and so also f is separable over $\mathbb{E}$.

(c) Since a is separable over $\mathbb{E}$, $p_a^{\mathbb{F}}$ has no double roots. By (a) $p_a^{\mathbb{E}}$ divides $p_a^{\mathbb{F}}$ and so also $p_a^{\mathbb{E}}$ has no double roots. Hence a is separable over $\mathbb{E}$.

(d) Let $a \in \mathbb{K}$. Since $\mathbb{K} : \mathbb{F}$ is separable, a is separable over $\mathbb{F}$. So by (c), a is separable over $\mathbb{E}$. Thus $\mathbb{K} : \mathbb{E}$ is separable. Let $a \in \mathbb{E}$. Then $a \in \mathbb{K}$ and so a is separable over $\mathbb{F}$. Hence $\mathbb{E} : \mathbb{F}$ is separable. □

3.5 Galois Theory

Definition 3.5.1. *Let $\mathbb{K} : \mathbb{F}$ be field extension.* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *is the set of all field isomorphism $\alpha : \mathbb{K} \to \mathbb{K}$ with $\alpha \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.*

Lemma 3.5.2. *Let $\mathbb{K} : \mathbb{F}$ be a field extension. Then* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *is a subgroup of* $\mathrm{Sym}(\mathbb{K})$*.*

Proof. Clearly $\mathrm{id}_{\mathbb{K}} \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Let $\alpha, \beta \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then by 3.2.17(a) $\alpha \circ \beta$ is a field isomorphism. If $a \in \mathbb{F}$, then $\alpha(\beta(a)) = \alpha(a) = a$ and so $(\alpha \circ \beta) \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$. So $\alpha \circ \beta \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. By 3.2.17(a) α^{-1} is a field isomorphism. Since $\alpha \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ also $\alpha^{-1} \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ and so $\alpha^{-1} \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. So by the Subgroup Proposition 1.5.3, $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ is a subgroup of $\mathrm{Sym}(\mathbb{K})$. □

Example 3.5.3.

What is $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$?

Let $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ and $a, b \in \mathbb{R}$. Since $\sigma_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$ we have $\sigma(a) = a$ and $\sigma(b) = b$. Thus

$$(*) \qquad \sigma(a + bi) = \sigma(a) = \sigma(b)\sigma(i) = a + b\sigma(i).$$

So we need to determine $\sigma(i)$. Since $i^2 = -1$, we get

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

Thus $\sigma(i) = i$ or $-i$. If $\sigma(i) = i$, then (*) shows that $\sigma = \mathrm{id}_{\mathbb{C}}$ and if $\sigma(i) = -i$, (*) shows that σ is complex conjugation. By Example 3.3.8, complex conjugation is indeed an automorphism of $\mathbb{C}$ and thus

$$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_C, \text{complex conjugation.}\}$$

Definition 3.5.4. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $H \subseteq \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. Then*

$$\mathrm{Fix}_{\mathbb{K}}(H) := \{k \in \mathbb{K} \mid \sigma(k) = k \textit{ for all } \sigma \in H\}.$$

$\mathrm{Fix}_{\mathbb{K}}(H)$ *is called the* fixed-field *of H in $\mathbb{K}$.*

Lemma 3.5.5. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and H a subset of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then $\mathrm{Fix}_{\mathbb{K}}(H)$ is subfield of $\mathbb{K}$ containing $\mathbb{F}$.*

Proof. By definition of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$, $\sigma(a) = a$ for all $a \in \mathbb{F}$, $\sigma \in H$. Thus $\mathbb{F} \subseteq \mathrm{Fix}_{\mathbb{K}}(H)$. In particular, $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathrm{Fix}_{\mathbb{K}}(H)$.

Let $a, b \in \mathrm{Fix}_{\mathbb{K}}(H)$ and $\sigma \in H$. Then

$$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b,$$

and so $a + b \in \mathrm{Fix}_{\mathbb{K}}(H)$.

$$\sigma(-a) = -\sigma(a) = -a,$$

and so $-a \in \mathrm{Fix}_{\mathbb{K}}(H)$.

$$\sigma(ab) = \sigma(a)\sigma(b) = ab,$$

and so $ab \in \mathrm{Fix}_{\mathbb{K}}(H)$. Finally if $a \neq 0_{\mathbb{F}}$, then

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1},$$

and so $a^{-1} \in \mathrm{Fix}_{\mathbb{K}}(H)$.

Hence $\mathrm{Fix}_{\mathbb{K}}(H)$ is a subfield of $\mathbb{K}$. $\square$

Example 3.5.6.

What is $\mathrm{Fix}_{\mathbb{C}}(\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}))$?

By Example 3.5.3, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$, where σ is complex conjugation. Let $a, b \in \mathbb{R}$. Then

$$\mathrm{id}_{\mathbb{C}}(a+bi) = a+bi \text{ and } \sigma(a+bi) = a-bi.$$

So $a+bi$ is fixed by $\mathrm{id}_{\mathbb{C}}$ and σ if and only if $b=0$, that is if and only if $a+bi \in \mathbb{R}$. Thus

$$\mathrm{Fix}_{\mathbb{C}}(\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})) = \mathbb{R}.$$

Proposition 3.5.7. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $0_{\mathbb{F}} \neq f \in \mathbb{F}[x]$.*

(a) Let $a \in \mathbb{K}$ and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then $\sigma(f(a)) = f(\sigma(a))$.

(b) The set of roots of f in $\mathbb{K}$ is invariant under $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. That is if a is a root of f in $\mathbb{K}$ and $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K})$, then $\sigma(a)$ is also a root of f in $\mathbb{K}$.

(c) Let $a \in \mathbb{K}$. Then $\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a) = \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$.

(d) Let a be root of f in $\mathbb{K}$. Then

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) / \mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})\}|.$$

Proof. (a) Let $f = \sum_{i=0}^{n} f_i x^i$. Then

$$\sigma(f(a)) = \sigma\left(\sum_{i=0}^{n} f_i a^i\right) = \sum_{i=0}^{n} \sigma(f_i)\sigma(a)^i = \sum_{i=0}^{n} f_i \sigma(a)^i = f(\sigma(a)).$$

(b) Let a be a root of f in $\mathbb{K}$ then $f(a) = 0_{\mathbb{K}}$ and so by (a)

$$f(\sigma(a)) = \sigma(f(a)) = \sigma(0_{\mathbb{K}}) = 0_{\mathbb{K}}.$$

(c) Put $H = \mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a) = \{\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \mid \sigma(a) = a\}$. Then clearly $\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K}) \subseteq H$. Note that $a \in \mathrm{Fix}_{\mathbb{K}}(H)$ and by 3.5.5 $\mathrm{Fix}_{\mathbb{K}}(H)$ is a subfield of $\mathbb{K}$ containing $\mathbb{F}$. So by Homework 11#2, $\mathbb{F}(a) \subseteq \mathrm{Fix}_{\mathbb{K}}(H)$ and thus $H \subseteq \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$. Therefore $H = \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$.

(d) By 2.1.16,

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) / \mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a)| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})\}|,$$

and so (d) follows from (c). $\square$

Theorem 3.5.8. *Let $\mathbb{F}$ be a field and $\mathbb{K}$ the splitting field of a separable polynomial over $\mathbb{F}$. Then*

$$|\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{K}.$$

Proof. The proof is by induction on $\dim_{\mathbb{F}} \mathbb{K}$. If $\dim_{\mathbb{F}} \mathbb{K} = 1$, then $\mathbb{K} = \mathbb{F}$ and $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K}) = \{\mathrm{id}_{\mathbb{F}}\}$. So the theorem holds in this case. Suppose now that theorem holds for all finite field extensions of degree less than $\dim_{\mathbb{F}} \mathbb{K}$. Let $f \in \mathbb{F}[x]$ be separable polynomial with $\mathbb{K}$ as splitting field and let a be a root of f with $a \notin \mathbb{F}$. Let R be the set of roots of f in $\mathbb{K}$. Since p_a has no double roots, $|R| = \deg p_a$ and so by 3.2.13(f),

$$(1) \qquad |R| = \dim_{\mathbb{F}} \mathbb{F}[a].$$

Put

$$S = \{\sigma(a) \mid \sigma \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})\}.$$

We will show that $S = R$. Let $b \in R$. Then by 3.3.7 applied with $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}, \mathbb{K}_1 = \mathbb{K}_2 = \mathbb{K}$, $\sigma = \mathrm{id}_{\mathbb{F}}$, $f_1 = f_2 = f$, $p_1 = p_2 = p_a$, $a_1 = a$ and $a_2 = b$, there exists a field isomorphism $\check{\sigma} : \mathbb{K} \to \mathbb{K}$ with

$$\check{\sigma} \mid_{\mathbb{F}} = \sigma = \mathrm{id}_{\mathbb{F}} \text{ and } \check{\sigma}(a) = b.$$

Then $\check{\sigma} \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ and so $b = \check{\sigma}(a) \in S$. Hence

$$R \subseteq S.$$

By 3.5.7(b), $\sigma(a)$ is a root of f for each $\sigma \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$. Thus $S \subseteq R$ and

$$(2) \qquad R = S.$$

By 3.5.7(d)

$$|\operatorname{Aut}_{\mathbb{F}}(\mathbb{K}) / \operatorname{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = |\{\sigma(a) \mid \sigma \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})\}| = |S|,$$

and so by (1) and (2)

$$(3) \qquad |\operatorname{Aut}_{\mathbb{F}}(\mathbb{K}) / \operatorname{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{F}[a].$$

Observe that $\mathbb{K}$ is a splitting field for f over $\mathbb{F}[a]$ and that by 3.4.3(b), f is separable over $\mathbb{F}[a]$. Moreover, by 3.2.7

$$\dim_{\mathbb{F}[a]} \mathbb{K} = \frac{\dim_{\mathbb{F}} \mathbb{K}}{\dim_{\mathbb{F}[a]}(\mathbb{K})} < \dim_{\mathbb{F}} \mathbb{K},$$

and so by induction

$$|\operatorname{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = \dim_{\mathbb{F}[a]} \mathbb{K}. \tag{4}$$

Multiplying (3) with (4) gives

$$|\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})/\operatorname{Aut}_{\mathbb{F}[a]}(\mathbb{K})| \cdot |\operatorname{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{F}[a] \cdot \dim_{\mathbb{F}[a]} \mathbb{K}. \tag{5}$$

So by Lagrange's Theorem and Corollary 3.2.7,

$$|\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{K}.$$

□

Example 3.5.9.

By Example 3.2.16 x^3-2 is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ and $\dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt[3]{2}\right] = 3$. The other roots of $x^3 - 2$ are $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$, where $\xi = e^{\frac{2\pi}{3}i}$. Also by Example 3.2.16 ξ is a root of $x^2 + x + 1$. Since $\xi \notin \mathbb{R}$, $\xi \notin \mathbb{Q}\left[\sqrt[2]{2}\right]$. Thus $x^2 + x + 1$ is the minimal polynomial of ξ over $\mathbb{Q}\left[\sqrt[3]{2}\right]$. Put $\mathbb{K} = \mathbb{Q}\left[\sqrt[3]{2}, \xi\right]$. Then $\dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]} \mathbb{K} = 2$ and so

$$\dim_{\mathbb{Q}} \mathbb{K} = \dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt[3]{2}\right] \cdot \dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]} \mathbb{K} = 3 \cdot 3 = 6$$

Note that

$$\mathbb{K} = \mathbb{Q}\left[\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\right],$$

and so $\mathbb{K}$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let $R = \left\{\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\right\}$, the set of roots of $x^3 - 2$. By 3.5.7, R is $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$-invariant and so by 2.2.10(b), $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$ acts on R. The homomorphism associated to this action is

$$\alpha : \operatorname{Aut}_{\mathbb{F}}(\mathbb{K}) \to \operatorname{Sym}(R), \sigma \to \sigma\mid_R .$$

Let $\sigma \in \ker\alpha$. Then $R \subseteq \operatorname{Fix}_{\mathbb{K}}(\sigma)$. Since $\operatorname{Fix}_{\mathbb{K}}(\sigma)$ is a subfield of $\mathbb{K}$ containing $\mathbb{Q}$, this implies $\operatorname{Fix}_{\mathbb{K}}(\sigma) = \mathbb{K}$ and so $\sigma = \ker\alpha$. Thus by 2.2.22 α is 1-1. By 3.5.8 $|\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{Q}} \mathbb{K} = 6$. Since also $|\operatorname{Sym}(R)| = 6$ we conclude that α is a bijection and so

$$\operatorname{Aut}_{\mathbb{F}}(\mathbb{K}) \cong \operatorname{Sym}(R) \cong \operatorname{Sym}(3).$$

Lemma 3.5.10. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and G a finite subgroup of $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ with $\operatorname{Fix}_{\mathbb{K}}(G) = \mathbb{F}$. Then $\dim_{\mathbb{F}} \mathbb{K} \leq |G|$.*

Proof. Put $m = |G|$ and let $G = \{\sigma_1, \sigma_2, \dots, \sigma_m\}$ with $\sigma_1 = \mathrm{id}_{\mathbb{K}}$.

Let $\mathbb{F}$-linear independent list $(k_1, k_2, \dots, k_n)$ in $\mathbb{K}$ and let $C_1, C_2, \dots, C_n$ be the columns of the matrix

$$(\sigma_i(k_j)) = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ \sigma_2(k_1) & \sigma_2(k_2) & \dots & \sigma_2(k_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_m(k_1) & \sigma_m(k_2) & \dots & \sigma_m(k_n) \end{pmatrix}.$$

Claim: $(C_1, C_2, \dots, C_n)$ is linearly independent over $\mathbb{K}$.

Before we prove the Claim we will show that Lemma follows from the Claim. Since $\mathbb{K}^m$ has dimension m over $\mathbb{K}$, 3.1.20 implies that any $\mathbb{K}$-linear independent list in $\mathbb{K}^m$ has length at most m. So if $(C_1, C_2, \dots, C_n)$ is linearly independent, then $n \leq m$ and $\dim_{\mathbb{F}} \mathbb{K} \leq |G|$.

We now proof the Claim via a proof by contradiction. So suppose the Claim is false and under all the $\mathbb{F}$ linear independent list $(k_1, \dots, k_n)$ for which $(C_1, C_2 \dots, C_n)$ is linearly dependent over $\mathbb{K}$ choose one with n as small as possible. Then there exist $l_1, l_2 \dots l_n \in \mathbb{K}$ not all zero with

$$\sum_{j=1}^{n} l_k C_j = \vec{0}. \tag{1}$$

If $l_1 = 0_{\mathbb{K}}$, then $\sum_{j=2} l_j C_j = \vec{0}$ and so also $(k_2, \dots, k_n)$ is a counterexample. This contradicts the minimal choice of n.

Hence $l_1 \neq 0_{\mathbb{K}}$. Note that also $\sum_{j=1} l_1^{-1} l_j C_j = \vec{0}$. So we may assume that $l_1 = 1_{\mathbb{F}}$.

Suppose that $l_j \in \mathbb{F}$ for all $1 \leq j \leq n$. Considering the first coordinates in the equation (1) we conclude

$$\sum_{j=1}^{n} l_j k_j = 0_{\mathbb{F}},$$

a contradiction since $(k_1, \dots, k_n)$ is linearly independent over $\mathbb{F}$. So there exists $1 \leq k \leq n$ with $l_k \notin \mathbb{F}$. Note that $l_1 = 1_{\mathbb{F}} \in \mathbb{F}$ and so $k > 1$. Without loss $k = 2$. So $l_2 \notin \mathbb{F}$. Since $\mathrm{Fix}_{\mathbb{K}}(G) = \mathbb{F}$, $l_2 \notin \mathrm{Fix}_{\mathbb{K}}(G)$ and so there exists $\rho \in G$ with $\rho(l_2) \neq l_2$. Note that (1) is equivalent to the system of equation

$$\sum_{j=1}^{n} l_j \sigma(k_j) = 0_{\mathbb{F}} \text{ for all } \sigma \in G.$$

Applying ρ to each of these equation we conclude

$$\sum_{j=1}^{n} \rho(l_k)(\rho \circ \sigma)(k_j) = 0_{\mathbb{F}} \text{ for all } \sigma \in G.$$

Since $\sigma = \rho \circ (\rho^{-1} \circ \sigma)$ these equations with $\rho^{-1} \circ \sigma$ in place of σ give

$$\sum_{j=1}^{n} \rho(l_j)\sigma(k_j) = 0_{\mathbb{F}} \text{ for all } \sigma \in G,$$

and so

$$(2) \qquad \sum_{j=1}^{n} \rho(l_j) C_j = \vec{0}.$$

Subtracting (1) from (2) gives

$$\sum_{j=1}^{n} (\rho(l_j) - l_j) C_j = \vec{0}.$$

Since $l_1 = 1_{\mathbb{F}} = \rho(1_{\mathbb{F}})$, $\rho(l_1) - l_1 = 0_{\mathbb{F}}$ and so

$$(3) \qquad \sum_{j=2}^{n} (\rho(l_j) - l_j) C_j = \vec{0}.$$

Since $\rho(l_2) \neq l_2$, $\rho(l_2) - l_2 \neq 0_{\mathbb{F}}$. So not all the coefficient in (3) are zero, a contradiction to the minimal choice of n. $\square$

Proposition 3.5.11. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and G a finite subgroup of* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *with* $\mathrm{Fix}_{\mathbb{K}}(G) = \mathbb{F}$. *Let $a \in \mathbb{K}$. Then a is algebraic over $\mathbb{F}$. Let $a_1, a_2, \dots a_n$ be the distinct elements of $Ga = \{\sigma(a) \mid \sigma \in G\}$. Then*

$$p_a = (x - a_1)(x - a_2) \dots (x - a_n).$$

In particular, p_a splits over $\mathbb{K}$ and $\mathbb{K}$ is separable over $\mathbb{F}$.

Proof. Put $q = (x - a_1)(x - a_2) \dots (x - a_n)$. Then $q \in \mathbb{K}[x]$. We will show that $q \in \mathbb{F}[x]$.

Let $\sigma \in G$. Then

$$(1) \qquad \sigma(q) = \sigma\big((x - a_1)(x - a_2) \dots (x - a_n)\big) = \big(x - \sigma(a_1)\big)\big(x - \sigma(a_2)\big) \dots \big(x - \sigma(a_n)\big).$$

By 2.1.11 $\sigma(b) \in Ga$ for all $b \in Ga$. So

$$\{\sigma(a_1)), \sigma(a_2), \dots, \sigma(a_n)\} = \{a_1, \dots, a_n\},$$

and hence

$$\big(x-\sigma(a_1)\big)\big(x-\sigma(a_2)\big)\ldots\big(x-\sigma(a_n)\big)=(x-a_1)(x-a_2)\ldots(x-a_n)=q.$$

Thus by (1)

$$\sigma(q)=q. \tag{2}$$

Let $q=\sum_{i=0}^n k_ix^i$ with $k_i\in\mathbb{K}$. Then

$$\sum_{i=0}^n k_ix^i=q\overset{(2)}{=}\sigma(q)=\sigma\left(\sum_{i=0}^n k_ix^i\right)=\sum_{i=0}^n\sigma(k_i),$$

and so

$$k_i=\sigma(k_i)\text{ for all }0\le i\le n,\sigma\in G.$$

It follows that for all $0\le i\le n$,

$$k_i\in\mathrm{Fix}_{\mathbb{K}}(G)=\mathbb{F}.$$

Hence $q\in\mathbb{F}[x]$.

Since $a=\mathrm{id}_{\mathbb{K}}(a)$ is one of the a_i's we have $q(a)=0_{\mathbb{F}}$. Thus 3.2.13(g) implies that $p_a\mid q$. By 3.5.7 each a_i is a root of p_a and so q divides p_a in $\mathbb{K}[x]$. Since p_a and q both are monic we conclude that $p_a=q$. So

$$p_a=(x-a_1)(x-a_2)\ldots(x-a_n).$$

Since each $a_i\in\mathbb{K}$, p_a splits over $\mathbb{K}$. Since the a_i's are pairwise distinct, p_a is separable. So a is separable over $\mathbb{K}$. Since $a\in\mathbb{K}$ was arbitrary, $\mathbb{K}:\mathbb{F}$ is separable. □

Definition 3.5.12. *Let $\mathbb{K}:\mathbb{F}$ be algebraic field extension. Then $\mathbb{K}:\mathbb{F}$ is called* normal *if for each $a\in\mathbb{K}$, p_a splits over $\mathbb{K}$.*

Theorem 3.5.13. *Let $\mathbb{K}:\mathbb{F}$ be a field extension. Then the following statements are equivalent.*

(a) $\mathbb{K}$ is the splitting field of a separable polynomial over $\mathbb{F}$.

(b) $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ is finite and $\mathbb{F}=\mathrm{Fix}_{\mathbb{K}}(\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}))$.

(c) $\mathbb{F}=\mathrm{Fix}_{\mathbb{K}}(G)$ for some finite subgroup G of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(d) $\mathbb{K}:\mathbb{F}$ is finite, separable and normal.

Proof. (a) $\Longrightarrow$ (b): By 3.5.8 $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ is finite of order $\dim_{\mathbb{F}} \mathbb{K}$. Let $\mathbb{E} = \mathrm{Fix}_{\mathbb{K}}(\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}))$. Then $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \subseteq \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \subseteq \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ and so

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}). \tag{1}$$

Since $\mathbb{K}$ is the splitting field of a separable polynomial f over $\mathbb{F}$, $\mathbb{K}$ is also the splitting field of f over $\mathbb{E}$. By 3.4.3 f is separable over $\mathbb{E}$ and so we can apply 3.5.8 to $\mathbb{K} : \mathbb{E}$ and $\mathbb{K} : \mathbb{F}$. Hence

$$\dim_{\mathbb{E}} \mathbb{K} \leq \dim_{\mathbb{F}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{K} \overset{3.2.7}{=} \dim_{\mathbb{F}} \mathbb{K} \overset{3.5.8}{=} |\,\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| \overset{(1)}{=} |\,\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})| \overset{3.5.8}{=} \dim_{\mathbb{E}} \mathbb{K}.$$

Hence equality must hold everywhere in the above inequalities. Thus $\dim_{\mathbb{E}} \mathbb{K} = \dim_{\mathbb{F}} \mathbb{K}$ and so $\dim_{\mathbb{F}} \mathbb{E} = 1$ and $\mathbb{E} = \mathbb{F}$.

(b) $\Longrightarrow$ (c): Just put $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(c) $\Longrightarrow$ (d): By 3.5.10 $\mathbb{K} : \mathbb{F}$ is finite and by 3.5.11, $\mathbb{K} : \mathbb{F}$ is normal and separable.

(d) $\Longrightarrow$ (a): Since $\mathbb{K} : \mathbb{F}$ is finite there exists a basis $(k_1, k_2, \ldots, k_n)$ for $\mathbb{K}$ over $\mathbb{F}$. Then $\mathbb{K} \subseteq \mathbb{F}[a_1, a_2 \ldots, a_n] \subseteq \mathbb{K}$ and

$$\mathbb{K} = \mathbb{F}[a_1, a_2 \ldots, a_n]. \tag{2}$$

Let p_i be the minimal polynomial of a_i over $\mathbb{F}$. Since $\mathbb{K} : \mathbb{F}$ is separable, p_i is separable over $\mathbb{F}$. Since $\mathbb{K} : \mathbb{F}$ is normal, p_i splits over $\mathbb{F}$. Put $f = p_1 p_2 \ldots p_n$. Then f is separable and splits over $\mathbb{K}$. Let $a_1, a_2, \ldots, a_n, \ldots, a_m$ be the roots of f in $\mathbb{K}$ then by (1), $\mathbb{K} \subseteq \mathbb{F}[a_1, a_2 \ldots, a_m] \subseteq \mathbb{K}$ and so

$$K = \mathbb{F}[a_1, a_2 \ldots, a_m].$$

Thus $\mathbb{K}$ is a splitting field of f over $\mathbb{F}$. $\square$

Lemma 3.5.14. *Let $\mathbb{K} : \mathbb{F}$ be a field extension. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ and let $\mathbb{E}$ be subfield field of $\mathbb{K}$ containing $\mathbb{F}$. Then*

$$\sigma \,\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} = \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K})$$

Proof. Let $\rho \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then

$$\begin{array}{clcl}
 & \rho \in \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) & & \\
\Longleftrightarrow & \rho(k) = k \text{ for all } k \in \sigma(\mathbb{E}) & - & \text{Definition of } \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) \\
\Longleftrightarrow & \rho(\sigma(e)) = \sigma(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma(\mathbb{E}) \\
\Longleftrightarrow & \sigma^{-1}(\rho(\sigma(e)) = e \text{ for all } e \in \mathbb{E} & - & \sigma \text{ is a bijection} \\
\Longleftrightarrow & (\sigma^{-1}\rho\sigma)(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma^{-1}\rho\sigma \\
\Longleftrightarrow & \sigma^{-1}\rho\sigma \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) & - & \text{Definition of } \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \\
\Longleftrightarrow & \rho \in \sigma \,\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} & - & 1.8.1(c)
\end{array}$$

$\square$

Definition 3.5.15. *(a) A* Galois *extension is a finite, separable and normal field extension.*

(b) Let $\mathbb{K} : \mathbb{F}$ be a field extension. An intermediate *field of $\mathbb{K} : \mathbb{F}$ is a subfield $\mathbb{E}$ of $\mathbb{K}$ with $\mathbb{F} \subseteq \mathbb{E}$.*

Lemma 3.5.16. *Let $\mathbb{K} : \mathbb{F}$ be a Galois extension and $\mathbb{E}$ an intermediate field of $\mathbb{K} : \mathbb{F}$. The following are equivalent:*

(a) $\mathbb{E} : \mathbb{F}$ is normal.

(b) $\mathbb{E} : \mathbb{F}$ is Galois.

(c) $\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$, that is $\sigma(\mathbb{E}) = \mathbb{E}$ for all $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

Proof. (a) $\Longrightarrow$ (b): Suppose $\mathbb{E} : \mathbb{F}$ is normal. Since $\mathbb{K} : \mathbb{F}$ is separable, 3.4.3(d) implies that $\mathbb{E} : \mathbb{F}$ is separable. Since $\mathbb{K} : \mathbb{F}$ is finite, 3.1.19 implies that $\mathbb{E} : \mathbb{F}$ is finite. Thus $\mathbb{E} : \mathbb{F}$ is Galois.

(b) $\Longrightarrow$ (c): Suppose $\mathbb{E} : \mathbb{F}$ is Galois. Let $a \in \mathbb{E}$ and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. By 3.5.7 $\sigma(a)$ is a root of p_a. Since $\mathbb{E} : \mathbb{F}$ is normal, p_a splits over $\mathbb{E}$ and so $\sigma(a) \in \mathbb{E}$.

(c) $\Longrightarrow$ (a): Suppose that $\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ and let $a \in \mathbb{E}$. By 3.5.13 $\mathbb{F} = \mathrm{Fix}_{\mathbb{K}}(G)$ for some finite subgroup G of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. So by 3.5.11 p_a splits over $\mathbb{K}$ and if b is a root of p_a, then $b = \sigma(a)$ for some $\sigma \in G$. Since $\mathbb{E}$ is invariant under $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$, $b = \sigma(a) \in \mathbb{E}$. So p_a splits over $\mathbb{E}$ and $\mathbb{E} : \mathbb{F}$ is normal. $\square$

Theorem 3.5.17 (Fundamental Theorem of Galois Theory)**.** *Let $\mathbb{K} : \mathbb{F}$ be a Galois Extension. Let $\mathbb{E}$ be an intermediate field of $\mathbb{K} : \mathbb{F}$ and $G \leq \mathrm{Aut}_{\mathbb{F}}(K)$.*

(a) The map

$$\mathbb{E} \to \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$$

is a bijection between to intermediate fields of $\mathbb{K} : \mathbb{F}$ and the subgroups of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. The inverse of this map is given by

$$G \to \mathrm{Fix}_{\mathbb{K}}(G).$$

(b) $|G| = \dim_{\mathrm{Fix}_{\mathbb{K}}(G)} \mathbb{K}$ and $\dim_{\mathbb{E}} \mathbb{K} = |\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})|$.

(c) $\mathbb{E} : \mathbb{F}$ is normal if and only if $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ is normal in $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(d) If $\mathbb{E} : \mathbb{F}$ is normal, then the map

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \mathrm{Aut}_{\mathbb{F}}(\mathbb{E}), \sigma\, \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \sigma\,|_{\mathbb{E}}$$

is a well-defined isomorphism of groups.

Proof. (a) We will show that the two maps are inverses to each other. Since $\mathbb{K}$ is the splitting field of a separable polynomial f over $\mathbb{F}$, $\mathbb{K}$ is also the splitting field of f over $\mathbb{E}$. So by 3.5.13

$$(1) \qquad \mathrm{Fix}_{\mathbb{K}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})) = \mathbb{E}.$$

Put $\mathbb{L} = \mathrm{Fix}_{\mathbb{K}}(G)$.

$$(2) \qquad |\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})| \overset{3.5.8}{=} \dim_{\mathbb{L}} \mathbb{K} \overset{3.5.10}{\leq} |G| \leq |\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})|,$$

where the last equality holds since $G \leq \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$. It follows that equality holds everywhere in (2). In particular, $|G| = \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$ and $G = \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$, that is

$$(3) \qquad \mathrm{Aut}_{\mathrm{Fix}_{\mathbb{K}}(G)}(\mathbb{K}) = G.$$

By (1) and (3) the two maps in (a) are inverse to each other and so (a) holds.

(b) follows since equality holds everywhere in (2).

(c) We have

$$\begin{array}{cccc}
 & \mathbb{E} : \mathbb{F} \text{ is normal} & & \\
\iff & \sigma(\mathbb{E}) = \mathbb{E} \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 3.5.16 \\
\iff & \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & (a) \\
\iff & \sigma \,\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 3.5.14 \\
\iff & \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \trianglelefteq \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 1.8.6(b)
\end{array}$$

(d) By 3.5.16 $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$-invariant. So by 2.2.10(b) $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ acts on $\mathbb{E}$. The homomorphism associated to this action is

$$\alpha : \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \to \mathrm{Sym}(\mathbb{E}), \sigma \to \sigma \mid_{\mathbb{E}} .$$

In particular, $\sigma \mid_{\mathbb{E}}$ is a bijection from $\mathbb{E}$ to $\mathbb{E}$. Clearly $\sigma \mid_{\mathbb{E}}$ is a homomorphism. Thus $\sigma \mid_{\mathbb{E}}$ is a field isomorphism. Moreover, $(\sigma \mid_{\mathbb{E}}) \mid_{\mathbb{F}} = \sigma \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ and so $\sigma \mid_{\mathbb{E}} \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Thus $\mathrm{Im}\,\alpha \leq \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Let $\rho \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Then by 3.3.7, applied with $\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{E}$, $\mathbb{K}_1 = \mathbb{K}_2 = \mathbb{K}$, $f_1 = f_2 = f$ and $\sigma = \rho$ there exists a field isomorphism $\hat{\rho} : \mathbb{K} \to \mathbb{K}$ with $\check{\rho} \mid_{\mathbb{E}} = \rho$. Since $\check{\rho} \mid_{\mathbb{F}} = \rho \mid_{\mathbb{E}} = \mathrm{id}_{\mathbb{F}}$, $\check{\rho} \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Then $\rho = \alpha(\check{\rho})$ and so $\rho \in \mathrm{Im}\,\alpha$ and $\mathrm{Im}\,\alpha = \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$.

Note that $\sigma \in \ker \alpha$ if and only if $\alpha \mid_{\mathbb{E}} = \mathrm{id}_{\mathbb{E}}$. So $\ker \alpha = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Hence (d) follows from the First Isomorphism Theorem.

$\square$

Example 3.5.18.

Let $\mathbb{K}$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$ in $\mathbb{C}$. Let

$$\xi = e^{\frac{2\pi}{3}i}, \quad a = \sqrt[3]{2}, \quad b = \xi\sqrt[3]{2}, \quad \text{ and } c = \xi^2\sqrt[3]{2}.$$

By Example 3.5.9

$$\mathbb{K} = \mathbb{Q}[a, \xi], \quad \dim_{\mathbb{Q}} \mathbb{K} = 6 \text{ and } \operatorname{Aut}_{\mathbb{Q}}(\mathbb{K}) \cong \operatorname{Sym}(R) \cong \operatorname{Sym}(3),$$

where $R = \{a, b, c\}$ is the set of roots of $x^3 - 2$. For $(x_1, \dots x_n)$ a cycle in $\operatorname{Sym}(R)$ let $\sigma_{x_1 \dots x_n}$ be the corresponding element in $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$. So for example σ_{ab} is the unique element of $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$ with $\sigma_{ab}(a) = b, \sigma_{ab}(b) = a$ and $\sigma_{ab}(c) = c$. Then by Example 1.9.15 the subgroup of $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$ are

$$\{\mathrm{id}_{\mathbb{K}}\}, \langle\sigma_{ab}\rangle, \langle\sigma_{ac}\rangle, \langle\sigma_{bc}\rangle, \langle\sigma_{ac}\rangle, \langle\sigma_{abc}\rangle, \operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$$

We now compute the corresponding intermediate fields:
Observe that

$$\operatorname{Fix}_{\mathbb{K}}(\{\mathrm{id}_{\mathbb{K}}\}) = \mathbb{K}.$$

$\langle\sigma_{ab}\rangle$ has order 2. Hence by the FTGT 3.5.17(b), $\dim_{\operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle)} \mathbb{K} = 2$. Since $\dim_{\mathbb{Q}} \mathbb{K} = 6$, 3.2.7 implies that $\dim_{\mathbb{Q}} \operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle) = 3$. Since c is fixed by σ_{ab} and $\dim_{\mathbb{Q}} \mathbb{Q}[c] = \deg p_c = \deg(x^3 - 2) = 3$ we have

$$\operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle) = \mathbb{Q}[c] = \mathbb{Q}\left[\xi^2\sqrt[3]{2}\right].$$

Similarly,

$$\operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{ac}\rangle) = \mathbb{Q}[b] = \mathbb{Q}\left[\xi\sqrt[3]{2}\right]$$

and

$$\operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{bc}\rangle) = \mathbb{Q}[a] = \mathbb{Q}\left[\sqrt[3]{2}\right].$$

Note that $\dim_{\mathbb{Q}} \mathbb{Q}[\xi] = 2$ and so $\dim_{\mathbb{Q}[\xi]} \mathbb{K} = 3$. Hence $|\operatorname{Aut}_{\mathbb{Q}[\xi]} \mathbb{K}| = 3$. Since $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})$ has a unique subgroup of order 3 we get $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K}) = \langle\sigma_{abc}\rangle$ and so

$$\operatorname{Fix}_{\mathbb{K}}(\langle\sigma_{abc}\rangle) = \mathbb{Q}[\xi].$$

Let us verify that σ_{abc} indeed fixes ξ. From $b = a\xi$ we have $\xi = a^{-1}b$ and so

$$\sigma_{abc}(\xi) = \sigma_{abc}(a^{-1}b) = (\sigma_{abc}(a))^{-1}\sigma_{abc}(b) = b^{-1}c = \xi.$$

Finally by 3.5.13

$$\operatorname{Fix}_{\mathbb{K}}(\operatorname{Aut}_{\mathbb{Q}}(\mathbb{K})) = \mathbb{Q}.$$

Note that the roots of x^2+x+1 are ξ and ξ^2. So $\mathbb{Q}[\xi]$ is the splitting field of x^2+x+1 and $\mathbb{Q}[\xi] : \mathbb{Q}$ is a normal extension, corresponding to the fact that $\langle \sigma_{abc} \rangle$ is normal in $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

Since $p_a = x^3 - 2$ and neither b or c are in $\mathbb{Q}[a]$, p_a does not split over $\mathbb{Q}[a]$. Hence $\mathbb{Q}[a] : \mathbb{Q}$ is not normal, corresponding to the fact that $\langle \sigma_{bc} \rangle$ is not normal in $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

Appendix A

Sets

A.1 Equivalence Relations

Definition A.1.1. *Let $\sim$ be a relation on a set A. Then*

(a) $\sim$ is called reflexive *if $a \sim a$ for all $a \in A$.*

(b) $\sim$ is called symmetric *if $b \sim a$ for all $a, b \in A$ with $a \sim b$.*

(c) $\sim$ is called transitive *if $a \sim c$ for all $a, b, c \in A$ with $a \sim b$ and $b \sim c$.*

(d) $\sim$ is called an equivalence relation *if $\sim$ is reflexive, symmetric and transitive.*

(e) For $a \in A$ we define $[a]_\sim := \{b \in R \mid a \sim b\}$. We often just write $[a]$ for $[a]_\sim$. If $\sim$ is an equivalence relation then $[a]_\sim$ is called the equivalence class *of $\sim$ containing a.*

Remark A.1.2.

Suppose $P(a, b)$ is a statement involving the variables a and b. Then we say that $P(a, b)$ is a *symmetric* in a and b if $P(a, b)$ is equivalent to $P(b, a)$. For example the statement $a + b = 1$ is symmetric in a and b. Suppose that $P(a, b)$ is a symmetric in a and b, $Q(a, b)$ is some statement and that

$$(*) \qquad \text{For all a,b} \qquad P(a, b) \Longrightarrow Q(a, b).$$

Then we also have

$$(**) \qquad \text{For all a,b} \qquad P(a, b) \Longrightarrow Q(b, a).$$

Indeed, since (*) holds for all a, b we can use (*) with b in place of a and a in place of b. Thus

$$\text{For all a,b} \qquad P(b, a) \Longrightarrow Q(b, a).$$

Since $P(b,a)$ is equivalent to $P(a,b)$ we see that (**) holds. For example we can add $-b$ to both sides of $a+b=1$ to conclude that $a=1-b$. Hence also $b=1-a$ (we do not have to repeat the argument.)

Theorem A.1.3. *Let $\sim$ be an equivalence relation on the set A and $a,b\in A$. Then the following statements are equivalent:*

(a) $a\sim b$.

(b) $b\in[a]$.

(c) $[a]\cap[b]\neq\emptyset$.

(d) $[a]=[b]$.

(e) $a\in[b]$

(f) $b\sim a$.

Proof. (a) $\implies$ (b): Just recall that $[a]=\{b\in A\mid a\sim b\}$.

(b) $\implies$ (c): Since $\sim$ is reflexive, $b\sim b$ and so $b\in[b]$. From (b), $b\in[a]$ and so $b\in[a]\cap[b]$. Therefore $[a]\cap[b]\neq\emptyset$.

(c) $\implies$ (d): By (c) there exists $c\in[a]\cap[b]$. We will first show that $[a]\subseteq[b]$. So let $d\in[a]$. Then $a\sim d$. Since $c\in[a]$, $a\sim c$ and since $\sim$ is symmetric, $c\sim a$. Since $a\sim d$ and $\sim$ is transitive, $c\sim d$. Since $c\in[b]$, $b\sim c$. Since $c\sim d$ and $\sim$ is transitive, $b\sim d$ and so $d\in[b]$. Thus $[a]\subseteq[b]$. Since statement (c) is symmetric in a and b, we conclude that also $[b]\subseteq[a]$ and so $[a]=[b]$.

(d) $\implies$ (e): Since a is reflexive $a\in[a]$. So $[a]=[b]$ implies $a\in[b]$.

(e) $\implies$ (f): From $a\in[b]$ and the definition of $[b]$, $b\sim a$.

(f) $\implies$ (a): Since $b\sim a$ and $\sim$ is symmetric, $a\sim b$. □

A.2 Bijections

Definition A.2.1. *Let $f:A\to B$ be a function.*

(a) f is called 1-1 *or* injective *if $a=c$ for all $a,c\in A$ with $f(a)=f(c)$.*

(b) f is called onto *or* surjective *if for all $b\in B$ there exists $a\in A$ with $f(a)=b$.*

(c) f is called a 1-1 correspondence *or* bijective *if for all $b\in B$ there exists a unique $a\in A$ with $f(a)=b$.*

(d) $\operatorname{Im} f:=\{f(a)\mid a\in A\}$. $\operatorname{Im} f$ *is called the* image *of f.*

□

Observe that f is 1-1 if and only if for each b in B there exists at most one $a\in A$ with $f(a)=b$. So f is 1-1 correspondence if and only f is 1-1 and onto.

Also f is onto if and only if $\operatorname{Im} f=B$.

Definition A.2.2. *(a) Let A be a set. The* identity function id_A *on A is the function*

$$\mathrm{id}_A : A\to A,\quad a\to a.$$

(b) Let $f : A \to B$ and $g : B \to C$ be function. Then $g \circ f$ is the function

$$g \circ f : A \to C, \quad a \to g(f(a)).$$

$g \circ f$ is called the composition *of g and f.*

Lemma A.2.3. *Let $f : A \to B$ and $B \to C$ be functions.*

(a) If f and g are 1-1, so is $g \circ f$.

(b) If f and g are onto, so is $g \circ f$.

(c) If f and g is a bijection, so is $g \circ f$.

Proof. (a) Let $x, y \in A$ with $(g \circ f)(x) = (g \circ f)(y)$. Then $g(f(x)) = g(f(y))$ Since g is 1-1, this implies $f(x) = f(y)$ and since f is 1-1, $x = y$. Hence $g \circ f$ is $1 - 1$.

(b) Let $c \in C$. Since g is onto, there exists $b \in B$ with $g(b) = c$. Since f is onto there exists $a \in A$ with $f(a) = b$. Thus

$$(g \circ f)(a) = g(f(a)) = g(b) = c,$$

and so $g \circ f$ is onto.

(c) Suppose f and g are bijections. By (a) , $g \circ f$ is 1-1 and by (b) $g \circ f$ is onto. So also $g \circ f$ is a bijection. □

Definition A.2.4. *Let $f : A \to B$ be a function.*

(a) If $C \subseteq A$, then $f(C) := \{f(c) \mid c \in C\}$. $f(C)$ is called the image *of C under f.*

(b) If $D \subseteq B$, then $f^{-1}(D) := \{c \in C \mid f(c) \in D\}$. $f^{-1}(D)$ is called the inverse image *of D under f.*

Lemma A.2.5. *Let $f : A \to B$ be a function.*

(a) Let $C \subseteq A$. Then $C \subseteq f^{-1}(f(C))$.

(b) Let $C \subseteq A$. If f is 1-1 then $f^{-1}(f(C)) = C$.

(c) Let $D \subseteq B$. Then $f(f^{-1}(D)) \subseteq D$.

(d) Let $D \subseteq B$. If f is onto then $f(f^{-1}(D)) = D$.

Proof. (a) Let $c \in C$, then $f(c) \in f(C)$ and so $c \in f^{-1}(f(C))$. Thus (a) holds.

(b) Let $x \in f^{-1}(f(C))$. Then $f(x) \in f(C)$ and so $f(x) = f(c)$ for some $c \in C$. Since f is 1-1, $x = c$ and so $f^{-1}(f(C)) \subseteq C$. By (a) $C \subseteq f^{-1}(f(C))$ and so (b) holds.

(c) Let $x \in f^{-1}(C)$. Then $f(x) \in C$ and so (d) holds.

(d) Let $d \in D$. Since f is onto, $d = f(a)$ for some $a \in D$. Then $f(a) \in D$ and so $a \in f^{-1}(D)$. It follows that $d = f(a) \in f(f^{-1}(D))$. Thus $D \subseteq f(f^{-1}(D))$. By $f(f^{-1}(D)) \subseteq D$ and so (d) holds. □

Lemma A.2.6. *Let $f : A \to B$ be a function and suppose $A \neq \emptyset$.*

(a) f is 1-1 if and only if there exists a function $g : B \to A$ with $g \circ f = \mathrm{id}_A$.

(b) f is onto if and only of there exists a function $g : B \to A$ with $f \circ g = \mathrm{id}_B$.

(c) f is a bijection if and only if there exists a function $g : B \to A$ with $f \circ g = \mathrm{id}_B$ and $g \circ A = \mathrm{id}_B$.

Proof. $\Longrightarrow$: We first prove the 'forward' direction of (a), (b) and (c). Since A is not empty, we can fix an element $a_0 \in A$. Let $b \in B$. If $b \in \operatorname{Im} f$ choose $a_b \in A$ with $f(a_b) = b$. If $b \notin \operatorname{Im} f$, put $a_b = a_0$. Define

$$g : B \to A, \quad b \to a_b$$

(a) Suppose f is 1-1. Let $a \in A$ and put $b = f(a)$. Then $b \in \operatorname{Im} f$ and so $f(a_b) = b = f(a)$. Since f is 1-1, $a_b = a$ and so $g(f(a)) = g(b) = a_b = a$. Thus $g \circ f = \mathrm{id}_A$.

(b) Suppose f is onto. Then $B = \operatorname{Im} f$ and so $f(a_b) = b$ for all $b \in B$. Thus $f(g(b)) = f(a_b) = b$ and $f \circ g = \mathrm{id}_B$.

(c) Suppose f is a 1-1 correspondence. Then f is 1-1 and onto and so by (a) and (b), $f \circ g = \mathrm{id}_B$ and $g \circ f = id_A$.

$\Longleftarrow$: Now we establish the backward directions.

(a) Suppose there exists $g : B \to A$ with $g \circ f = \mathrm{id}_A$. Let $a, c \in A$ with $f(a) = f(c)$.

$$\begin{array}{cccc} & f(a) & = & f(c) \\ \Longrightarrow & g(f(a)) & = & g(f(c)) \\ \Longrightarrow & (g \circ f)(a) & = & (g \circ f)(a) \\ \Longrightarrow & \mathrm{id}_A(a) & = & \mathrm{id}_A(c) \\ \Longrightarrow & a & = & c \end{array} .$$

Thus $f(a) = f(c)$ implies $a = c$ and f is 1-1.

(b) Suppose there exists $g : B \to A$ with $f \circ g = \mathrm{id}_B$. Let $b \in B$ and put $a = g(b)$. Then $f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b$ and so f is onto.

(c) Suppose there exists $g : B \to A$ with $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. Then by (a) and (b), f is 1-1 and onto. So f is a 1-1 correspondence. $\square$

A.3 Cardinalities

Definition A.3.1. *Let A and B be sets. We write $A \approx B$ if there exists a bijection from A to B. We write $A \prec B$ if there exists injection from A to B.*

Lemma A.3.2. *(a) $\approx$ is an equivalence relation.*

(b) If A and B are sets with $A \approx B$, then $A \prec B$.

(c) $\prec$ is reflexive and transitive.

(d) Let A and B be sets. Then $A \prec B$ if and only if there exists $C \subseteq B$ with $A \approx C$.

Proof. (a) Let A be a set. Then id_A is a bijection and so $A \approx B$. Hence $\approx$ is reflexive. Let

$$f : A \to B$$

be a bijection. Then by A.2.6(c) there exists a bijection $g : B \to A$. So $\approx$ is symmetric. Let $f : A \to B$ and $g : B \to C$ be bijections. Then by A.2.3(c) $g \circ f$ is a bijection and so $A \approx C$ and $\approx$ is transitive.

(b) Obvious since any bijection is an injection.

(c) By (a) $A \approx A$ and so by (b) $A \prec A$. A.2.3(a) shows that $\prec$ is transitive.

(c) Suppose $f : A \to B$ is an injection. Then $A \approx \operatorname{Im} f$ and $\operatorname{Im} f \subseteq B$.

Suppose that $A \approx C$ for some $C \subseteq B$. By (b) $A \prec C$. The inclusion map from C to B shows that $C \prec B$. Since $\prec$ is transitive we get $A \prec B$. □

Definition A.3.3. *Let A be a set. Then $|A|$ denotes the equivalence class of $\approx$ containing. An* cardinal *is a class of the form $|A|$, A a set. If a, b are cardinals then we write $a \leq b$ if there exist sets A and B with $a = |A|$, $b = |B|$ and $A \prec B$.*

Lemma A.3.4. *Let A and B be sets.*

(a) $|A| = |B|$ if and only if $A \approx B$.

(b) $|A| \leq |B|$ if and only if $A \prec B$.

Proof. (a) follows directly from the definition of $|A|$.

(b) If $A \prec B$, then by definition of $'\leq'$, $|A| \leq |B|$. Suppose that $|A| \leq |B|$. Then there exist sets A' and B' with $|A| = |A'|$, $|B| = |B'|$ and $A' \prec B'$. Then also $A \approx A'$ and $B \approx B'$ and so by A.3.2, $A \prec B$. □

Theorem A.3.5 (Cantor-Bernstein)**.** *Let A and B be sets. Then $A \approx B$ if and only if $A \prec B$ and $B \prec A$.*

Proof. If $A \approx B$, then by A.3.2(a) $B \approx C$ and by A.3.2(b), $A \prec B$ and $B \prec C$.

Suppose now that $A \prec B$ and $B \prec A$. Since $B \prec A$, A.3.2(d) implies $B \approx B^*$ for some $B^* \subseteq A$. Then by A.3.2 $B^* \prec A$ and $A \prec B^*$. So replacing B by B^* we may assume that $B \subseteq A$. Since $A \prec B$, $A \approx C$ for some $C \subseteq B$. Let $f : A \to C$ be a bijection. Define

$$E := \{a \in A \mid i = f^n(d) \text{ for some } n \in \mathbb{N}, d \in A \setminus B\},$$

and

$$g : A \to A, \quad a \to \begin{cases} f(a) & \text{if } a \in E \\ a & \text{if } a \notin E \end{cases}.$$

We will show that g is 1-1 and $\operatorname{Im} g = B$.
Let $x, y \in A$ with $g(x) = g(y)$. We need to show that $x = y$.

Case 1: $x \notin E$ and $y \notin E$.
Then $x = g(x) = g(y) = y$.

Case 2': $x \in E$ and $y \notin E$.
Then $x = f^n(d)$ for some $d \in A \setminus B$ and $y = g(y) = g(x) = f(x) = f^{n+1}(d)$. But then $y \in E$, a contradiction.

Case 3: $x \notin E$ and $y \in E$.
This leads to the same contradiction as in the previous case.

Case 4: $x \in E$ and $y \in E$.
Then $f(x) = g(x) = g(y) = f(y)$. Since f is 1-1 we conclude that $x = y$.

So in all four cases $x = y$ and g is 1-1.

We will now show that $\operatorname{Im} g \subseteq B$. For this let $a \in A$.
If $a \in E$, then $g(a) = f(a) \in C \subseteq B$.
If $a \notin E$, then $a \in B$ since otherwise $a \in A \setminus B$ and $a = f^0(a) \in E$. Hence $g(a) = a \in B$. Thus $\operatorname{Im} g \subseteq B$.
Next we show that $B \subseteq \operatorname{Im} g$. For this let $b \in B$.
If $b \notin E$, the $b = g(b) \in \operatorname{Im} g$.
If $b \in E$, pick $n \in \mathbb{N}$ and $d \in A \setminus B$ with $b = f^n(a)$. Since $b \in B$, $b \neq d$ and so $n > 0$. Observer that $f^{n-1}(d) \in E$ and so $b = f(f^{n-1}(d)) = g(f^{n-1}(d)) \in \operatorname{Im} g$. Thus $B \subseteq \operatorname{Im} g$.
It follows that $B = \operatorname{Im} g$. Therefore g is a bijection from A to B and so $A \approx B$. □

Corollary A.3.6. *Let c and d be cardinals. Then $c = d$ if and only if $c \leq d$ and $d \leq c$.*

Proof. Follows immediately from A.3.5 and A.3.4. □

Definition A.3.7. *Let I be a set. Then I is called* finite *if the exists $n \in \mathbb{N}$ and a bijection $f : I \to \{1, 2, \ldots, n\}$. I is called* countable *if either I is finite or there exists a bijections $f : I \to \mathbb{Z}^+$.*

Example A.3.8.

We will show that

$$|\mathbb{Z}^+| < |\mathbb{R}|,$$

where $<$ means $\leq$ but not equal. In particular $\mathbb{R}$ is not countable Since $|[0,1)| \leq |\mathbb{R}|$ it suffices to show that $|\mathbb{Z}^+| < |[0,1)|$. Since the map $\mathbb{Z}^+ \to [0,1, \quad n \to \frac{1}{n}$ is 1-1, $|\mathbb{Z}^+| \leq |[0,1)|$. So it suffices to show that $|\mathbb{Z}^+| \neq |[0,1)|$.

Let $f : \mathbb{Z}^+ \to [1,0)$ be function. We will show that f is not onto. Note that any $r \in [0,1)$ can be unique written as

$$r = \sum_{i=1}^{\infty} \frac{r_i}{10^i},$$

where r_i is an integer with $0 \le r_i \le 9$, and not almost all r_i are equal to 9. (almost all means all but finitely many). For $i \in \mathbb{Z}^+$ define

$$s(i) := \begin{cases} 0 & \text{if } f(i)_i \neq 0 \\ 1 & \text{if } f(i)_i = 0 \end{cases}.$$

This definition is made so that $s(i) \neq f(i)_i$ for all $i \in \mathbb{Z}^+$.

Put $s := \sum_{i=1}^{\infty} \frac{s(i)}{10^i}$. Then for any $i \in \mathbb{Z}^+$, $s_i = s(i) \neq f(i)_i$ and so $s \neq f(i)$. Thus $s \notin \operatorname{Im} f$ and f is not onto.

We proved that there does not exist an onto function from $\mathbb{Z}^+$ to $[1,0)$. In particular, there does not exist a bijection from $\mathbb{Z}^+$ to $[1,0)$ and $|\mathbb{Z}^+| \neq |[1,0)|$.

Lemma A.3.9. *(a) Let A and B be countable sets. Then $A \times B$ is countable.*

(b) Let A be a countable set. Then B^n is countable for all positive integers n.

Proof. (a) It suffices to show that $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable. Let $(a,b),(c,d) \in \mathbb{Z}^+$. We define the relation $<$ on $\mathbb{Z}^+ \times \mathbb{Z}^+$ by $(a,b) < (c,d)$ if one of the following holds:

$$\max(a,b) < \max(c,d);$$

$$\max(a,b) = \max(c,d), \quad \text{and } a < c; \qquad \text{or}$$

$$\max(a,b) = \max(c,d), \qquad a = c \qquad \text{and } b < d$$

So $(1,1) < (1,2) < (2,1) < (2,2) < (1,3) < (2,3) < (3,1) < (3,2)) < (3,3) < (1,4) < (2,4) < (3,4) < (4,1) < (4,2) < (4,3) < (4,4) < (1,5) < \ldots$

Let $a_1 = (1,1)$ and inductively let a_{n+1} smallest element (with respect to $'<'$) which is larger than a_n in $\mathbb{Z}^+ \times \mathbb{Z}^+$. So $a_2 = (1,2)$, $a_3 = (2,1)$, $a_4 = (2,2)$, $a_5 = (1,3)$ and so on. We claim that

$$f : \mathbb{Z}^+ \to \mathbb{Z}^+ \times \mathbb{Z}^+, \quad n \to a_n$$

is a bijection. Indeed if $n < m$, then $a_n < a_m$ and so f is 1-1. Let $(c,d) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Then $\max(a,b) < \max(c,d)$ for all (a,b) with $(a,b) < (c,d)$. Hence there exist only finitely many $(a,b)'s$ with $(a,b) < (c,d)$. Let (x,y) be the largest of these. Then by induction $(x,y) = a_n$ for some n and so $(c,d) = a_{n+1}$. Thus f is onto.

(b) The proof is by induction on n. If $n = 1$, (b) clearly holds. So suppose that (b) holds for $n = k$. So A^k is countable. Since $A^{k+1} = A \times A^k$, (a) implies that A^{k+1} is countable. So by the Principal of Mathematical Induction, (b) holds for all positive integers n. $\square$

Appendix B

List of Theorems, Definitions, etc

B.1 List of Theorems, Propositions and Lemmas

Lemma 1.2.1. *Let u, a, b be objects with $\{u, a\} = \{u, b\}$. Then $a = b$.*

Proposition 1.2.2. *Let a, b, c, d be objects. Then*

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

Lemma 1.3.7. *Let $*$ be a binary operation on the set I, then $*$ has at most one identity in I.*

Proof. Let e and f be identities of $*$. Then $e * f = f$ since e is an identity and $e * f = e$ since f is an identity. Hence $e = f$. So any two identities of $*$ are equal. □

Lemma 1.3.10. *Let $*$ be an associative binary operation on the set I with identity e. Then each $a \in I$ has at most one inverse in I with respect to $*$.*

Lemma 1.4.2. *Let G be a group and $a, b \in G$.*

(a) $(a^{-1})^{-1} = a$.

(b) $a^{-1}(ab) = b$, $(ba)a^{-1} = b$, $(ba^{-1})a = b$ *and* $a(a^{-1}b) = b$.

Lemma 1.4.3. *Let G be a group and $a, b, c \in G$. Then*

$$\begin{aligned} & ab = ac \\ \iff & \ \ b = c \\ \iff & ba = ca \ . \end{aligned}$$

Lemma 1.4.4. *Let G be a group and $a, b \in G$.*

(a) The equation $ax = b$ has a unique solution in G, namely $x = a^{-1}b$.

(b) The equation $ya = b$ has a unique solution in G, namely $y = ba^{-1}$.

(c) $b = a^{-1}$ if and only if $ab = e$ and if and only if $ba = e$.

(d) $(ab)^{-1} = b^{-1}a^{-1}$.

Lemma 1.4.7. *Let G be a group, $a \in G$ and $n, m \in \mathbb{Z}$. Then*

(a) $a^n a^m = a^{n+m}$.

(b) $a^{nm} = (a^n)^m$.

Proposition 1.5.3 (Subgroup Proposition)**.** *(a) Let $(G, *)$ be a group and H a subset of G. Suppose that*

(i) H is closed under $*$, that is $a * b \in H$ for all $a, b \in H$.

(ii) $e_G \in H$.

(iii) H is closed under inverses, that is $a^{-1} \in H$ for all $a \in H$.(where a^{-1} is the inverse of a in G with respect to $*$.

Define $\triangle : H \times H \to H, (a, b) \to a * b$. Then $\triangle$ is a well-defined binary operation on H and $(H, \triangle)$ is a subgroup of $(G, *)$.

(b) Suppose $(H, \triangle)$ is a subgroup of $(G, *)$. Then

(a) (a:i),(a:ii) and (a:iii) hold.

(b) $e_H = e_G$.

(c) Let $a \in H$. Then the inverse of a in H with respect to $\triangle$ is the same as the inverse of a in G with respect to $*$.

Lemma 1.5.4. *Let G be a group.*

(a) Let A and B be subgroups of G. Then $A \cap B$ is a subgroup of G.

(b) Let $(G_i, i \in I)$ a family of subgroups of G, i.e. I is a set and for each $i \in I, G_i$ is a subgroup of G. Then

$$\bigcap_{i \in I} G_i$$

is a subgroup of G.

Lemma 1.5.5. *Let I be a subset of the group G.*

- *Put $H_1 := \bigcap_{I \subseteq H \leq G} H$. In words, H_1 is the intersection of all the subgroups of G containing I.*

- *Let H_2 be a subgroup of G such that $I \subseteq H$ and whenever K is a subgroup of G with $I \subseteq K$, then $H_2 \subseteq K$.*

- *Let J be subset of G. We say that e is* product *of length* 0 *of J. Inductively, we say that $g \in G$ is a product of length $k+1$ of J if $g = hj$ where h is a product of length k of J and $j \in J$. Set $I^{-1} = \{i^{-1} \mid i \in I\}$ and let H_3 be the set of all products of arbitrary length of $I \cup I^{-1}$.*

Then $H_1 = H_2 = H_3$.

Lemma 1.6.2. *Let $f : A \to B$ be a function and define $g : A \to \operatorname{Im} f, a \to f(a)$.*

(a) g is onto.

(b) f is 1-1 if and only if g is 1-1.

Lemma 1.6.5. *Let $f : G \to H$ be a homomorphism of groups.*

(a) $f(e_G) = e_H$.

(b) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

(c) $\operatorname{Im} f$ is a subgroup of H.

(d) If f is 1-1, then $G \cong \operatorname{Im} f$.

Theorem 1.6.7 (Cayley's Theorem)**.** *Every group is isomorphic to group of permutations.*

Proposition 1.7.3. *Let K be a subgroup of the group G. Then $'\equiv \pmod{K}'$ is an equivalence relation on G.*

Proposition 1.7.6. *Let K be a subgroup of the group G and $a, b \in G$. Then aK is the equivalence class of $'\equiv \pmod{K}'$ containing a. Moreover, the following statements are equivalent*

(a) $b = ak$ for some $k \in K$.

(b) $a^{-1}b = k$ for some $k \in K$.

(c) $a^{-1}b \in K$.

(d) $a \equiv b \pmod{K}$.

(e) $b \in aK$.

(f) $aK \cap bK \neq \emptyset$.

(g) $aK = bK$.

(h) $a \in bK$.

(i) $b \equiv a \pmod{K}$.

(j) $b^{-1}a \in K$.

(k) $b^{-1}a = j$ for some $j \in K$.

(l) $a = bj$ for some $j \in K$.

Proposition 1.7.7. *Let K be a subgroup of the group G.*

(a) Let $T \in G/K$ and $a \in G$. Then $a \in T$ if and only if $T = aK$.

(b) G is the disjoint union of its cosets, that is every element of G lies in a unique coset of K.

(c) Let $T \in G/K$ and $a \in T$. Then the map $\delta : K \to T, k \to ak$ is a bijection. In particular, $|T| = |K|$.

Theorem 1.7.9 (Lagrange)**.** *Let G be a finite group and K a subgroup of G. Then*

$$|G| = |K| \cdot |G/K|.$$

In particular, $|K|$ divides $|G|$.

Corollary 1.7.11. *Let G be a finite group.*

(a) If $a \in G$, then the order of a divides the order of G.

(b) If $|G| = n$, then $a^n = e$ for all $a \in G$.

Lemma 1.7.14. *Let G be a group of finite order n.*

(a) Let $g \in G$. Then $G = \langle g \rangle$ if and only if $|g| = n$.

(b) G is cyclic if and only if G contains an element of order n.

Corollary 1.7.15. *Any group of prime order is cyclic.*

Lemma 1.8.1. *Let G be a group, A, B, C subsets of G and $g, h \in G$. Then*

(a) $A(BC) = \{abc \mid a \in A, b \in B, c \in C\} = (AB)C$.

(b) $A(gh) = (Ag)h$, $(gB)h = g(Bh)$ and $(gh)C = g(hC)$.

(c) $Ae = A = Ae = (Ag)g^{-1} = g^{-1}(gA)$.

(d) $A = B$ if and only if $Ag = Bg$ and if and only if $gA = gB$.

(e) $A \subseteq B$ if and only if $Ag \subseteq Bg$ and if and only if $gA \subseteq gB$.

(f) If A is subgroup of G, then $AA = A$ and $A^{-1} = A$.

(g) $(AB)^{-1} = B^{-1}A^{-1}$.

(h) $(gB)^{-1} = B^{-1}g^{-1}$ and $(Ag)^{-1} = g^{-1}A^{-1}$.

Lemma 1.8.5. *Let G be an abelian group. Then $AB = BA$ for all subsets A, B of G. In particular, every subgroup of G is normal in G.*

Lemma 1.8.6. *Let N be a subgroup of the group G. Then the following statements are equivalent:*

(a) N is normal in G.

(b) $aNa^{-1} = N$ for all $a \in G$.

(c) $aNa^{-1} \subseteq N$ *for* $a \in G$.

(d) $ana^{-1} \in N$ *for all* $a \in G$ *and* $n \in N$.

(e) Every right coset of N *is a left coset of* N.

Proposition 1.8.7 (Normal Subgroup Proposition)**.** *Let* N *be a subset of the group* G. *Then* N *is a normal subgroup of* G *if and only if*

(i) N *is closed under multiplication, that is* $ab \in N$ *for all* $a, b \in N$.

(ii) $e_G \in N$.

(iii) N *is closed under inverses, that is* $a^{-1} \in N$ *for all* $a \in N$.

(iv) N *is invariant under conjugation, that is* $gng^{-1} \in N$ *for all* $g \in G$ *and* $n \in N$.

Corollary 1.8.8. *Let* N *be a normal subgroup of the group* G, $a, b \in G$ *and* $T \in G/N$.

(a) $(aN)(bN) = abN$.

(b) $(aN)^{-1} = a^{-1}N$.

(c) $NT = T$.

(d) $T^{-1} \in G/N$, $TT^{-1} = N$ *and* $T^{-1}T = N$.

Theorem 1.8.10. *Let* G *be a group and* $N \trianglelefteq G$. *Then* $(G/N, *_{G/N})$ *is group. The identity of* G/N *is*

$$e_{G/N} = N = eN,$$

and the inverse of $T = gN \in G/N$ *with respect to* $*_{G/N}$ *is*

$$(gN)^{-1} = T^{-1} = \{t^{-1} \mid t \in T\} = g^{-1}N.$$

Lemma 1.9.2. *Let* $\phi : G \to H$ *be a homomorphism of groups. Then* $\ker \phi$ *is a normal subgroup of* G.

Lemma 1.9.3. *Let* N *be a normal subgroup of* G *and define*

$$\phi : G \to G/N, g \to gN.$$

Then ϕ *is an onto group homomorphism with* $\ker \phi = N$. ϕ *is called the* natural homomorphism *from* G *to* G/N.

Corollary 1.9.4. *Let* N *be a subset of the group* G. *Then* N *is a normal subgroup of* G *if and only if* N *is the kernel of a homomorphism.*

Theorem 1.9.5 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism of groups. Then*

$$\overline{\phi} : G/\ker\phi \to \operatorname{Im}\phi, \quad g\ker\phi \to \phi(g)$$

is well-defined isomorphism of groups. In particular

$$G/\ker\phi \cong \operatorname{Im}\phi.$$

Proof. Put $N = \ker\phi$ and Let $a, b \in G$. Then

$$\begin{array}{rcll} & gN = hN & & \\ \iff & g^{-1}h \in N & - & 1.7.6 \\ \iff & \phi(g^{-1}h) = e_H & - & \text{Definition of } N = \ker\phi \\ \iff & \phi(g)^{-1}\phi(h) = e_H & - & \phi \text{ is a homomorphism}, 1.6.5(b) \\ \iff & \phi(h) = \phi(g) & - & \text{Multiplication with } \phi(g) \text{ from the left,} \\ & & & \qquad \text{Cancellation law} \end{array}$$

So

$$(*) \qquad gN = hN \iff \phi(g) = \phi(h).$$

Since $gN = hN$ implies $\phi(g) = \phi(h)$ we conclude that $\overline{\phi}$ is well-defined.
Let $S, T \in G/N$. Then there exists $g, h \in N$ with $S = gN$ and $T = hN$.
Suppose that $\overline{\phi}(T) = \overline{\phi}(S)$. Then

$$\phi(g) = \overline{\phi}(gN) = \overline{\phi}(S) = \overline{\phi}(T) = \overline{\phi}(hN) = \phi(h),$$

and so by (*) $gN = hN$. Thus $S = T$ and ϕ is 1-1.

Let $b \in \operatorname{Im}\phi$. Then there exists $a \in G$ with $b = \phi(a)$ and so $\overline{\phi}(aN) = \phi(a) = b$. Therefore $\overline{\phi}$ is onto.

Finally

$$\overline{\phi}(ST) = \overline{\phi}(gNhN) \overset{1.8.8(a)}{=} \overline{\phi}(ghN) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(gN)\overline{\phi}(hN) = \overline{\phi}(S)\overline{\phi}(T)$$

and so $\overline{\phi}$ is a homomorphism. We proved that $\overline{\phi}$ is a well-defined, 1-1 and onto homomorphism, that is a well-defined isomorphism. $\square$

Lemma 1.9.8. *Let $(A, *)$ and $(B, \Box)$ be groups. Then*

(a) $(A \times B,\ * \times \Box)$ *is a group.*

(b) $e_{A\times B} = (e_A, e_B)$.

(c) $(a, b)^{-1} = (a^{-1}, b^{-1})$.

(d) If A and B are abelian, so is $A \times B$.

Lemma 1.9.10. *Let G be a group, H a subgroup of G and $T \subseteq H$.*

(a) T is a subgroup of G if and only if T is a subgroup of H.

(b) If $T \trianglelefteq G$, then $T \trianglelefteq H$.

(c) If $\alpha : G \to F$ is a homomorphism of groups, then $\alpha_H : H \to F, h \to \alpha(h)$ is also a homomorphism of groups. Moreover, $\ker \alpha_H = H \cap \ker \alpha$ and if α is 1-1 so is α_H.

Theorem 1.9.11 (Second Isomorphism Theorem)**.** *Let G be a group, N a normal subgroup of G and A a subgroup of G. Then $A \cap N$ is a normal subgroups of A, AN is a subgroup of G, N is a normal subgroup of AN and the map*

$$A/A \cap N \to AN/N, \quad a(A \cap N) \to aN$$

is a well-defined isomorphism. In particular,

$$A/A \cap N \cong AN/N.$$

Lemma 1.9.13. *Let $\phi : G \to H$ be a homomorphism of groups.*

(a) If $A \leq G$ then $\phi(A)$ is a subgroup of H, where $\phi(A) = \{\phi(a) \mid a \in A\}$.

(b) If $A \trianglelefteq G$ and ϕ is onto, $\phi(A) \trianglelefteq H$.

(c) If $B \leq H$, then $\phi^{-1}(B)$ is a subgroup of G, where $\phi^{-1}(B) := \{a \in A \mid \phi(a) \in A\}$

(d) If $B \trianglelefteq H$, then $\phi^{-1}(B) \trianglelefteq G$.

Theorem 1.9.14 (Correspondence Theorem)**.** *Let N be a normal subgroup of the group G. Put*

$$S(G, N) = \{H \mid N \leq H \leq G\} \text{ and } S(G/N) = \{F \mid F \leq G/N\}.$$

Let

$$\pi : G \to G/N, \quad g \to gN$$

be the natural homomorphism.

(a) Let $N \leq K \leq G$. Then $\pi(K) = K/N$.

(b) Let $F \leq G/N$. Then $\pi^{-1}(F) = \bigcup_{T \in F} T$.

(c) Let $N \leq K \leq G$ and $g \in G$. Then $g \in K$ if and only if $gN \in K/N$.

(d) The map

$$\beta : \quad \mathcal{S}(G, N) \to \mathcal{S}(G/N), \quad K \to K/N$$

is a well-defined bijection with inverse

$$\alpha : \quad \mathcal{S}(G/N) \to \mathcal{S}(G, N), \quad F \to \pi^{-1}(F).$$

In other words:

(a) *If $N \leq K \leq G$, then K/N is a subgroup of G/N.*

(b) *For each subgroup F of G/N there exists a unique subgroup K of G with $N \leq K$ and $F = K/N$. Moreover, $K = \pi^{-1}(F)$.*

(e) *Let $N \leq K \leq G$. Then $K \trianglelefteq G$ if and only if $K/N \trianglelefteq G/N$.*

(f) *Let $N \leq H \leq G$ and $N \leq K \leq G$. Then $H \subseteq K$ if and only if $H/N \subseteq K/N$.*

(g) **(Third Isomorphism Theorem)** *Let $N \leq H \trianglelefteq G$. Then the map*

$$\rho : \quad G/H \to (G/N)\big/(H/N), \quad gH \to (gN) * (H/N)$$

is a well-defined isomorphism.

Lemma 2.1.3. *Let G be a group and I a set.*

(a) *Suppose $\diamond$ is an action of G on I. For $a \in G$ define*

$$f_a : \quad I \to I, \quad i \to a \diamond i.$$

Then $f_a \in \mathrm{Sym}(I)$ and the map

$$\Phi_\diamond : \quad G \to \mathrm{Sym}(I), \quad a \to f_a$$

is a homomorphism. $\Phi_\diamond$ is called the homomorphism associated to the action of *G on I.*

(b) *Let $\Phi : G \to \mathrm{Sym}(I)$ be homomorphisms of groups. Define*

$$\diamond : G \times I \to I, (g, i) \to \Phi(g)(i).$$

Then $\diamond$ is an action of G on I.

Lemma 2.1.5. *Let G be a group and H a subgroups of G. Define*

$$\diamond_{G/H} : \quad G \times G/H \to G/H, \quad (g, T) \to gT$$

Then $\diamond_{G/H}$ is well-defined action of G on G/H. This action is called the action of G on G/H by left multiplication.

Lemma 2.1.7 (Cancellation Law for Action)**.** *Let G be a group acting on the set I, $a \in G$ and $i, j \in H$. Then*

(a) $a^{-1}(ai) = i$.

(b) $i = j \iff ai = aj$.

(c) $j = ai \iff i = a^{-1}j$.

Lemma 2.1.10. *Let G be a group acting in the set I. Then $' \equiv \pmod G'$ is an equivalence relation on I. The equivalence class of $' \equiv \pmod G'$ containing $i \in I$ is Gi.*

Proposition 2.1.11. *Let G be a group acting on the set I and $i, j \in G$. Then following are equivalent.*

(a) $j = gi$ *for some* $g \in G$.

(b) $i \equiv j \pmod G$

(c) $j \in Gi$.

(d) $Gi \cap Gj \neq \emptyset$

(e) $Gi = Gj$

(f) $i \in Gj$.

(g) $j \equiv i \pmod G$.

(h) $i = hj$ *for some* $h \in G$

Corollary 2.1.13. *Let* G *be group acting on the non-empty set* I. *Then the following are equivalent*

(a) G *acts transitively on* I.

(b) $I = Gi$ *for all* $i \in I$.

(c) $I = Gi$ *for some* $i \in I$.

(d) I *is an orbit for* G *on* I.

(e) G *has exactly one orbit on* I.

(f) $Gi = Gj$ *for all* $i, j \in G$.

(g) $i \equiv j \pmod G$ *for all* $i, j \in G$.

Theorem 2.1.16 (Isomorphism Theorem for G-sets)**.** *Let* G *be a group and* $(I, \diamond)$ *a* G*-set. Let* $i \in I$ *and put* $H = \mathrm{Stab}_G(i)$. *Then*

$$\phi : \quad G/H \to Gi, \quad aH \to ai$$

is a well-defined G*-isomorphism.*

In particular

$$G/H \cong_G Gi, \quad |Gi| = |G/\,\mathrm{Stab}_G(i)| \quad \text{and} \quad |Gi| \text{ divides } |G|$$

Theorem 2.1.18 (Orbit Equation)**.** *Let* G *be a group acting on a finite set* I. *Let* $I_k, 1 \leq k \leq n$ *be the distinct orbits for* G *on* I. *For each* $1 \leq k \leq n$ *let* i_k *be an element of* I_k. *Then*

$$|I| = \sum_{i=1}^{n} |I_k| = \sum_{i=1}^{n} |G/\,\mathrm{Stab}_G(i_k)|.$$

Lemma 2.2.4. *Let* G *be a finite group,* p *a prime and let* $|G| = p^k l$ *with* $k \in \mathbb{N}$, $l \in \mathbb{Z}^+$ *and* $p \nmid l$.

(a) If P *is a* p*-subgroup of* G, *then* $|P| \leq p^k$.

(b) If $S \leq G$ *with* $|S| = p^k$, *then* S *is a Sylow* p*-subgroup of* G.

Lemma 2.2.7 (Fixed-Point Formula)**.** *Let p be a prime and P a p-group acting on finite set I. Then*

$$|I| \equiv |\operatorname{Fix}_I(P)| \pmod{p}.$$

In particular, if $p \nmid |I|$, then P has a fixed-point on I.

Lemma 2.2.10. *Let G be a group and $(I, \diamond)$ a G-set.*

(a) $\diamond_{\mathcal{P}}$ is an action of G on $\mathcal{P}(I)$.

(b) Let $H \leq G$ and J be a H-invariant subset of I. Then $\diamond_{H,J}$ is an action of H on J.

Lemma 2.2.12. *Let G be a group, H a subgroup of G and $a \in G$.*

(a) aHa^{-1} is a subgroup of G isomorphic to H. So conjugate subgroups of G are isomorphic.

(b) If H is a p-subgroup of G for some prime p, so is aHa^{-1}.

Lemma 2.2.13. *Let G be a finite group and p a prime. Then*

$$\diamond: \quad G \times \operatorname{Syl}_p(G) \to \operatorname{Syl}_p(G), \quad (g, P) \to gPg^{-1}$$

is a well-defined action of G on $\operatorname{Syl}_p(G)$. This action is called the action of G on $\operatorname{Syl}_p(G)$ by conjugation.

Lemma 2.2.14 (Order Formula)**.** *Let A and B be subgroups of the group G.*

(a) Put $AB/B = \{gB \mid g \in AB\}$. The map

$$\phi: \quad A/A \cap B \to AB/B, \quad a(A \cap B) \to aB$$

is a well-defined bijection.

(b) If A and B are finite, then

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Theorem 2.2.15. *Let G be a finite group and p a prime.*

(a) (Second Sylow Theorem) *G acts transitively on $\operatorname{Syl}_p(G)$ by conjugation, that is any two Sylow p-subgroups of G are conjugate in G and so if S and T are Sylow p-subgroups of G, then $S = gTg^{-1}$ for some $g \in G$.*

(b) (Third Sylow Theorem) *The number of Sylow p-subgroups of G divides $|G|$ and is congruent to 1 modulo p.*

Lemma 2.2.16. *Let I be a set. Then $\operatorname{Sym}(n)$ acts on I^n via*

$$f \diamond (i_1, i_2, \ldots i_n) = (i_{f^{-1}(1)}, i_{f^{-1}(2)}, \ldots, i_{f^{-1}(n)}).$$

So if $i = (i_1, i_2, \ldots, i_n) \in I^n$ and $j = f \diamond i = (j_1, j_2, \ldots, j_n)$ then $j_{f(l)} = i_l$.

Theorem 2.2.17 (Cauchy's Theorem)**.** *Let G be a finite group and p a prime dividing the order of G. Then G has an element of order p.*

Proposition 2.2.18. *Let G be a finite group and p a prime. Then any p-subgroup of G is contained in a Sylow p-subgroup of G. In particular, G has a Sylow p-subgroup.*

Theorem 2.2.19 (First Sylow Theorem)**.** *Let G be a finite group, p a prime and $S \in \mathrm{Syl}_p(G)$. Let $|G| = p^k l$ with $k \in \mathbb{N}$, $l \in \mathbb{Z}^+$ and $p \nmid l$ (p^k is called the p-part of $|G|$). Then $|S| = p^k$. In particular,*

$$\mathrm{Syl}_p(G) = \{P \leq G \big| |P| = p^k\}$$

and G has a subgroup of order p^k.

Lemma 2.2.21. *Let G be a finite group and p a prime. Let S be a Sylow p-subgroup of G. Then S is normal in G if and only if S is the only Sylow p-subgroup of G.*

Lemma 2.2.22. *Let $\phi : A \to B$ be a homomorphism of groups. Then ϕ is 1-1 if and only of $\ker \phi = \{e_A\}$.*

Lemma 2.2.24. *Let G be a group and A, B normal subgroups of G with $A \cap B = \{e\}$. Then AB is a subgroup of G, $ab = ba$ for all $a \in A, b \in B$ and the map*

$$\phi : A \times B \to AB, (a, b) \to ab$$

is an isomorphism of groups. In particular,

$$AB \cong A \times B.$$

Lemma 2.2.25. *Let A be finite abelian groups. Let $p_1, p_2, \dots p_n$ be the distinct prime divisor of $|A|$ (and so $|A| = p_1^{m_1} \phi_2 m_2 \dots p_n^{m_k}$ for some positive integers m_i). Then for each $1 \leq i \leq n$, G has a unique Sylow p_i-subgroup A_i and*

$$A \cong A_1 \times A_2 \times \dots \times A_n.$$

Lemma 3.1.5. *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $\mathcal{L} = (v_1, \dots, v_n)$ a list of vectors in V. Then $\mathcal{L}$ is a basis for V if and only if for each $v \in V$ there exists uniquely determined $k_1, \dots, k_n \in \mathbb{K}$ with*

$$v = \sum_{i=1}^{m} k_i v_i.$$

Lemma 3.1.6. *Let $\mathbb{K}$ be field and V a $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \dots, v_n)$ be a list of vectors in V. Suppose the exists $1 \leq i \leq n$ such that v_i is linear combination of $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$. Then $\mathcal{L}$ is linearly dependent.*

Lemma 3.1.7. *Let $\mathbb{K}$ be field, V an $\mathbb{K}$-space and $\mathcal{L} = (v_1, v_2, \dots v_n)$ a finite list of vectors in V. Then the following three statements are equivalent:*

(a) $\mathcal{L}$ is basis for V.

(b) $\mathcal{L}$ is a minimal spanning list, that is $\mathcal{L}$ spans V but for all $1 \leq i \leq n$,

$$(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$$

does not span V.

(c) $\mathcal{L}$ is maximal linearly independent list, that is $\mathcal{L}$ is linearly independent, but for all $v \in V$, $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent.

Lemma 3.1.10. *Let $\mathbb{K}$ be a field and V and W be $\mathbb{K}$-spaces. Suppose that $(v_1, v_2, \ldots, v_n)$ is basis of V and let $w_1, w_2, \ldots w_n \in W$. Then*

(a) There exists a unique $\mathbb{K}$-linear map $f : V \to W$ with $f(v_i) = w_i$ for each $1 \leq i \leq n$.

(b) $f(\sum_{i=1}^n k_i v_i) = \sum_{i=1}^n k_i w_i$. for all $k_1, \ldots, k_n \in \mathbb{K}$.

(c) f is 1-1 if and only if $(w_1, w_2, \ldots, w_n)$ is linearly independent.

(d) f is onto if and only if $(w_1, w_2, \ldots, w_n)$ spans W.

(e) f is an isomorphism if and only if $(w_1, w_2, \ldots, w_n)$ is a basis for W.

Corollary 3.1.11. *Let $\mathbb{K}$ be a field and W a $\mathbb{K}$-space with basis $(w_1, w_2 \ldots, w_n)$. Then the map*

$$f : \mathbb{K}^n \to W, (a_1, \ldots a_n) \to \sum_{i=1}^n a_i w_i$$

is a $\mathbb{K}$-isomorphism. In particular,

$$W \cong_{\mathbb{K}} \mathbb{K}^n.$$

Proposition 3.1.13 (Subspace Proposition)**.** *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and W an $\mathbb{K}$-subspace of V.*

(a) Let $v \in V$ and $k \in \mathbb{K}$. Then $0_{\mathbb{K}} v = v$, $(-1_{\mathbb{K}})v = -v$ and $k0_V = 0_V$.

(b) W is a subgroup of V with respect to addition.

(c) W together with the restriction of the addition and scalar multiplication to W is a well-defined $\mathbb{K}$-space.

Proposition 3.1.14 (Quotient Space Proposition)**.** *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space and W a $\mathbb{K}$-subspace of V.*

(a) $V/W := \{v + W \mid v \in V\}$ *together with the addition*

$$+_{V/W}: \quad V/W \times V/W \to V/W, (u+V, v+W) \to (u+v)+W$$

and scalar multiplication

$$\diamond_{V/W}: \quad \mathbb{K} \times V/W \to V/W, (k, v+W) \to kv+W$$

is a well-defined vector space.

(b) The map $\phi : V \to V/W, v + W$ *is an onto and* $\mathbb{K}$*-linear. Moreover,* $\ker \phi = W$.

Lemma 3.1.15. *Let* $\mathbb{K}$ *be field,* V *a* $\mathbb{K}$*-space,* W *a subspace of* V*. Suppose that* $(w_1, \dots, w_l)$ *be a basis for* W *and let* $(v_1, \dots, v_l)$ *be a list of vectors in* V*. Then the following are equivalent*

(a) $(w_1, w_2, \dots, w_k, v_1, v_2, \dots v_l)$ *is a basis for* V.

(b) $(v_1 + W, v_2 + W, \dots, v_l + W)$ *is a basis for* V/W.

Lemma 3.1.16. *Let* $\mathbb{K}$ *be field,* V *a* $\mathbb{K}$*-space and* $(v_1, \dots, v_n)$ *and* $(w_1, \dots w_m)$ *be bases for* V*. Then* $n = m$.

Lemma 3.1.18. *Let* $\mathbb{K}$ *be a field and* V *an* $\mathbb{K}$*-space with a finite spanning list* $\mathcal{L} = (v_1, v_2, \dots, v_n)$*. Then some sublist of* $\mathcal{L}$ *is a basis for* V*. In particular,* V *is finite dimensional and* $\dim_{\mathbb{K}} V \leq n$.

Theorem 3.1.19 (Dimension Formula)**.** *Let* V *be a vector space over the field* $\mathbb{K}$*. Let* W *be an* $\mathbb{K}$*-subspace of* V*. Then* V *is finite dimensional if and only if both* W *and* V/W *are finite dimensional. Moreover, if this is the case, then*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

Corollary 3.1.20. *Let* V *be a finite dimensional vector space over the field* $\mathbb{K}$ *and* $\mathcal{L}$ *a linearly independent list of vectors in* V*. Then* $\mathcal{L}$ *is contained in a basis of* V *and so*

$$|\mathcal{L}| \leq \dim_{\mathbb{K}} V.$$

Lemma 3.2.3. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension. Then* $\mathbb{K}$ *is vector space over* $\mathbb{F}$*, where the scalar multiplication is given by*

$$\mathbb{F} \times \mathbb{K} \to \mathbb{K}, (f, k) \to fk$$

Lemma 3.2.6. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* V *a* $\mathbb{K}$*-space. Then with respect to the restriction of the scalar multiplication to* $\mathbb{F}$*,* V *is an* $\mathbb{F}$*-space. If* V *is finite dimensional over* $\mathbb{K}$ *and* $\mathbb{K} : \mathbb{F}$ *is finite, then* V *is finite dimensional over* $\mathbb{F}$ *and*

$$\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} V.$$

Corollary 3.2.7. *Let $\mathbb{E} : \mathbb{K}$ and $\mathbb{K} : \mathbb{F}$ be finite field extensions. Then also $\mathbb{E} : \mathbb{F}$ is a finite field extension and*

$$\dim_{\mathbb{F}} \mathbb{E} = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} \mathbb{E}.$$

Lemma 3.2.8. *Let $\mathbb{F}$ be a field and I a non-zero ideal in $\mathbb{F}[x]$.*

(a) There exists a unique monic polynomial $p \in \mathbb{F}[x]$ with $I = \mathbb{F}[x]p = (p)$.

(b) $F[x]/I$ is an integral domain if and only if p is irreducible and if and only if $F[x]/I$ is field.

Lemma 3.2.11. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$.*

(a) The map $\phi_a : \mathbb{F}[x] \to \mathbb{K}, f \to f(a)$ is a ring homomorphism.

(b) $\operatorname{Im} \phi_a = \mathbb{F}[a]$ is a subring of $\mathbb{K}$.

(c) ϕ_a is 1-1 if and only if $\ker \phi_a = \{0_{\mathbb{F}}\}$ and if and only if a is transcendental.

Theorem 3.2.12. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$. Suppose that a is transcendental over $\mathbb{F}$. Then*

(a) $\tilde{\phi}_a : \mathbb{F}[x] \to \mathbb{F}[a], f \to f(a)$ is an isomorphism of rings.

(b) For all $n \in \mathbb{N}$, $(1, a, a^2, \ldots, a^n)$ is linearly independent over $\mathbb{F}$.

(c) $\mathbb{F}[a]$ is not finite dimensional over $\mathbb{F}$ and $\mathbb{K} : \mathbb{F}$ is not finite.

(d) $a^{-1} \notin \mathbb{F}[a]$ and $\mathbb{F}[a]$ is not a subfield of $\mathbb{K}$.

Theorem 3.2.13. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$. Suppose that a is algebraic over $\mathbb{F}$. Then*

(a) There exists a unique monic polynomial $p_a \in \mathbb{F}[x]$ with $\ker \phi_a = (p_a)$.

(b) $\overline{\phi}_a : \quad \mathbb{F}[x]/(p_a) \to \mathbb{F}[a], \quad f + (p_a) \to f(a)$ is a well-defined isomorphism of rings.

(c) p_a is irreducible.

(d) $\mathbb{F}[a]$ is a subfield of $\mathbb{K}$.

(e) Let Put $n = \deg p_a$. Then $(1, a, \ldots, a^{n-1})$ is an $\mathbb{F}$-basis for $\mathbb{F}[a]$

(f) $\dim_{\mathbb{F}} \mathbb{F}[a] = \deg p_a$.

(g) Let $g \in \mathbb{F}[x]$. Then $g(a) = 0_{\mathbb{K}}$ if and only if $p_a \mid g$ in $\mathbb{F}[x]$.

Lemma 3.2.15. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Let $p \in \mathbb{F}[x]$. Then $p = p_a$ if and only of p is monic, and irreducible and $p(a) = 0_{\mathbb{F}}$.*

Lemma 3.2.17. *(a) Let $\alpha : R \to S$ and $\beta : S \to T$ be ring isomorphisms. Then*

$$\beta \circ \alpha : R \to T, r \to \beta(\alpha(r))$$

and

$$\alpha^{-1} : S \to R, s \to \alpha^{-1}(s)$$

are ring isomorphism.

(b) Let R and S be rings, I an ideal in R and $\alpha : R \to S$ a ring isomorphism. Put $J = \alpha(I)$. Then

- *(a) J is an ideal in S.*
- *(b) $\beta : I \to J, \quad i \to \alpha(i)$ is a ring isomorphism.*
- *(c) $\gamma : R/I \to S/J, \quad r + I \to \alpha(i) + J$ is a well-defined ring isomorphism.*
- *(d) $\alpha\big((a)\big) = \big(\alpha(a)\big)$ for all $a \in R$. That is α maps to ideal in R generated by a to the ideal in S generated in $\alpha(a)$.*

(c) Let R and S be commutative rings with identities and $\sigma : R \to S$ a ring isomorphism. Then

$$R[x] \to S[x], \quad \sum_{i=1}^{n} f_i x^i \to \sum_{i=1}^{n} \sigma(i) x^i$$

is a ring isomorphism. In the following, we will denote this ring isomorphism also by σ. So if $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}[x]$, then $\sigma(f) = \sum_{i=0}^{n} \sigma(f_i) x^i$.

Corollary 3.2.18. *Let $\sigma : \mathbb{K}_1 \to \mathbb{K}_2$ be a field isomorphism. For $i = 1, 2$ let $\mathbb{E}_i : \mathbb{K}_i$ be a field extension and suppose $a_i \in \mathbb{K}_i$ is algebraic over $\mathbb{K}_i$ with minimal polynomial p_i. Suppose that $\sigma(p_1) = p_2$. Then there exists a field isomorphism*

$$\check{\sigma} : \mathbb{K}_1[a_1] \to \mathbb{K}_2[a_2]$$

with

$$\rho(a_1) = a_2 \text{ and } \rho\mid_{\mathbb{K}_1} = \sigma$$

Lemma 3.3.3. *Any finite field extension is algebraic.*

Proposition 3.3.6. *Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$. Then there exists a splitting field $\mathbb{K}$ for f over $\mathbb{F}$. Moreover, $\mathbb{K} : \mathbb{F}$ is finite of degree at most $n!$.*

Theorem 3.3.7. *Suppose that*

(i) $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ is an isomorphism of fields;

(ii) For $i = 1$ and 2, $f_i \in \mathbb{F}[x]$ and $\mathbb{K}_i$ a splitting field for f_i over $\mathbb{F}_i$; and

(iii) $\sigma(f_1) = f_2$

Then there exists a field isomorphism

$$\breve{\sigma} : \mathbb{K}_1 \to \mathbb{K}_2 \text{ with } \breve{\sigma} \mid_{\mathbb{F}_1} = \sigma.$$

Suppose in addition that

(iv) *For* $i = 1$ *and* 2, p_i *is an irreducible factor of* f_i *in* $\mathbb{F}[x]$ *and* a_i *is a root of* p_i *in* $\mathbb{K}_i$*; and*

(v) $\sigma(p_1) = \sigma(p_2)$.

Then $\breve{\sigma}$ *can be chosen such that*

$$\sigma(a_1) = a_2.$$

Lemma 3.4.3. *Let* $\mathbb{K} : \mathbb{E}$ *and* $\mathbb{E} : \mathbb{F}$ *be a field extensions.*

(a) *Let* $a \in \mathbb{K}$ *be algebraic over* $\mathbb{F}$. *Then* a *is algebraic over* $\mathbb{E}$. *Moreover, if* $p_a^{\mathbb{E}}$ *is the minimal polynomial of* a *over* $\mathbb{E}$, *and* $p_a^{\mathbb{F}}$ *is the minimal polynomial of* a *over* $\mathbb{F}$, *then* $p_a^{\mathbb{E}}$ *divides* $p_a^{\mathbb{F}}$ *in* $\mathbb{E}[x]$.

(b) *If* $f \in \mathbb{F}[x]$ *is separable over* $\mathbb{F}$, *then* f *is separable over* $\mathbb{E}$.

(c) *If* $a \in \mathbb{K}$ *is separable over* $\mathbb{F}$, *then* a *is separable over* $\mathbb{E}$.

(d) *If* $\mathbb{K} : \mathbb{F}$ *is separable, then also* $\mathbb{K} : \mathbb{E}$ *and* $\mathbb{E} : \mathbb{K}$ *are separable.*

Lemma 3.5.2. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension. Then* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *is a subgroup of* $\mathrm{Sym}(\mathbb{K})$.

Lemma 3.5.5. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* H *a subset of* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. *Then* $\mathrm{Fix}_{\mathbb{K}}(H)$ *is subfield of* $\mathbb{K}$ *containing* $\mathbb{F}$.

Proposition 3.5.7. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* $0_{\mathbb{F}} \neq f \in \mathbb{F}[x]$.

(a) *Let* $a \in \mathbb{K}$ *and* $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. *Then* $\sigma(f(a)) = f(\sigma(a))$.

(b) *The set of roots of* f *in* $\mathbb{K}$ *is invariant under* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. *That is if* a *is a root of* f *in* $\mathbb{K}$ *and* $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K})$, *then* $\sigma(a)$ *is also a root of* f *in* $\mathbb{K}$.

(c) *Let* $a \in \mathbb{K}$. *Then* $\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a) = \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$.

(d) *Let* a *be root of* f *in* $\mathbb{K}$. *Then*

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})\}|.$$

Theorem 3.5.8. *Let* $\mathbb{F}$ *be a field and* $\mathbb{K}$ *the splitting field of a separable polynomial over* $\mathbb{F}$. *Then*

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{K}.$$

Lemma 3.5.10. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and G a finite subgroup of $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ with $\operatorname{Fix}_{\mathbb{K}}(G) = \mathbb{F}$. Then $\dim_{\mathbb{F}} \mathbb{K} \leq |G|$.*

Proposition 3.5.11. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and G a finite subgroup of $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ with $\operatorname{Fix}_{\mathbb{K}}(G) = \mathbb{F}$. Let $a \in \mathbb{K}$. Then a is algebraic over $\mathbb{F}$. Let $a_1, a_2, \ldots a_n$ be the distinct elements of $Ga = \{\sigma(a) \mid \sigma \in G\}$. Then*

$$p_a = (x - a_1)(x - a_2) \ldots (x - a_n).$$

In particular, p_a splits over $\mathbb{K}$ and $\mathbb{K}$ is separable over $\mathbb{F}$.

Theorem 3.5.13. *Let $\mathbb{K} : \mathbb{F}$ be a field extension. Then the following statements are equivalent.*

(a) $\mathbb{K}$ *is the splitting field of a separable polynomial over* $\mathbb{F}$.

(b) $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ *is finite and* $\mathbb{F} = \operatorname{Fix}_{\mathbb{K}}(\operatorname{Aut}_{\mathbb{F}}(\mathbb{K}))$.

(c) $\mathbb{F} = \operatorname{Fix}_{\mathbb{K}}(G)$ *for some finite subgroup* G *of* $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$.

(d) $\mathbb{K} : \mathbb{F}$ *is finite, separable and normal.*

Lemma 3.5.14. *Let $\mathbb{K} : \mathbb{F}$ be a field extension. Let $\sigma \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$ and let $\mathbb{E}$ be subfield field of $\mathbb{K}$ containing $\mathbb{F}$. Then*

$$\sigma \operatorname{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} = \operatorname{Aut}_{\sigma(\mathbb{E})}(\mathbb{K})$$

Lemma 3.5.16. *Let $\mathbb{K} : \mathbb{F}$ be a Galois extension and $\mathbb{E}$ an intermediate field of $\mathbb{K} : \mathbb{F}$. The following are equivalent:*

(a) $\mathbb{E} : \mathbb{F}$ *is normal.*

(b) $\mathbb{E} : \mathbb{F}$ *is Galois.*

(c) $\mathbb{E}$ *is invariant under* $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$, *that is* $\sigma(\mathbb{E}) = \mathbb{E}$ *for all* $\sigma \in \operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$.

Theorem 3.5.17 (Fundamental Theorem of Galois Theory)**.** *Let $\mathbb{K} : \mathbb{F}$ be a Galois Extension. Let $\mathbb{E}$ be an intermediate field of $\mathbb{K} : \mathbb{F}$ and $G \leq \operatorname{Aut}_{\mathbb{F}}(K)$.*

(a) The map

$$\mathbb{E} \to \operatorname{Aut}_{\mathbb{E}}(\mathbb{K})$$

is a bijection between to intermediate fields of $\mathbb{K} : \mathbb{F}$ and the subgroups of $\operatorname{Aut}_{\mathbb{F}}(\mathbb{K})$. The inverse of this map is given by

$$G \to \operatorname{Fix}_{\mathbb{K}}(G).$$

(b) $|G| = \dim_{\operatorname{Fix}_{\mathbb{K}}(G)} \mathbb{K}$ *and* $\dim_{\mathbb{E}} \mathbb{K} = |\operatorname{Aut}_{\mathbb{E}}(\mathbb{K})|$.

(c) $\mathbb{E} : \mathbb{F}$ *is normal if and only if* $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ *is normal in* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(d) If $\mathbb{E} : \mathbb{F}$ *is normal, then the map*

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) / \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \mathrm{Aut}_{\mathbb{F}}(\mathbb{E}), \sigma \, \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \sigma \mid_{\mathbb{E}}$$

is a well-defined isomorphism of groups.

Theorem A.1.3. *Let* $\sim$ *be an equivalence relation on the set* A *and* $a, b \in A$. *Then the following statements are equivalent:*

(a) $a \sim b$.

(b) $b \in [a]$.

(c) $[a] \cap [b] \neq \emptyset$.

(d) $[a] = [b]$.

(e) $a \in [b]$

(f) $b \sim a$.

Lemma A.2.3. *Let* $f : A \to B$ *and* $B \to C$ *be functions.*

(a) If f *and* g *are 1-1, so is* $g \circ f$.

(b) If f *and* g *are onto, so is* $g \circ f$.

(c) If f *and* g *is a bijection, so is* $g \circ f$.

Lemma A.2.5. *Let* $f : A \to B$ *be a function.*

(a) Let $C \subseteq A$. *Then* $C \subseteq f^{-1}(f(C))$.

(b) Let $C \subseteq A$. *If* f *is 1-1 then* $f^{-1}(f(C)) = C$.

(c) Let $D \subseteq B$. *Then* $f(f^{-1}(D)) \subseteq D$.

(d) Let $D \subseteq B$. *If* f *is onto then* $f(f^{-1}(D)) = D$.

Lemma A.2.6. *Let* $f : A \to B$ *be a function and suppose* $A \neq \emptyset$.

(a) f *is 1-1 if and only if there exists a function* $g : B \to A$ *with* $g \circ f = \mathrm{id}_A$.

(b) f *is onto if and only of there exists a function* $g : B \to A$ *with* $f \circ g = \mathrm{id}_B$.

(c) f *is a bijection if and only if there exists a function* $g : B \to A$ *with* $f \circ g = \mathrm{id}_B$ *and* $g \circ A = \mathrm{id}_B$.

Lemma A.3.2. *(a)* $\approx$ *is an equivalence relation.*

(b) If A *and* B *are sets with* $A \approx B$, *then* $A \prec B$.

(c) $\prec$ *is reflexive and transitive.*

(d) Let A *and* B *be sets. Then* $A \prec B$ *if and only if there exists* $C \subseteq B$ *with* $A \approx C$.

Lemma A.3.4. *Let A and B be sets.*

(a) $|A| = |B|$ *if and only if* $A \approx B$.

(b) $|A| \leq |B|$ *if and only if* $A \prec B$.

Theorem A.3.5 (Cantor-Bernstein)**.** *Let A and B be sets. Then $A \approx B$ if and only if $A \prec B$ and $B \prec A$.*

Corollary A.3.6. *Let c and d be cardinals. Then $c = d$ if and only if $c \leq d$ and $d \leq c$.*

Lemma A.3.9. *(a) Let A and B be countable sets. Then $A \times B$ is countable.*

(b) Let A be a countable set. Then B^n is countable for all positive integers n.

B.2 Definitions from the Lecture Notes

Definition 1.3.1. *Let S be a set. A binary operation is a function $* : S \times S \to S$. We denote the image of (s, t) under $*$ by $s * t$.*

Definition 1.3.3. *Let $*$ be a binary operation on a set I. Then $*$ is called* associative *if*

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in I$$

Definition 1.3.5. *Let I be a set and $*$ a binary operation on I. An* identity *of $*$ in I is a element $e \in I$ with $e * i = i$ and $i = i * e$ for all $i \in I$.*

Definition 1.3.8. *Let $*$ be a binary operation on the set I with identity e. The $a \in I$ is called* invertible *if there exists $b \in I$ with $a * b = e$ and $b * a = e$. Any such b is called an* inverse *of a with respect to $*$.*

Definition 1.3.11. *A* group *is tuple $(G, *)$ such that G is a set and*

(i) $* : G \times G \to G$ *is a binary operation.*

(ii) $*$ *is associative.*

(iii) $*$ *has an identity e in G.*

(iv) Each $a \in G$ is invertible in G with respect to $*$.

Definition 1.4.5. *Let G be a group, $a \in G$ and $n \in \mathbb{N}$. Then*

(a) $a^0 := e$,

(b) Inductively $a^{n+1} := a^n a$.

(c) $a^{-n} := (a^{-1})^n$.

(d) *We say that a has finite* order *if there exists a positive integer n with $a^n = e$. The smallest such positive integer is called the order of a and is denoted by $|a|$.*

Definition 1.5.1. *Let $(G, *)$ and $(H, \triangle)$ be groups. Then $(H, \triangle)$ is called a* subgroup *of $(G, *)$ provided that*

(a) $H \subseteq G$.

(b) $a \triangle b = a * b$ *for all* $a, b \in H$.

Definition 1.5.6. *Let I be a subset of the group G. Then*

$$\langle I \rangle = \bigcap_{I \subseteq H \leq G} H$$

$\langle I \rangle$ is called the subgroup of G generated by I

Definition 1.6.1. *Let $f : A \to B$ be a function. Then* $\operatorname{Im} f := \{f(a) \mid a \in A\}$. $\operatorname{Im} f$ *is called the* image *of f.*

Definition 1.6.3. *Let $(G, *)$ and $(H, \Box)$ be groups.*

(a) *A* homomorphism *from $(G, *)$ from to $(H, \Box)$ is a function $f : G \to H$ such that*

$$f(a * b) = f(a) \Box f(b)$$

for all $a, b \in G$.

(b) *An* isomorphism *from G to H is a 1-1 and onto homomorphism from G to H.*

(c) *If there exists an isomorphism from G to H we say that G is* isomorphic *to H and write $G \cong H$.*

Definition 1.6.6. *Let G be a group. Then G is called a* group of permutations *or a* permutation group *if $G \leq \operatorname{Sym}(I)$ for some set I.*

Definition 1.7.1. *Let K be a subgroup of the group G and $a, b \in G$. Then we say that a is* congruent *to b modulo K and write $a \equiv b \pmod{K}$ if $a^{-1}b \in K$.*

Definition 1.7.4. *Let $(G, *)$ be a group and $g \in G$*

(a) *Let A, B be subsets of G and $g \in G$. Then*

$$A * B := \{a * b \mid a \in A, b \in B\},$$

$$g * A = \{g * a \mid a \in A\}$$

and

$$A * g := \{a * g \mid a \in A\}.$$

We often just write AB, gA and Ag for $A * B, g * A$ and $A * g$.

(b) *Let K be a subgroup of the group $(G,*)$. Then $g*K$ called the* left coset *of g in G with respect to K. Put*

$$G/K := \{gK \mid g \in G\}.$$

So G/K is the set of left cosets of K in G.

Definition 1.7.13. *A group G is called* cyclic *if $G = \langle g \rangle$ for some $g \in G$.*

Definition 1.8.2. *Let N be a subgroup of the group G. N is called a* normal *subgroup of G and we write $N \trianglelefteq G$ provided that*

$$gN = Ng$$

for all $g \in G$.

Definition 1.8.4. *A binary operation $*$ on I is called* commutative *if $a * b = b * a$ for all $a, b \in I$. A group is called* abelian *of its binary operation is commutative.*

Definition 1.8.9. *Let G be a group and $N \trianglelefteq G$. Then $*_{G/N}$ denotes the binary operation*

$$*_{G/N} : G/N \times G/N \to G/N, \quad (S,T) \to S * T$$

Note here that by 1.8.8(a), $S * T$ is a coset of N, whenever S and T are cosets of N. G/N is called the quotient group *of G with respect to N.*

Definition 1.9.1. *Let $\phi : G \to H$ be a homomorphism of groups. Then*

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\}.$$

$\ker \phi$ *is called the* kernel *of ϕ.*

Definition 1.9.7. *Let $*$ be a binary operation on the set A and $\Box$ a binary operation on the set B. Then $*\times\Box$ is the binary operation on $A \times B$ defined by*

$$*\times\Box : (A \times B) \times (A \times B) \to A \times B, \quad ((a,b),(c,d)) \to (a * c, b \Box d)$$

$(A \times B,\ *\times\Box)$ *is called the* direct product *of $(A,*)$ and $(B,\Box)$.*

Definition 2.1.1. *Let G be group and I a set. An* action *of G on I is a function*

$$\diamond : \quad G \times I \to I \quad (g,i) \to (g \diamond i)$$

such that

(act:i) $e \diamond i = i$ *for all $i \in I$.*

(act:ii) $g \diamond (h \diamond i) = (g * h) \diamond i$ *for all $g, h \in G$, $i \in I$.*

The pair $(I, \diamond)$ is called a G-set. *We also say that G acts on I via $\diamond$. Abusing notations we often just say that I is a G-set. Also we often just write gi for $g \diamond i$.*

Definition 2.1.8. *Let G be a group and $(I, \diamond)$ a G-set.*

(a) *The relation $\equiv_\diamond \pmod G$ on I is defined by $i \equiv_\diamond j \pmod G$ if there exists $g \in G$ with $gi = j$.*

(b) *$G \diamond i := \{g \diamond i \mid g \in G\}$. $G \diamond i$ is called the* orbit *of G on I (with respect to $\diamond$) containing i. We often write Gi for $G \diamond i$.*

Definition 2.1.12. *Let G be a group acting on the set I. We say that G acts* transitively *on I if for all $i, j \in G$ there exists $g \in G$ with $gi = j$.*

Definition 2.1.14. *(a) Let G be a group and $(I, \diamond)$ and $(J, \Box)$ be G-sets. A function $f : I \to J$ is called* G-homomorphism *if*

$$f(a \diamond i) = a \Box f(i)$$

for all $a \in G$ and i. A G-isomorphism *is bijective G-homomorphism. We say that I and H are G-isomorphic and write*

$$I \cong_G J$$

if there exists an G-isomorphism from I to J.

(b) *Let I be a G set and $J \subseteq I$. Then*

$$\mathrm{Stab}_G^\diamond(J) = \{g \in G \mid gj = j \text{ for all } j \in J\}$$

and for $i \in I$

$$\mathrm{Stab}_G^\diamond(i) = \{g \in G \mid gi = i\}$$

$\mathrm{Stab}_G^\diamond(i)$ *is called the* stabilizer *of i in G with respect to $\diamond$.*

Definition 2.2.1. *Let p be a prime and G a group. Then G is a* p-group *if $|G| = p^k$ for some $k \in \mathbb{N}$.*

Definition 2.2.3. *Let G be a finite group and p a prime. A* p-subgroup *of G is a subgroup of G which is a p-group. A* Sylow p-subgroup *of G is a maximal p-subgroup of G, that is S is a Sylow p-subgroup of G provided that*

(i) *S is a p-subgroup of G.*

(ii) *If P is a p-subgroup of G with $S \leq P$, then $S = P$.*

$\mathrm{Syl}_p(G)$ *denotes the set of Sylow p-subgroups of G.*

Definition 2.2.6. *Let G be a group acting on a set I. Let $i \in I$. Then i is called a* fixed-point *of G on I provided that $gi = i$ for all $g \in G$. $\mathrm{Fix}_I(G)$ is the set of all fixed-points for G on I. So*

$$\mathrm{Fix}_I(G) = \{i \in I \mid gi = i \text{ for all } g \in G\}.$$

Definition 2.2.9. *Let G be a group and $(I, \diamond)$ a G-set.*

(a) $\mathcal{P}(I)$ is the sets of all subsets of $\mathcal{I}$. $\mathcal{P}(I)$ is called the power set *of I.*

(b) For $a \in G$ and $J \subseteq I$ put $a \diamond J = \{a \diamond j \mid j \in J\}$.

(c) $\diamond_{\mathcal{P}}$ denotes the function

$$\diamond_{\mathcal{P}} : \quad G \times \mathcal{P}(I) \to \mathcal{P}(I), \quad (a, J) \to a \diamond J$$

*(d) Let J be a subset of I and $H \leq G$. Then J is called H-*invariant *if*

$$hj \in J$$

for all $h \in H, j \in J$.

(e) Let $H \leq G$ and J be a H-invariant. Then $\diamond_{H,J}$ denotes the function

$$\diamond_{H,J} : \quad H \times J \to J, \quad (h, j) \to h \diamond j$$

Definition 2.2.11. *Let A and B be subsets of the group G. We say that A is* conjugate *to B in G if there exists $g \in G$ with $A = gBg^{-1}$.*

Definition 3.1.1. *Let $\mathbb{K}$ be a field. A* vector space *over $\mathbb{K}$ (or a $\mathbb{K}$-space) is a tuple $(V, +, \diamond)$ such that*

(i) $(V, +)$ is an abelian group.

(ii) $\diamond : \mathbb{K} \times V \to V$ is a function called scalar multiplication *.*

(iii) $a \diamond (v + w) = (a \diamond v) + (a \diamond w)$ for all $a \in \mathbb{K}, v, w \in V$.

(iv) $(a + b) \diamond v = (a \diamond v) + (b \diamond v)$ for all $a, b \in \mathbb{K}, v \in V$.

(v) $(ab) \diamond v = a \diamond (b \diamond v)$ for all $a, b \in \mathbb{K}, v \in V$.

(vi) $1_{\mathbb{K}} \diamond v = v$ for all $v \in V$

The elements of a vector space are called vectors*. The usually just write kv for $k \diamond v$.*

Definition 3.1.3. *Let $\mathbb{K}$ be a field and V and $\mathbb{K}$-space. Let $\mathcal{L} = (v_1, \ldots, v_n) \in V^n$ be a list of vectors in V.*

(a) *$\mathcal{L}$ is called* $\mathbb{K}$-linearly independent *if*

$$a_1v_1 + av_2 + \dots av_n = 0_V$$

for some $a_1, a_2, \dots, a_n \in \mathbb{K}$ implies $a_1 = a_2 = \dots = a_n = 0_{\mathbb{K}}$.

(b) *Let $(a_1, a_2 \dots, a_n) \in \mathbb{K}^n$. Then $a_1v_1 + a_2v_2 + \dots + a_nv_n$ is called a* $\mathbb{K}$-linear combination *of $\mathcal{L}$.*

$$\operatorname{Span}_{\mathbb{K}}(\mathcal{L}) = \{a_1v_1 + a_2v_2 + \dots a_nv_n \mid (a_1, \dots, a_n) \in \mathbb{K}^n\}$$

is called the $\mathbb{K}$-span *of $\mathcal{L}$. So $\operatorname{Span}_{\mathbb{K}}(\mathcal{L})$ consists of all the $\mathbb{K}$-linear combination of $\mathcal{L}$. We consider 0_V to be a linear combination of the empty list $()$ and so $\operatorname{Span}_{\mathbb{K}}\big(()\big) = \{0_V\}$.*

(c) *We say that $\mathcal{L}$* spans *V, if $V = \operatorname{Span}_{\mathbb{K}}(\mathcal{L})$, that is if every vector in V is a linear combination of $\mathcal{L}$.*

(d) *We say that $\mathcal{L}$ is a* basis *of V if $\mathcal{L}$ is linearly independent and spans V.*

(e) *We say that $\mathcal{L}$ is a* linearly dependent *if it's not linearly independent, that is, if there exist $k_1, \dots, k_n \in \mathbb{K}$, not all zero such that*

$$k_1v_1 + kv_2 + \dots kv_n = 0_V.$$

Definition 3.1.8. *Let $\mathbb{K}$ be a field and V and W $\mathbb{K}$-spaces. A* $\mathbb{K}$-linear map from V to W is function

$$f : V \to W$$

such that

(a) $f(u + v) = f(u) + f(v)$ for all $u, v \in W$

(b) $f(kv) = kf(v)$ for all $k \in \mathbb{K}$ and $v \in V$.

A $\mathbb{K}$-linear map is called a $\mathbb{K}$-*isomorphism* if it's 1-1 and onto.

We say that V and W are $\mathbb{K}$-isomorphic and write $V \cong_{\mathbb{K}} W$ if there exists a $\mathbb{K}$-isomorphism from V to W.

Definition 3.1.12. *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and $W \subseteq V$. Then W is called a* $\mathbb{K}$-subspace *of V provided that*

(i) $0_V \in W$.

(ii) $v + w \in W$ for all $v, w \in W$.

(iii) $kw \in W$ for all $k \in \mathbb{K}$, $w \in W$.

Definition 3.1.17. *A vector space V over the field $\mathbb{K}$ is called* finite dimensional *if V has a finite basis $(v_1, \dots, v_n)$. n is called the* dimension *of $\mathbb{K}$ and is denoted by $\dim_{\mathbb{K}} V$. (Note that this is well-defined by 3.1.16).*

Definition 3.2.1. *Let $\mathbb{K}$ be a field and $\mathbb{F}$ a subset of $\mathbb{K}$. $\mathbb{F}$ is a called a* subfield *of $\mathbb{K}$ provided that* *(i)* $a + b \in \mathbb{F}$ *for all* $a, b \in \mathbb{F}$.

(ii) $0_{\mathbb{K}} \in \mathbb{F}$.

(iii) $-a \in \mathbb{F}$ *for all* $a \in \mathbb{F}$.

(iv) $ab \in \mathbb{F}$ *for all* $a, b \in \mathbb{F}$.

(v) $1_{\mathbb{K}} \in \mathbb{F}$.

(vi) $a^{-1} \in \mathbb{F}$ *for all* $a \in \mathbb{F}$ *with* $a \neq 0_{\mathbb{K}}$.

If $\mathbb{F}$ *is a subfield of* $\mathbb{K}$ *we also say that* $\mathbb{K}$ *is an* extension field *of* $\mathbb{F}$ *and that* $\mathbb{K} : \mathbb{F}$ *is a field extension.*

Definition 3.2.4. *A field extension* $\mathbb{K} : \mathbb{F}$ *is called* finite *if* $\mathbb{K}$ *is a finite dimensional* $\mathbb{F}$-*space..* $\dim_{\mathbb{F}} \mathbb{K}$ *is called the* degree *of the extension* $\mathbb{K} : \mathbb{F}$.

Definition 3.2.9. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* $a \in \mathbb{K}$.

(a) $\mathbb{F}[a] = \{f(a) \mid f \in \mathbb{F}[x]\}$.

(b) If there exists a non-zero $f \in F[x]$ *with* $f(a) = 0_{\mathbb{F}}$ *then* a *is called* algebraic *over* $\mathbb{F}$. *Otherwise* a *is called transcendental over* $\mathbb{F}$.

Definition 3.2.14. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and let* $a \in \mathbb{F}$ *be algebraic over* $\mathbb{F}$. *The unique monic polynomial* $p_a \in \mathbb{F}[x]$ *with* $\ker \phi_a = (p_a)$ *is called the* minimal polynomial *of* a *over* $\mathbb{F}$.

Definition 3.3.1. *A field extension* $\mathbb{K} : \mathbb{F}$ *is called* algebraic *if each* $k \in \mathbb{K}$ *is algebraic over* $\mathbb{F}$.

Definition 3.3.4. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* $a_1, a_2 \ldots, a_n \in \mathbb{K}$. *Inductively, define* $\mathbb{F}[a_1, \alpha_2, \ldots, a_k] := \mathbb{F}[a_1, a_2, \ldots, a_{k-1}][a_k]$.

Definition 3.3.5. *Let* $\mathbb{K} : \mathbb{F}$ *be field extensions and* $f \in \mathbb{F}[x]$. *We say that* f splits *in* $\mathbb{K}$ *if there exists* $a_1 \ldots a_n \in \mathbb{K}$ *with*

(i) $f = \mathrm{lead}(f)(x - a_1)(x - a_2) \ldots (x - a_n)$.

We say that $\mathbb{K}$ *is a* splitting field *for* f *over* $\mathbb{F}$ *if* f *splits in* $\mathbb{K}$ *and*

(ii) $\mathbb{K} = \mathbb{F}[a_1, a_2, \ldots, a_n]$.

Definition 3.4.1. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension.*

(a) Let $f \in \mathbb{F}[x]$. *If* f *is irreducible, then* f *is called* separable *over* $\mathbb{F}$ *provided that* f *does not have a double root in its splitting field over* $\mathbb{F}$. *In general,* f *is called separable over* $\mathbb{F}$ *provided that all irreducible factors of* f *in* $\mathbb{F}[x]$ *are separable over* $\mathbb{F}$.

(b) $a \in \mathbb{K}$ *is called separable over* $\mathbb{K}$ *if* a *is algebraic over* $\mathbb{F}$ *and the minimal polynomial of* a *over* $\mathbb{F}$ *is separable over* $\mathbb{F}$.

(c) $\mathbb{K} : \mathbb{F}$ *is called separable over* $\mathbb{F}$ *if each* $a \in \mathbb{K}$ *is separable over* $\mathbb{F}$.

Definition 3.5.1. *Let* $\mathbb{K} : \mathbb{F}$ *be field extension.* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *is the set of all field isomorphism* $\alpha : \mathbb{K} \to \mathbb{K}$ *with* $\alpha \mid_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.

Definition 3.5.4. *Let* $\mathbb{K} : \mathbb{F}$ *be a field extension and* $H \subseteq \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$. *Then*

$$\mathrm{Fix}_{\mathbb{K}}(H) := \{k \in \mathbb{K} \mid \sigma(k) = k \textit{ for all } \sigma \in H\}.$$

$\mathrm{Fix}_{\mathbb{K}}(H)$ *is called the* fixed-field *of* H *in* $\mathbb{K}$.

Definition 3.5.12. *Let* $\mathbb{K} : \mathbb{F}$ *be algebraic field extension. Then* $\mathbb{K} : \mathbb{F}$ *is called* normal *if for each* $a \in \mathbb{K}$, p_a *splits over* $\mathbb{K}$.

Definition 3.5.15. *(a) A* Galois *extension is a finite, separable and normal field extension.*

(b) Let $\mathbb{K} : \mathbb{F}$ *be a field extension. An* intermediate *field of* $\mathbb{K} : \mathbb{F}$ *is a subfield* $\mathbb{E}$ *of* $\mathbb{K}$ *with* $\mathbb{F} \subseteq \mathbb{E}$.

Definition A.1.1. *Let* $\sim$ *be a relation on a set* A. *Then*

(a) $\sim$ *is called* reflexive *if* $a \sim a$ *for all* $a \in A$.

(b) $\sim$ *is called* symmetric *if* $b \sim a$ *for all* $a, b \in A$ *with* $a \sim b$.

(c) $\sim$ *is called* transitive *if* $a \sim c$ *for all* $a, b, c \in A$ *with* $a \sim b$ *and* $b \sim c$.

(d) $\sim$ *is called an* equivalence relation *if* $\sim$ *is reflexive, symmetric and transitive.*

(e) For $a \in A$ *we define* $[a]_\sim := \{b \in R \mid a \sim b\}$. *We often just write* $[a]$ *for* $[a]_\sim$. *If* $\sim$ *is an equivalence relation then* $[a]_\sim$ *is called the* equivalence class *of* $\sim$ *containing* a.

Definition A.2.1. *Let* $f : A \to B$ *be a function.*

(a) f *is called* 1-1 *or* injective *if* $a = c$ *for all* $a, c \in A$ *with* $f(a) = f(c)$.

(b) f *is called* onto *or* surjective *if for all* $b \in B$ *there exists* $a \in A$ *with* $f(a) = b$.

(c) f *is called a* 1-1 correspondence *or* bijective *if for all* $b \in B$ *there exists a unique* $a \in A$ *with* $f(a) = b$.

(d) $\mathrm{Im}\, f := \{f(a) \mid a \in A\}$. $\mathrm{Im}\, f$ *is called the* image *of* f.

□

Definition A.2.2. *(a) Let* A *be a set. The* identity function id_A *on* A *is the function*

$$\mathrm{id}_A : A \to A, \quad a \to a.$$

(b) Let $f : A \to B$ *and* $g : B \to C$ *be function. Then* $g \circ f$ *is the function*

$$g \circ f : A \to C, \quad a \to g(f(a)).$$

$g \circ f$ *is called the* composition *of* g *and* f.

Definition A.2.4. *Let $f : A \to B$ be a function.*

(a) If $C \subseteq A$, then $f(C) := \{f(c) \mid c \in C\}$. $f(C)$ is called the image *of C under f.*

(b) If $D \subseteq B$, then $f^{-1}(D) := \{c \in C \mid f(c) \in D\}$. $f^{-1}(D)$ is called the inverse image *of D under f.*

Definition A.3.1. *Let A and B be sets. We write $A \approx B$ if there exists a bijection from A to B. We write $A \prec B$ if there exists injection from A to B.*

Definition A.3.3. *Let A be a set. Then $|A|$ denotes the equivalence class of $\approx$ containing. An* cardinal *is a class of the form $|A|$, A a set. If a, b are cardinals then we write $a \leq b$ if there exist sets A and B with $a = |A|$, $b = |B|$ and $A \prec B$.*

Definition A.3.7. *Let I be a set. Then I is called* finite *if the exists $n \in \mathbb{N}$ and a bijection $f : I \to \{1, 2, \ldots, n\}$. I is called* countable *if either I is finite or there exists a bijections $f : I \to \mathbb{Z}^+$.*

B.3 Definitions from the Homework

Definition H1.8. *Let I be a set.*

(a) For $a \in \mathrm{Sym}(I)$ define

$$\mathrm{Supp}(a) := \{i \in I \mid a(i) \neq i\}$$

$\mathrm{Supp}(a)$ *is called the* support *of a.*

(b) $\mathrm{FSym}(I) := \{a \in \mathrm{Sym}(I) \mid \mathrm{Supp}(a) \textit{ is finite }\}$.

$\mathrm{FSym}(I)$ *is called the* finitary symmetric group *on I.*

Definition H2.4. *Let G be a group and $a \in G$. Put*

$$C_G(a) := \{g \in G \mid ga = ag\}$$

$C_G(a)$ *is called the* centralizer *of a in G.*

Definition HPMT.3. *A group G is called* perfect *if $G = H$ for any $H \trianglelefteq G$ with G/H abelian.*

Definition HRMT.4. *A group G is called* simple *if $\{e\}$ and G are the only normal subgroups of G.*

Definition H8.6. *Let G be a group. Put*

$$Z(G) = \{a \in G \mid ab = ba \textit{ for all } b \in G$$

$Z(G)$ *is called the* center *of G.*

Definition H11.2. *Let $\mathbb{K} : \mathbb{F}$ be a field extension and $a \in \mathbb{K}$. Then*

$$\mathbb{F}(a) = \{xy^{-1} \mid x, y \in \mathbb{F}[a], y \neq 0_{\mathbb{K}}\}$$

Bibliography

[Hung] T.W. Hungerford *Abstract Algebra, An Introduction* second edition, Brooks/Cole **1997**.

[Lang] S. Lang *Algebra* Addison-Wesley **1978**

[Lay] D.C. Lay *Linear Algebra And Its Application* third edition, Addison Wesley **2003**

[Levy] A. Levy *Basic Set Theory* Springer **1979**

[310] U. Meierfrankenfeld *MTH 310 Lecture Notes* **2005**, http://www.math.msu.edu/∼meier/Classnotes/MTH310F05/abstract.html