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

April 28, 2017

Contents

1 Groups **5**
1.1 Sets 5
1.2 Functions and Relations 7
1.3 Definition and Examples 10
1.4 Basic Properties of Groups 16
1.5 Subgroups 21
1.6 Homomorphisms 26
1.7 Lagrange's Theorem 31
1.8 Normal Subgroups 38
1.9 The Isomorphism Theorems 44

2 Group Actions and Sylow's Theorem **63**
2.1 Group Action 63
2.2 Sylow's Theorem 75

3 Field Extensions **87**
3.1 Vector Spaces 87
3.2 Simple Field Extensions 98
3.3 Splitting Fields 106
3.4 Separable Extension 109
3.5 Galois Theory 110

A Sets **125**
A.1 Equivalence Relations 125
A.2 Bijections 127
A.3 Cardinalities 129

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

$$B \in B \quad \overset{\text{Definition of } B}{\iff} \quad B \text{ is nice} \quad \overset{\text{Definition of nice}}{\iff} \quad B \notin B.$$

which contradicts the basis property of a set.

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.

Theorem 1.1.1. *Let A and B be sets, then $A = B$ if and only if for all objects d*

$$d \in A \quad \iff d \in B$$

Theorem 1.1.2. (a) *Given an object s. Then there exists a set, denoted by $\{s\}$, such tat*

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

(b) *Let A and B be sets. Then there exists a set, called the unions of A and B and denoted by $A \cap B$ such that*

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

(c) *Let A and B be sets. Then there exists a set, called the intersection of A and B and denoted by $A \cap B$ such that*

$$\text{For all objects } x : x \in A \cap B \text{ if and only if } x \in A \text{ and } x \in B.$$

(d) *Let A and B be sets. The there exists a set, called A removed B and denoted by $A \setminus B$ such that*

$$\text{For all objects } x : x \in A \setminus B \text{ if and only if } x \in A \text{ and } x \notin B.$$

(e) *There exists a set, denote called* empty set *and denote by $\{\}$ or $\varnothing$, such that*

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

(f) *Let a, b be objects. Then there exists a set, denoted by $\{a, b\}$, such that*

$$x \in \{a, b\} \quad \text{if and only if} \quad x = a \text{ or } x = b.$$

Proof. (a) and (b): These are axioms of set theory.

(c) and (d) follow from the so called Replacement Axiom of set theory.

(e) One axiom of set theory guarantees the existence of a set A. Then one can define

$$\varnothing := A \setminus A$$

(f) Define

$$\{a, b\} := \{a\} \cup \{b\}.$$

□

Definition 1.1.3. *The* natural numbers *are defined as follows:*

$$\begin{array}{rcrcrcr}
0 & := & & & & & \varnothing \\
1 & := & 0 \cup \{0\} & = & \{0\} & = & \{\varnothing\} \\
2 & := & 1 \cup \{1\} & = & \{0,1\} & = & \{\varnothing, \{\varnothing\}\} \\
3 & := & 2 \cup \{2\} & = & \{0,1,2\} & = & \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\
4 & := & 4 \cup \{4\} & = & \{0,1,2,3\} & = & \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
n+1 & := & n \cup \{n\} & = & \{0,1,2,3,\ldots n\} & &
\end{array}$$

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

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

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

Theorem 1.2.1 (Principal of Substitution)**.** *Let* $\Phi(x)$ *be formula involving a variable* x*. For an object* d *let* $\Phi(d)$ *be the formula obtained from* $\Phi(x)$ *by replacing all occurrences of* x *by* d*. If* a *and* b *are objects with* $a = b$*, then* $\Phi(a) = \Phi(b)$*.*

Proof. See your favorite logic book □

Example 1.2.2. Let $\Phi(x) = x^2 + 3 \cdot x + 9$. If $a = 2$, then the Principal of Substitution gives

$$a^2 + 3 \cdot a + 9 = 2^2 + 3 \cdot 2 + 9.$$

We now introduce two important notations which we will use frequently to construct new sets from old ones.

Theorem 1.2.3. *Let* $I_1, I_2, \dots I_n$ *be sets and let* $\Phi(x_1, \dots, x_n)$ *be some formula involving the variables* $x_1, \dots x_n$*. Then there exists a set, denoted by*

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

such that for all objects y*,*

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

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* $x = \Phi(i_1, i_2, \dots, i_n)$.

Example 1.2.4. (1) $\{2a \mid a \in \mathbb{Z}\}$ is the set of even integers.

(2) $\{3a + b \mid a \in \mathbb{Z}, b \in \{1, 2\}\}$ is the set of integers which are not divisible by 3.

Theorem 1.2.5. *Let* I *be a set and* $P(x)$ *a statement involving the variable* x*. Then there exists a set, denoted by*

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

such that for all objects a*,*

$$a \in \{i \in I \mid P(i)\} \quad \textit{if and only if} \quad b \in I \textit{ and } P(a) \textit{ is true}$$

Example 1.2.6.

$$\{n \in \mathbb{Z} \mid n^2 = 1\} = \{-1, 1\}$$

Definition 1.2.7. *Let a,b and c be objects.*

(a) *The* ordered pair (a,b) *is defined as* $(a,b) := \{\{a\},\{a,b\}\}$.

(b) *The ordered triple* (a,b,c) *is defined as*

$$(a,b,c) := \big((a,b),c\big)$$

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 1.2.8. (a) *Let a be an object. Then* $\{a,a\} = \{a\}$.

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

Proof. (a):

$$\begin{aligned} & x \in \{a,a\} \\ \iff & x = a \text{ or } x = a \\ \iff & x = a \\ \iff & x \in \{a\} \end{aligned}$$

So 1.1.1 shows that $\{a,a\} = \{a\}$.

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

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

Proposition 1.2.9. *Let a,b,c,d be objects. Then*

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

Proof. $\Longrightarrow$: Suppose that $(a,b) = (c,d)$. The definition of an ordered pair gives

$$(*) \qquad \{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}.$$

Since $\{a\} \in \{\{a\},\{a,b\}\}$ the Principal of Substitution implies

$$\{a\} \in \{\{c\},\{c,d\}\},$$

Thus

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

In the first case we get $a \in \{c\}$ and so $a = c$. In the second case we get $c \in \{a\}$. So $c = a$ and again $a = c$.

Since $a = c$ we can apply the Principal of Substitution to the formula (*) and conclude:

$$\{\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, d\}.$$

Now 1.2.8 shows that

$$\{a, b\} = \{a, d\}$$

Applying 1.2.8 one more time gives $b = d$.

$\Longleftarrow$: Suppose $a = c$ and $b = d$. Then the Principal of Substitution gives $(a, b) = (c, d)$. □

Definition 1.2.10. *Let I and J be sets.*

(a) $I \times J := \{(i, j) \mid i \in I, j \in J\}$.

(b) *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 $(i, j) \in R$.*

(c) *A relation $r = (I, J, R)$ is called* 1-1 *if $i = k$ whenever $i, k \in I$ and $j \in R$ with irj and krj.*

(d) *A relation $r = (I, J, R)$ is called* onto *if for each $j \in I$ there exists $i \in I$ with irj.*

(e) *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 $f(i)$.*

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

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

(f) *A function f is called bijective, it its is a 1-1 and onto.*

(g) *A permutation of I is a bijective function $f : I \to I$.*

(h) *Let $f : I \to J$ and $g : J \to K$ be 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 $i \in I$.*

Example 1.2.11. (1) 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 $0, 1, 2, 3, \ldots, m-1$.

(2)

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

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

Remark 1.2.12. (a) *Let $f = (I, J, R)$ be a function. Then for all $i \in I$, $j \in J$:*

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

(b) *A function $f : I \to J$ is bijective if and only if for each $j \in J$ there exists a unique $i \in I$ with $f(i) = j$.*

Remark 1.2.13. *Let I, J, K be sets and $F(x)$ and $G(x)$ be a formulas involving the variable x. Define $R := \{(F(k), G(k)) \mid k \in K\}$ and $f := (I, J, R)$. Suppose that*

(i) *For all $i \in I$ there exist $k \in K$ with $i = F(k)$.*

(ii) *If $k, l \in K$ with $F(k) = F(l)$, then $G(k) = G(l)$.*

(iii) *If $k \in K$, then $F(k) \in I$ and $G(k) \in J$.*

Then f is a function from I to J. We call f a well-defined function and denote f by

$$f : \quad I \to J, \quad F(k) \mapsto G(k), \quad (k \in K)$$

Example 1.2.14. (1)

$$f : \quad \mathbb{Z}_3 \to \mathbb{Z}_9, \quad [n]_3 \mapsto [3n]_9, \quad (n \in \mathbb{Z})$$

is well-defined function. (Here for $n, m \in \mathbb{Z}$, $[n]_m$ is the congruence class of n modulo m.)

Indeed if $[n]_3 = [m]_3$, then 3 divides $n - m$. So 9 divides $3(n - m)$. Thus 9 divides $3n - 3m$. Hence $[3n]_9 = [3m]_9$ and so f is well-defined.

(2)

$$f : \quad \mathbb{Z}_3 \to \mathbb{Z}_9, \quad [n]_3 \mapsto [3n]_9, \quad (n \in \mathbb{Z})$$

is not a function, since its not well-defined:

$$[0]_3 = [3]_3, \quad [3 \cdot 0]_8 = [0]_8, \quad [3 \cdot 3]_8 = [9]_8$$

So $[3 \cdot 0]_8 \neq [3 \cdot 3]_8$ and f is not well-defined.

1.3 Definition and Examples

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

Definition 1.3.2. *Let $*$ be a binary operation on the set I.*

(a) *$*$ is called* associative *if*

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

for all $a, b, c \in I$.

(b) *An* identity *of $*$ is an element $e \in I$ with*

$$e * i = i \quad \text{and} \quad i = i * e$$

for all $i \in I$.

(c) *Suppose e is an identity of $*$. Let $a \in I$. An element b of I is called an* inverse *of a with respect to $*$ provided that*

$$a * b = e \quad \textit{and} \quad b * a = e.$$

If there exists an inverse *of a, then a is called* invertible *with respect to $*$.*

Definition 1.3.3. *A* group *is pair $(G, *)$ such that G is a set and*

(i) *$*$ is a binary operation on G.*

(ii) *$*$ is associative.*

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

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

Example 1.3.4. (1)

$$+: \quad \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (n, m) \mapsto n + m$$

is a binary operation. $+$ is associative, 0 is a identity of $+$ and $-n$ is a inverse of n with respect to $+$. So $(\mathbb{Z}, +)$ is a group.

(2)

$$\cdot: \quad \mathbb{Z} \times \mathbb{Z}, \quad (n, m) \mapsto nm$$

is a binary operation. $\cdot$ is associative, 1 is an identity of $\cdot$, but 2 does not have an inverse with respect to $\cdot$. So $(\mathbb{Z}, \cdot)$ is not a group.

(3)

$$\cdot: \quad \mathbb{Q} \times \mathbb{Q}, \quad (n, m) \mapsto nm$$

is a binary operation. $\cdot$ is associative, 1 is an identity of $\cdot$, but 0 does not have an inverse with respect to $\cdot$. So $(\mathbb{Q}, \cdot)$ is not a group.

(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. $*$ is not associative. For example

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

Suppose that x is an identity of $*$ in 1.3.4(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 $x = b$. Since $y * x = x$ for all $y \in I$ column x must be equal to the header column. But column b is not equal to the header column. case. Hence $*$ does not have an identity. In particular, $(I, *)$ is not a group.

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

No row of the multiplication table is equal to the header row. Thus $\square$ does not have an identity. In particular, $(I, \square)$ is not a group.

(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)

$$\diamond : \quad \mathbb{Z}_3 \times \mathbb{Z}_3, \quad ([a]_3, [b]_3) \mapsto \left[a^{b^2+1}\right]_3, \quad (a, b) \in \mathbb{Z} \times \mathbb{Z}$$

is not a binary operation. Indeed we have $[0]_3 = [3]_3$ but

$$\left[(-1)^{0^2+1}\right]_3 = \left[(-1)^1\right]_3 = [-1]_3$$

but

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

So $\diamond$ is not well-defined.

(8)

$$\oplus: \quad \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \quad (a,b) \mapsto \frac{a}{b}$$

is not a binary operation. Since $\frac{1}{0}$ is not defined, $\oplus$ is not well-defined.

Example 1.3.5. Let I be a set. $\mathrm{Sym}(I)$ denotes the set of all permutations of I. If f and g are permutations of S then by A.2.3(c) also the composition $f \circ g$ is a permutation of I. Hence the map

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

is a binary operation on $\mathrm{Sym}(I)$. Observe that 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 $f \circ (g \circ h) = (f \circ g) \circ h$.

The function

$$\mathrm{id}_I : \qquad I \to I, \qquad i \mapsto i$$

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 $\mathrm{Sym}(I)$.

Let $f \in \mathrm{Sym}(I)$. Define

$$g : \qquad I \to I, \qquad i \mapsto j$$

where j is the unique element in I with $f(j) = i$. Let $i \in I$. Then

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

Put $k := g(f(i)) = k$. Then by definition of g we have $f(k) = f(i)$. Since f is 1-1 this implies $k = i$. Thus $g(f(i)) = i = \mathrm{id}_I(i)$. We proved that $f \circ g = \mathrm{id}_I$ and $g \circ f = \mathrm{id}_I$. Hence f is invertible with inverse g. Thus $(\mathrm{Sym}(I), \circ)$ is a group, 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 work with permutations.

Notation 1.3.6. *Let $n \in \mathbb{N}$.*

$$\begin{aligned} [1 \dots n] &:= \quad \{i \in \mathbb{N} \mid 1 \le i \le n\} \quad = \{1, 2, 3, \dots, n\}. \\ \mathrm{Sym}(n) &:= \quad \mathrm{Sym}\big([1 \dots n]\big). \end{aligned}$$

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 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:*

Let $a_{i,j}, 1 \le i \le k_j, 1 \le j \le l$ be elements of $[1 \dots n]$ such that for each $m \in [1 \dots n]$ there exist unique i, j with $m = a_{i,j}$. Then

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

denotes the permutation π with

$$\pi(a_{i,j}) = a_{i+1,j}, \quad \textit{and} \quad \pi(a_{k_j,j}) = a_{1,j}$$

for all $1 \le i < k_j$ and $1 \le j \le l$.

$(a_{1,j}, a_{2,j}, \dots a_{k_j,j})$ is called a cycle *of length k_j of π.*

We often will omit some or all of the cycles of length 1 in the cycle notation of π.

Example 1.3.7. (1)

$$(1,3,4)(2,6)(5) \quad = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$$

(2) Compute $(1,3)(2,4) \circ (1,4)(2,5,6)$ in $\mathrm{Sym}(6)$.

We have

$$\begin{array}{ccccc} & (1,4)(2,5,6) & & (1,3)(2,4) & \\ 1 & \mapsto & 4 & \mapsto & 2 \\ 2 & \mapsto & 5 & \mapsto & 5 \\ 5 & \mapsto & 6 & \mapsto & 6 \\ 6 & \mapsto & 2 & \mapsto & 4 \\ 4 & \mapsto & 1 & \mapsto & 3 \\ 3 & \mapsto & 3 & \mapsto & 1 \end{array}$$

and so

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

(3) Compute the inverse of $(1,4,5,6,8)(2,3,7)$.

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: The inverse of

$$(1,4,5,6,8)(2,3,7)$$

is

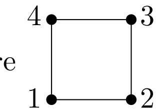
$$(8,6,5,4,1)(7,3,2)$$

Example 1.3.8. In cycle notation the elements of $\mathrm{Sym}(3)$ are

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

Keep here in mind that $(1) = (1)(2)(3)$, $(1,2) = (1,2)(3)$ and so on. The multiplication table of $\mathrm{Sym}(3)$ 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 1.3.9. Consider the square 

.

Let D_4 be the set of all permutations of $\{1,2,3,4\}$ which map the edges of the squar 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°:

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

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

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

How many elements does D_4 have: Let $\pi \in D_4$.

$\pi(1)$ 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

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

Is $(D_4, \circ)$ a group?

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. So D_4 is closed under multiplication and inverses. Thus $\circ$ is an associative binary operation on D_4, (1) is an identity and each α in D_4 is invertible. So $(D_4, \circ)$ is a group, called the *dihedral group of degree* 4.

1.4 Basic Properties of Groups

Lemma 1.4.1. *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 1.4.2. *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. □

Example 1.4.3. 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.

Notation 1.4.4. *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 1.4.5. *Let $(G, *)$ be a group and define*

$$\diamond : \qquad G \times G \to G, \quad (a, b) \mapsto b * a.$$

(a) *$\diamond$ is a binary operation on H, called the opposite operation of $*$.*

(b) *$\diamond$ is associative.*

(c) *Let e be an identity of $*$ in H. Then e is an identity of $\diamond$.*

(d) *Let $a \in G$ and let a^{-1} be inverse of b in G with respect to $*$, then a^{-1} is also an inverse of b in G with respect to $\diamond$.*

(e) *$(G, \diamond)$ is a group, called the opposite group of $(G, *)$.*

Proof. See Homework 1 □

Lemma 1.4.6. *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)

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

So the first statement holds. The second follows from the first applied to the opposite group of G. The last two follow from the first to applied with a replaced by a^{-1} and so a^{-1} replaced by a. □

Lemma 1.4.7 (Cancellation Law)**.** *Let G be a group and $a, b, c \in G$. Then*

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

Proof. Suppose first that $ab = ac$. The Principal of Substitution implies that $a^{-1}(ab) = a^{-1}(ac)$ and so by 1.4.6 $a = b$.

Suppose $b = c$. The Principal of Substitution implies that $ab = ac$.

So the first two statement are equivalent. This fact, applied to the opposite group, shows that the last two statements are equivalent. □

Lemma 1.4.8. *Let G be a group and $a, b \in G$.*

(a) *There exists a unique $x \in G$ with $ax = b$, namely $x = a^{-1}b$.*

(b) *There exists a unique $y \in G$ with $ya = b$, 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 1.4.7 $ax = b$ if and only if $a^{-1}(ax) = a^{-1}b$ and so by 1.4.6 if and only if $x = a^{-1}b$.

(b) follows from (a) applied to the opposite group.

(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 $b = a^{-1}$. This fact, applied to the opposite group, shows that $ba = e$ if and only if $b = a^{-1}$.

(d)

$$\begin{array}{ccccl} & (ab)(b^{-1}a^{-1}) & & \\ = & a(b(b^{-1}a^{-1})) & - & * \text{ is associative} \\ = & aa^{-1} & - & 1.4.6(b) \\ = & e & - & \text{definition of } a^{-1} \end{array}$$

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

Definition 1.4.9. *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) *$a^{-n} := (a^{-1})^n$.*

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

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

Lemma 1.4.10. *Let G be a group, $a \in G$ and $n, m \in \mathbb{Z}$. Then*

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

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

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

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

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

$$a^n a^{-n} = a^{n-n} = a^0 = e, \quad \text{so } (a^n)^{-1} = (a^n)^{-1}.$$

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

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 $m \geq 0$.

Suppose that $m = 0$. Then $a^n a^0 = a^n e = a^n = a^{n+0}$ and (a) is true.

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

Suppose $m = 1$ and $n < 0$. Let $k := -n$. Then $k \in \mathbb{Z}^+$, $n = -k$ and $n + 1 = -k + 1 = -(k-1)$. By definition of a^{-k} we have

$$a^n = a^{-k} = (a^{-1})^k$$

If $k > 1$, then $k - 1 > 0$ and the definition of $a^{-(k+1)}$ gives

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

If $k = 1$, then $n + 1 = 0 = k - 1$ and the preceeding equation still holds since all terms are equal to e. We compute

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

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

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

$$(1) \qquad a^n a^m = a^{n+m},$$

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 $a^{-m}a^m = a^0 = e$ and so for all $m \in \mathbb{N}$,

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

From (a) applied with $n - m$ in place of n we have

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

Multiplying with a^{-m} from the left gives

$$(a^{n-m}a^m)a^{-m} = a^n a^{-m}$$

By (2) $a^{-m} = (a^m)^{-1}$. Hence the left hand side of the preceding equation equals a^{n-m}. Thus

$$a^{n-m} = a^n a^{-m}$$

Since m is an arbitrary positive integer, $-m$ is an arbitrary negative integer. So (a) also holds for negative integers.

(b): By (a) $a^n a^{-n} = a^{n-n} = a^0 = e$. Thus 1.4.8(c) implies $(a^n)^{-1} = (a^n)^{-1}$.

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

□

Definition 1.4.11. *Let G be a group and $a \in G$. 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 $|a|$.*

Example 1.4.12. Determine the order of $(1,2,3,4)$ in Sym(4):

$$\begin{aligned}
(1,2,3,4)^2 &= (1,2,3,4)\circ(1,2,3,4)) = (1,3)(2,4)\\
(1,2,3,4)^3 &= (1,2,3,4)^2\circ(1,2,3,4) = (1,3)(2,4)\circ(1,2,3,4) = (1,4,3,2)\\
(1,2,3,4)^4 &= (1,2,3,4)^3\circ(1,2,3,4) = (1,4,3,2)\circ(1,2,3,4) \quad = (1)(2)(3)(4)
\end{aligned}$$

So $(1,2,3,4)$ has order 4.

1.5 Subgroups

Definition 1.5.1. *Let $(G,*)$ be a group. A pair $(H,\triangle)$ is called a* subgroup *of $(G,*)$ provided that*

(i) *$(H,\triangle)$ is a group,*

(ii) *$H\subseteq G$, and*

(iii) *$a\triangle b = a*b$ 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) $(\mathbb{Q}\smallsetminus\{0\},\cdot)$ is a subgroup of $(\mathbb{R}\smallsetminus\{0\},\cdot)$.

(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).

Lemma 1.5.3. *Let $(H,\triangle)$ be a subgroup of the group $(G,*)$.*

(a) $e_H = e_G$.

(b) *Let $h\in H$. Let h^{-1} be the inverse of h in G with respect to $*$. Then h^{-1} is also the inverse of h in H with respect to $\triangle$.*

Proof. (a) $e_H * e_H = e_H\triangle e_H = e_H = e_H * e_G$. Thus the Cancellation Law implies that $e_H = e_G$,

(b) Let b the inverse of h in H with respect to $\triangle$. Then

$$h*b = h\triangle b = e_H = e_G = h*h^{-1}$$

and the Cancellation Law implies $b = a$. □

Proposition 1.5.4 (Subgroup Proposition)**.** *Let $(G,*)$ be a group and H a subset of G. Define*

$$\triangle:\quad H\times H\to H, (a,b)\mapsto a*b.$$

Then $(H,\triangle)$ is a subgroup of $(G,*)$ if and only if

(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 $*$.*

Proof. $\Longrightarrow$: Suppose $(H, \triangle)$ is a subgroup of G. Then $(H, \triangle)$ is a group. Hence $\triangle$ is a binary operation on H and so $a * b \in H$ for all $a, b \in H$. By 1.5.3(a) we have $e_G = e_H$ and so $e_G \in H$. Let $a \in H$. By 1.5.3(b) a^{-1} is also the inverse of a in H with respect to $\triangle$. So $a^{-1} \in H$.

$\Longleftarrow$: Suppose next that (i), (ii) and (iii) hold. We need to show that $(H, \triangle)$ is a subgroup of $(G, *)$. By hypothesis, $H \subseteq G$ and by definition of $\triangle$ we have $a \triangle b = a * b$ for all $a, b \in H$. So we just need to show that $(H, \triangle)$ is a group.

Since H is closed under $*$, $\triangle$ is a well-defined function from $H \times H$ to H and so $\triangle$ is a binary operation on H.

Let $a, b, c \in H$. Since $H \subseteq G$, we have $a, b, c \in G$. As $*$ is associative we get

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

and so $\triangle$ is associative.

By (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 (iii) $h^{-1} \in H$. Thus $h \triangle h^{-1} = h * h^{-1} = e_G$ and $h^{-1} \triangle h = h^{-1} * h = e_G$. So h^{-1} is an inverse of h with respect to $\triangle$.

So $(H, \triangle)$ is a group. □

Lemma 1.5.5. *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 $(G_i)_{i \in I}$ be 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 1.5.4

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. □

Definition 1.5.6. *Let $*$ be a binary operation on the set H. Let $n \in \mathbb{N}$ and $a_1, \dots, a_n \in H$. Inductively, we call $h \in H$ a product of $(a_1, \dots, a_n)$ with respect to $*$ if either*

(1) *$n = 0$ and h is an identity of $*$.*

(2) *$n = 1$ and $h = a_1$,or*

(3) *There exist $k \in \mathbb{N}$ and $x, y \in H$ such that*

   (i) *$0 < k < n$,*
   (ii) *x is product of $(a_1, \dots, a_k)$,*
   (iii) *y is a product of $(a_{k+1}, \dots, a_n)$.*
   (iv) *$h = x * y$.*

Theorem 1.5.7 (General Associative Law)**.** *Let $*$ be an associative binary operation on the set H. Let $n \in \mathbb{N}$ and $a_1, \dots, a_n \in H$. If h and h' are products of $(a_1, \dots, a_n)$ in H then $h = h'$. We denote the unique product of $(a_1, \dots, a_n)$ by*

$$a_1 * a_2 * \dots * a_n$$

Proof. The proof is by complete induction on n.

If $n = 0$, then both h and h' are identities of $*$ and so $h = h'$ by 1.4.1.

If $n = 1$, then $h = a_1 = h'$ and again $h = h'$.

So suppose $n > 1$. Then there exist $k, k', \mathbb{Z}^+$ and $x, y, x', y' \in H$ such that

(i) $0 < k < n$ and $0 < k' < n$;

(ii) x is a product of $(a_1, \dots, a_k)$, and x' is a product of $(a_1, \dots, a_{k'})$;

(iii) y is a product of $(a_{k+1}, \dots, a_n)$, and y' is a product of $(a_{k'+1}, \dots, a_n)$;

(iv) $h = x * y$ and $h' = x' * y'$.

Suppose first that $k = k'$. Then both x and x' are products of $(a_1, \dots, a_k)$ and so by induction $x = x'$. Similarly, both y and y' are products of $(a_{k+1}, \dots, a_n)$ and so by induction $y = y'$. Hence $h = x * y = x' * y' = h'$.

Suppose next that $k \neq k'$. Without loss $k < k'$. Let z be any product of $(a_{k+1}, \dots, a_{k'})$.

$$\rlap{$\underbrace{\phantom{a_1\cdots a_k\,a_{k+1}\cdots a_{k'}}}_{x'}$}\overbrace{a_1\cdots a_k}^{x}\,\overbrace{\underbrace{a_{k+1}\cdots a_{k'}}_{z}\,\underbrace{a_{k'+1}\cdots a_n}_{y'}}^{y}$$

Then both $x * z$ and x' are products of $(a_1, \dots, a_{k'})$ and so by induction $x * z = x'$. Similarly, $z * y'$ and y are products of $(a_{k+1}, \dots, a_n)$ and so by induction $z * y' = y$. Thus

$$h = x * y = x * (z * y') = (x * z) * y' = x' * y' = h'$$

□

Definition 1.5.8. *Let G be a group and $I \subseteq G$.*

(a) $\langle I \rangle := \bigcap_{I \subseteq H \leq G} H$, *that is $\langle I \rangle$ is the intersection of all the subgroups of G containing I. $\langle I \rangle$ is called the subgroup of G generated by I.*

(b) *Let $g \in G$ and $n \in \mathbb{N}$. Then g is called a product of length n of I in G if there exist $a_1, \dots a_n \in I$ such that $g = a_1 * a_2 * \dots * a_n$.*

(c) $I^{-1} = \{a^{-1} \mid a \in I\}$.

Lemma 1.5.9. *Let G be a group and $I \subseteq G$.*

(a) *$\langle I \rangle$ is the smallest subgroup of G containing I, that is*

   (i) *$\langle I \rangle$ is a subgroup of G.*

   (ii) *$I \subseteq \langle I \rangle$.*

   (iii) *If H is a subgroup of G and $I \subseteq H$, then $\langle I \rangle \subseteq H$.*

(b) *The elements of $\langle I \rangle$ are exactly the products of $I \cup I^{-1}$ in G.*

Proof. (a): Let $\mathcal{H} := \{H \leq G \mid I \subseteq H\}$. By definition, $\langle I \rangle = \bigcap_{H \in \mathcal{H}} H$. By 1.5.5(b) intersections of subgroups are subgroups and so $\langle I \rangle$ is a subgroup of G. As $I \subseteq H$ for all $H \in \mathcal{H}$, we get $I \subseteq \bigcap_{H \in \mathcal{H}} H = \langle I \rangle$. Let $H \in \mathcal{H}$. Then $g \in H$ for all $g \in \bigcap_{H \in \mathcal{H}} H$ and so $\langle I \rangle \subseteq H$.

(b): Set $J := I \cup I^{-1}$ and let P be the set of products of J in G. We will first use the Subgroup Proposition to show that P is a subgroup of G.

Let $a, b \in J$. Then $a = a_1 \dots a_n$ and $b = b_1 \dots b_m$ with $a_1, \dots, a_n, b_1, \dots b_m \in J$. Thus $ab = a_1 \dots a_n b_1 \dots b_m$ is a product of J in G, so $ab \in P$.

e is the product of the empty family. So $e \in P$.

Let $x \in J$. Then either $x \in I$ and $x^{-1} \in I^{-1}$ or $x = y^{-1}$ for some $y \in I$ and so $x^{-1} = (y^{-1})^{-1} = y \in I$. In either case $x^{-1} \in J$. Since $a^{-1} = (a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$ we conclude that $a^{-1} \in P$.

We verified the three conditions of the subgroup theorem and so P is a subgroup of G.

Observe that each elements of I is a product of I, that is $I \subseteq P$. Hence P is subgroup of G containing I and (a) shows that $\langle I \rangle \subseteq P$.

Since $I \subseteq \langle I \rangle$ and $\langle I \rangle$ is closed under inverse we have $I^{-1} \subseteq \langle I \rangle$. So $J \subseteq \langle I \rangle$ and since $\langle I \rangle$ is closed under multiplication we conclude that $P \subseteq \langle I \rangle$. Hence $\langle I \rangle = P$. □

Example 1.5.10. (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)

New products of length 1: (1,2), (2,3).

Possible new products of length 2:

hj	$(1,2)$	$(2,3)$
$(1,2)$	(1)	$(1,2,3)$
$(2,3)$	$(1,3,2)$	(1)

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

Possible new products of length 3.

hj	$(1,2)$	$(2,3)$
$(1,2,3)$	$(1,3)$	$(1,2)$
$(1,3,2)$	$(2,3)$	$(1,3)$

New products of length 3: $(1,3)$

Possible new products of length 4:

hj	$(1,2)$	$(2,3)$
$(1,3)$	$(1,2,3)$	$(1,3,2)$
$(1,3,2)$	$(2,3)$	$(1,3)$

So there are no new products of length 4, and so also no new products of length larger than 4. Thus

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

(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. Observe that any subgroup of G containing a must contain H. Hence H is the smallest subgroup of G containing a, so $H = \langle a \rangle$ by1.5.9.

(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

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

(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 $0 \le r < n$. Then $g^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r$. Thus

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

Suppose that $0 \le r < s < n$. 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 $g^r, 0 \le r < n$ are pairwise distinct. Hence

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

and

$$g^n = e \quad \iff \quad r = 0 \quad \iff n \mid m.$$

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*

$$g : \quad A \to \operatorname{Im} f, \quad a \mapsto f(a).$$

Then

(a) *g is onto.*

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

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 bijective.

(b)

$$\begin{array}{llll}
 & f \text{ is 1-1} & & \\
\Longleftrightarrow & \text{For all } a, b \in A: & f(a) = f(b) \Longrightarrow a = b & - \text{ definition of 1-1} \\
\Longleftrightarrow & \text{For all } a, b \in A: & g(a) = g(b) \Longrightarrow a = b & - \text{ definition of } g \\
\Longleftrightarrow & g \text{ is 1-1} & & - \text{ definition of 1-1} \\
\Longleftrightarrow & g \text{ is bijective} & & - \text{ since } g \text{ is onto}
\end{array}$$

□

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

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

$$f(a * b) = f(a) \,\square\, f(b)$$

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 $f : \mathbb{Z} \to H, m \to h^m$. We compute

$$f(n + m) = h^{n+m} \overset{1.4.10(a)}{=} h^n * h^m = f(n) * f(m).$$

So f is a homomorphism from $(\mathbb{Z}, +)$ to $(H, *)$. We compute

$$\operatorname{Im} f = \{f(n) \mid n \in \mathbb{Z}\} = \{g^n \mid n \in \mathbb{Z}\} \overset{1.5.10(4)}{=} \langle g \rangle.$$

(2) Let $\mathbb{F}$ be a field and $n \in \mathbb{Z}^+$. Let $\mathrm{M}_n(\mathbb{F})$ be the rings of $n \times n$-matrices with coefficients in $\mathbb{F}$. Let $\mathrm{GL}_n(\mathbb{F})$ be the set of invertible elements of $\mathrm{M}_n(\mathbb{F})$. Since matrix multiplication is associative, Exercise 4 on Homework 1 shows that $\mathrm{GL}_n(\mathbb{F})$ is a group under matrix multiplication. Let $\mathbb{F}^\sharp := \mathbb{F} \smallsetminus \{0\}$ and observe that $\mathbb{F}^\sharp$ is a group under multiplication (by the same exercise). For $A \in \mathrm{M}_n(F)$ let $\det(A)$ be the determinant of A. From Linear Algebra we know that $\det(AB) = \det(A)\det(B)$ and that A is invertible if and only if $\det(A) \neq 0$. Hence

$$\mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\sharp, \quad A \mapsto \det(A)$$

is a homomorphism of groups. Since

$$\det\left(\begin{bmatrix} a & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}\right) = a$$

this homomorphism is onto.

If $n > 1$,then

$$\det\left(\begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ a & 0 & \dots & 0 & 1 \end{bmatrix}\right) = 1$$

for all $a \in \mathbb{F}$ and since $|\mathbb{F}| > 1$, the function is not 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*

$$g : \quad G \to \operatorname{Im} f, \quad a \mapsto f(a).$$

is an isomorphism. In particular, $G \cong \operatorname{Im} f$.

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 1.4.7 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 1.4.8(c) , $f(a^{-1}) = f(a)^{-1}$.

(c) We will first verify the three conditions of the Subgroup Proposition 1.5.4. Let $x, y \in \operatorname{Im} f$. Then by definition of $\operatorname{Im} f$, $x = f(a)$ and $y = f(b)$ for some $a, b \in G$.

(i): $xy = f(a)f(b) = f(ab) \in \operatorname{Im} f$.

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

(iii): By (b), $x^{-1} = f(a)^{-1} = f(a^{-1}) \in \operatorname{Im} F$.

So $\operatorname{Im} f$ fulfills all three conditions in 1.5.4 and so $\operatorname{Im} f$ is a subgroup of H.

(d) Define

$$g \quad G \to \operatorname{Im} f, \quad a \mapsto f(a).$$

Since f is 1-1, 1.6.2 implies that f is bijective. 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 homomorphism. Hence g is an isomorphism and thus $G \cong \operatorname{Im} f$. □

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.*

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 $\operatorname{Sym}(G)$. For $g \in G$ define

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

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

$$(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = a(bx) = (ab)x = \phi_{ab}(x)$$

and so

$$\phi_a \circ \phi_b = \phi_{ab}.$$

Since $ex = x$ for all $x \in G$ we have

$$\phi_e = \mathrm{id}_G.$$

In particular,

$$\phi_a \circ \phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e = \mathrm{id}_G \qquad \text{and} \quad \phi_{a^{-1}} \circ \phi_a = \mathrm{id}_G$$

Thus ϕ_a is invertible and so a bijection. Thus $\phi_a \in \operatorname{Sym}(G)$ and we obtain a well-defined function

$$f : \quad G \to \operatorname{Sym}(G), \quad g \mapsto \phi_g$$

Observe that

$$f(ab) = \phi_{ab} = \phi_a \circ \phi_b = f(a) \circ f(b)$$

and so f is a homomorphism.

If $f(a) = f(b)$, then $\phi_a = \phi_b$ and so also $\phi_a(e) = \phi_b(e)$. Thus $ae = be$ and $a = b$. So f is 1-1. Hence by 1.6.5(d), G is isomorphic to the subgroup $\operatorname{Im} f$ of $\operatorname{Sym}(G)$. □

Example 1.6.8. Let U_8 be the set of units (invertible elements) in $\mathbb{Z}_8$, where $\mathbb{Z}_8$ is the ring of integers modulo 8. The multiplication table of U_8 is

$$\begin{array}{c|cccc} \cdot & 1 & 3 & 5 & 7 \\ \hline 1 & 1 & 3 & 5 & 7 \\ 3 & 3 & 9 & 15 & 21 \\ 5 & 5 & 15 & 25 & 35 \\ 7 & 7 & 21 & 35 & 49 \end{array} \qquad \text{and so} \qquad \begin{array}{c|cccc} \cdot & 1 & 3 & 5 & 7 \\ \hline 1 & 1 & 3 & 5 & 7 \\ 3 & 3 & 1 & 7 & 5 \\ 5 & 5 & 7 & 1 & 3 \\ 7 & 7 & 5 & 3 & 1 \end{array}$$

So

$$\phi_1 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{pmatrix} = (1)$$

$$\phi_3 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{pmatrix} = (13)(57)$$

$$\phi_5 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{pmatrix} = (15)(37)$$

$$\phi_7 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{pmatrix} = (17)(35)$$

Thus U_8 is isomorphic to the subgroup

$$\{(1), (13)(57), (15)(37), (17)(35)\}$$

of $\operatorname{Sym}(\{1,3,5,7\})$.

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

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 (left)* 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 K in G containing g. Put*

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

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

Example 1.7.5. Let $G = \mathrm{Sym}(3)$ and $K = \langle (1,2) \rangle$. Compute G/K.

We need to determine all the cosets of K in G. Note first that $K = \{(1),(1,2)\}$.

$$\begin{aligned}
(1)\circ K = \{(1)\circ k \mid k \in K\} = \{(1)\circ(1),(1)\circ(1,2)\} &= \{(1),(1,2)\},\\
(1,2)\circ K = \{(1,2)\circ(1),(1,2)\circ(1,2)\} &= \{(1,2),(1)\},\\
(2,3)\circ K = \{(2,3)\circ(1),(2,3)\circ(1,2)\} &= \{(2,3),(1,3,2)\},\\
(1,3)\circ K = \{(1,3)\circ(1),(1,3)\circ(1,2)\} &= \{(1,3),(1,2,3)\},\\
(1,2,3)\circ K = \{(1,2,3)\circ(1),(1,2,3)\circ(1,2)\} &= \{(1,2,3),(1,3)\},\\
(1,3,2)\circ K = \{(1,3,2)\circ(1),(1,3,2)\circ(1,2)\} &= \{(1,3,2),(2,3)\}.
\end{aligned}$$

Thus

$$G/K = \Big\{ \quad \{(1),(1,2)\}, \quad \{(2,3),(1,3,2)\}, \quad \{(1,2,3),(1,3)\} \quad \Big\}.$$

Note that each element of Sym(3) lies in exactly one of the three cosets. Also each of the cosets has size two, that is the same size as K.

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) $aK \cap bK \neq \varnothing$.

(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) $\Longleftrightarrow$ (b): Let $k \in G$. Then

$$\begin{aligned}
& b = ak \\
\Longleftrightarrow\quad & a^{-1}b = a^{-1}(ak) && \text{– Cancellation Law}\\
\Longleftrightarrow\quad & a^{-1}b = k && \text{– 1.4.6(b)}
\end{aligned}$$

(b) $\Longleftrightarrow$ (c): Should be clear.

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

(a) $\Longleftrightarrow$ (e): Recall that $aK = \{ak \mid k \in K\}$. So $b \in aK$ if and only if $b = ak$ for some $k \in K$.

We proved that statements (a)-(e) are equivalent.

Let $[a]$ be the equivalence class of $' \equiv \pmod K'$ containing a. We will show that $[a] = Ka$:

$$\begin{array}{lll} & b \in [a] & \\ \iff & a \equiv b \pmod K & \text{– Definition of } [b] \\ \iff & b \in aK & \text{– Since (d) and (e) are equivalent} \end{array}$$

Hence $[a] = aK$ by 1.1.1, so the first statement of the lemma holds.

Moreover, Theorem A.1.3 now implies that Statements (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 $a \in G$. Then a is contained in a unique coset X of K in G, namely $X = aK$.*

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

(c) *G/K is a partition of G.*

(d) *Let $T \in G/K$ and $a \in T$. Then the function*

$$\delta : \quad K \to T, \quad k \to ak$$

is a well defined bijection. In particular, $|T| = |K|$.

Proof. (a) By A.1.4(a), a is contained in a unique equivalence class X of $\equiv \pmod K$, namely $[a]$. As $[a] = aK$, this gives (a).

(b) Observe that $K = eK$. So K is a coset of K in G. Thus (b) follows from (a).

(c) Follows from (a).
(d) Define

$$\epsilon : \quad K \to G, \quad k \mapsto ak$$

Let $k, l \in K$ with $\epsilon(k) = \epsilon(l)$. Then $ak = al$ and the Cancellation Law 1.4.7 implies that $k = l$. Thus ϵ is 1-1. Since $a \in T$, (a) gives

$$T = aK = \{ak \mid k \in K\} = \epsilon(k) \mid k \in K\} = \operatorname{Im} \epsilon$$

Hence 1.6.2(b) shows that δ is a well-defined bijection. □

Theorem 1.7.8 (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(c), G/K is partition of in G. Hence

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

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

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

□

Example 1.7.9. (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 Sym(4).

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

(3) Since 5 does not divide 24, Sym(4) does not have subgroup of order 5.

Corollary 1.7.10. *Let G be a finite group.*

(a) *If $a \in G$, then $|a|$ divides $|G|$.*

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

Proof. (a) By Example 1.5.10(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 $a^n = a^{mk} = (a^m)^k = e^k = e$. □

Definition 1.7.11. *Let I be a finite set and $g \in \mathrm{Sym}(I)$. Suppose, in cycle notation,*

$$g = (a_{1,1}, a_{2,1}, a_{3,1}, \ldots a_{k_1,1})(a_{1,2}, a_{2,2} \ldots a_{k_2,2}) \ldots (a_{1,l}, a_{2,l} \ldots a_{k_l,l})$$

with $k_1 \geq k_2 \geq \ldots \geq k_l$ and all cycles of length 1 listed. Then

$$(k_1, \ldots, k_l)$$

is called the cycle type of g.

Example 1.7.12. (1) $(1,4,7,9)(2,3)(5,8) \in \mathrm{Sym}(10)$ has cycle type $(4,2,2,1,1)$,

(2) The possible cycle type of elements of Sym(4) are

$$(4), \quad (3,1), \quad (2,2), \quad (2,1,1), (1,1,1,1).$$

Lemma 1.7.13. *Let I be a finite set and $g \in \mathrm{Sym}(I)$.*

(a) *Suppose $g = (a_1, a_2, \ldots, a_k)$ for pairwise distinct $a_j, 1 \leq j \leq k$ in I. Then $|g| = k$.*

(b) *Suppose g has cycle type $(k_1, \ldots, k_l)$. Then $|g| = \mathrm{lcm}(k_1, k_2, \ldots, k_l)$.*

Proof. Let $i \in I$. Then

$$g(i) = \begin{cases} a_{j+1} & \text{if } i = a_j \text{ for some } 1 \le j \le k \\ i & \text{otherwise} \end{cases}$$

where subscript are read modulo k, that is $a_{k+1} = a_1$. Hence for $n \in \mathbb{Z}^+$:

$$g^n(i) = \begin{cases} a_{j+n} & \text{if } i = a_j \text{ for some } 1 \le j \le k \\ i & \text{otherwise} \end{cases}$$

If follows that $g^n = \mathrm{id}_I$ if and only if $j \equiv j + n \pmod k$ for all $1 \le j \le k$ and so if and only if $k \mid n$. Thus $|g| = n$.

(b) Let

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

in cycle notation. For $1 \le j \le l$ define

$$g_j := (a_{1,j}, a_{2,j} \dots a_{k_j,j}).$$

Then

$$g = g_1 \circ g_2 \circ \dots \circ g_l$$

and

$$g^n = g_1^n \circ g_2^n \circ \dots \circ g_l^n.$$

Hence $g^n = \mathrm{id}_I$ if and only if $g_i^n = \mathrm{id}_I$ for all $1 \le j \le l$. As seen in (a), this holds if and only if $k_j \mid n$ for all $1 \le j \le l$ and so if and only if $\mathrm{lcm}(k_1, \dots, k_l)$ divides n. □

Example 1.7.14. We will investigate the elements of $\mathrm{Sym}(4)$ according to their cycle type:

Cycle type (4):

$g = (a, b, c, d)$ where a, b, c, d are four distinct elements of $\mathrm{Sym}(4)$. Then $|g| = 4$. How many elements of this form? There are 24 choices for the tuple (a, b, c, d) but always four of these choices give the same elements:

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

So there are $\frac{24}{6} = 6$ elements of cycle type (4). We can list them explicitly:

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

Cycle type (3,1):

$g = (a, b, c)(d) = (a, b, c)$. Then $|g| = 3$. Always three of these choices give the same elements:

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

So there are $\frac{24}{3} = 8$ elements of cycle type (4). We can list them explicitly:

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

Cycle type $(2,2)$:

$g = (a,b)(c,d)$. Then $|g| = 2$. Always eight of these choices give the same elements:

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

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

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

Cycle type $(2,1,1)$:

$g = (a,b)(c)(d) = (a,b)$. Then $|g| = 2$. Always four of these choices give the same elements:

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

So there are $\frac{24}{4} = 6$ elements in Sym(4) of cycle type $(2,1,1)$:

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

Cycle type (1,1,1,1):

$g = (a)(b)(c)(d)$. Then $|g| = 1$. All twenty-four choices of (a,b,c,d) give the same element, namely the identity function. So

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

is the only elements if cycle type $(1,1,1,1)$.

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

Definition 1.7.15. *A group G is called* cyclic *if $G = \langle g \rangle$ for some $g \in G$.*

Lemma 1.7.16. *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 1.5.10(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 $|g| = n$. □

Example 1.7.17. (1) We compute in $(\mathbb{Z}_4, +)$:

$$1 + 1 = 2 \neq 0, \quad 1 + 1 + 1 = 3 \neq 0, \quad 1 + 1 + 1 + 1 = 4 = 0.$$

Hence 1 has order 4 in $(\mathbb{Z}_4, +)$. As $|\mathbb{Z}_4| = 4$ this shows that $\mathbb{Z}_4$ is cyclic.

(2) We have $a^2 = 1$ for all $a \in U_8$. Thus $(U_8, \cdot)$ does not have an element of order four and so U_8 is not cyclic.

Corollary 1.7.18. *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 1.7.10(b) $|g|$ divides p. Since $g \neq e$, $|g| \neq 1$. Since p is a prime this implies $|g| = p$. So by 1.7.16(b), $G = \langle g\rangle$ and so g is cyclic. □

Example 1.7.19. All groups of order 3 are cyclic.

Example 1.7.20. Let $G = \mathrm{GL}_2(\mathbb{Q})$, the group of invertible 2×2 matrices with coefficients in $\mathbb{Q}$ and let

$$g := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Let $n \in \mathbb{Z}$. Then

$$g^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$$

and so

$$\langle g\rangle = \left\{ \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \;\middle|\; n \in \mathbb{Z} \right\}.$$

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 1.7.16 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) $(A^{-1})^{-1} = A$

(g) $A \subseteq B$ *if and only if* $A^{-1} \subseteq B^{-1}$.

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

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

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

Proof. (a)

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

(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) If $A = B$ the Principal of Substitution gives $Ag = Bg$. 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)

$$A = \{a \mid a \in A\} = \{(a^{-}1)^{-1} \mid a \in A = \{a^{-1} \mid a \in A\}^{-1} = (A^{-1})^{-1}$$

(g) Suppose $A \subseteq B$. Let $d \in A^{-1}$. Then $d = a^{-1}$ for some $a \in A$. Then $a \in B$ and so $d = a^{-1} \in B^{-1}$. Thus $A^{-1} \subseteq B^{-1}$

Suppose $A^{-1} \subseteq B^{-1}$. Then $(A^{-1})^{-1} \subseteq (B^{-1})^{-1}$ and (f) gives $A \subseteq B$.

(h) Let $A \leq G$. By the Subgroup Proposition A is $e \in A$, A is closed under multiplication and A is closed under inverses. Hence

$$A = eA = \{ea \mid a \in A\} \subseteq AA, \quad AA = \{ab \mid a, b \in A\} \subseteq A, \quad A^{-1} = \{a^{-1} \mid a \in A\}, \quad A = A^{-1})^{-1} \subseteq A^{-1}$$

Thus $A = AA$ and $A = A^{-1}$.

$$(i) \qquad \begin{array}{rclcl} (AB)^{-1} & = & \{d^{-1} \mid d \in AB\} & = & \{(ab)^{-1} \mid a \in A, b \in B\} \\ & \overset{1.4.8(\mathrm{d})}{=} & \{b^{-1}a^{-1} \mid a \in A, b \in B\} & = & \{cd \mid c \in B^{-1}, d \in A^{-1}\} \\ & = & B^{-1}A^{-1} & & \end{array}$$

(j) By (i) applied 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 G be a finite group and $H \leq G$ with $\frac{|G|}{|H}| = 2$. Then by Lagrange's Theorem $|G/H| = \frac{|G|}{|H|} = 2$.

Let $g \in H$. Then 1.7.7(c) gives $gH = H$.

Let $g \in G \smallsetminus H$. Then $g \in gH$ and $g \notin H$. So $H \neq gH$ and since $|G/H| = 2$ we get $G/H = \{H, gH\}$. As G/H is a partition of G this gives

$$g \circ H = G \smallsetminus H = \{(1,2),(2,3),(1,3)\}$$

Applying these these two results to the opposite group of G gives $Hg = H$ for $g \in H$ and $Hg = G \smallsetminus H$ for $g \in G \smallsetminus H$. In either case $gH = Hg$ and so H is a normal subgroup of G.

(3) Let $H := \langle(1,2,3)\rangle \leq G := \mathrm{Sym}(3)$. Since $(1,2,3)$ has order three,

$$H = \{(1), (1,2,3), (1,2,3)^2\} = \{(1), (1,2,3), (1,3,2)\}.$$

Note that H has order three and G has order six. Thus (2) shows that $H \trianglelefteq G$.

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 $(G, *)$ is called* abelian *if $*$ 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 (that is $aN = Na$ for all $a \in G$).*

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

(c) *$Na \subseteq aN$ for all $a \in G$.*

(d) *$aN \subseteq Na$ for all $a \in G$.*

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

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

(g) *Every right-coset of N in G is a (left) coset of N.*

Proof. We will first show that first five statements are equivalent. Let $a \in G$. Then

$$\begin{array}{ccccc} & a^{-1}Na \subseteq N & & \\ \iff & a(a^{-1}Na) \subseteq aN & - & 1.8.1(e) \\ \iff & (a(a^{-1}N))a \subseteq aN & - & 1.8.1(a) \\ \iff & Na \subseteq aN & - & 1.8.1(c) \end{array}$$

So

$$(*) \qquad a^{-1}Na \subseteq N \iff Na \subseteq aN.$$

Thus result applied to the opposite group gives

$$(**) \qquad aNa^{-1} \subseteq N \iff aN \subseteq Na$$

Thus

$$\begin{array}{rlll} & Na \subseteq aN & \text{for all } a \in G & \\ \iff & a^{-1}Na \subseteq N & \text{for all } a \in G & -(*) \\ \iff & aNa^{-1} \subseteq N & \text{for all } a \in G & -G \to G,\ a \mapsto a^{-1} \text{is a bijection} \\ \iff & Na \subseteq Na & \text{for all } a \in G & -(**) \end{array}$$

It follows that

$$\begin{array}{rll} & Na \subseteq aN & \text{for all } a \in G \\ \iff & (Na \subseteq aN) \text{ and } (aN \subseteq Na) & \text{for all } a \in G \\ \iff & Na = aN & \text{for all } a \in G \end{array}$$

Hence (a)-(d) are equivalent.

(a) $\implies$ (e):

$$\begin{array}{rll} & aN = Na & \\ \iff & (aN)a^{-1} = (Na)a^{-1} & -1.8.1(d) \\ \iff & aNa^{-1} = N & -1.8.1(c) \end{array}$$

(b) $\iff$ (f): Since $aNa^{-1} = \{ana^{-1} \mid a \in N\}$ we get $aNa^{-1} \subseteq N$ if and only if $ana^{-1} \in N$ for all $m \in N$.

(a) $\iff$ (g): Let $a \in G$.
Suppose (a) holds. Then $Na = aN$ and so every right-coset is a coset.

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

Definition 1.8.7. *Let G be a group.*

(a) *An automorphism of G is a isomorphism from G to G.*

(b) *Let $a \in G$. Then function*
$$\mathrm{inn}_a : \quad G \to G, \quad g \mapsto aga^{-1}$$
is called conjugation by a in G. It is also called the inner automorphism of G induced by a.

(c) *Let $g, h \in G$ we say that g and h are conjugate in G if $h = aga^{-1}$ for some $a \in G$.*

Proposition 1.8.8 (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 1.5.4 N is a subgroup of G if and only if (i),(ii) and (iii) hold. By 1.8.6(f), 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. □

Corollary 1.8.9. *Let N be a normal subgroup of the group G, $a, b \in G$ and $S, T \in G/N$.*

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

(b) *$ST \in G/N$.*

(c) *$N \in G/N$, $NS = S$ and $SN = S$.*

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

(e) *$S^{-1} \in G/N$, $SS^{-1} = N$ and $S^{-1}S = N$.*

Proof. (a) Since $N \trianglelefteq G$ we have $bN = Nb$. 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) follows from (a).

(c) $N = eN \in G/N$. We may assume $S = aN$. Then

$$NS = N(aN) = (Na)N = (aN)N = a(NN) = aN = S.$$

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

(e) From (d) we get $S^{-1} = (aN)^{-1} = a^{-1}N \in G/N$. Also

$$SS^{-1} = (aN)(a^{-1}N) = (aNa^{-1})N \overset{1.8.6(e)}{=} NN \overset{1.8.1(h)}{=} N$$

and similarly $S^{-1}S = N$. □

Definition 1.8.10. *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 1.8.9(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 1.8.11. *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 $T \in G/N$ with respect to $*_{G/N}$ is T^{-1}.

Proof. By definition $*_{G/N}$ is a binary operation on G/N. By 1.8.1(a), $*_{G/N}$ is associative; by 1.8.9(c), N is an identity for $*_{G/N}$; and by 1.8.9(e), T^{-1} is an inverse of T. □

Example 1.8.12. (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(3) $\langle(1,2,3)\rangle$ 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.

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

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

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

Lemma 1.8.13. *Let I be a finite set and $f, g \in \mathrm{Sym}(I)$.*

(a) *Suppose*

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

in cycle notation. Then

$$f \circ g \circ f^{-1} = \Big(f(a_{1,1}), f(a_{2,1}), \dots f(a_{k_1,1})\Big)\Big(f(a_{1,2}), f(a_{2,2}) \dots f(a_{k_2,2})\Big) \dots \Big(f(a_{1,l}), f(a_{2,l}) \dots f(a_{k_l,l})\Big)$$

(b) *Two elements of* Sym(I) *are conjugate if and only if they have the same cycle type.*

Proof. (a) Just observe that

$$(fgf^{-1})(f(a_{ij})) = f\Big(g\big(f^{-1}(f(a_{ij}))\big)\Big) = f\big(g(a_{ij})\big) = f(a_{i+1,j}))$$

(b) From (a) we conclude that if g has cycle-type $(k_1,\dots,k_l)$, then also $f\circ g\circ f^{-1}$ has cycle type $(k_1,\dots,k_l)$.

Conversely suppose that $h\in\mathrm{Sym}(I)$ same the same cycle type $(k_1,\dots,k_l)$ as g. Then

$$h = (b_{1,1},b_{2,1},b_{3,1},\dots b_{k_1,1})(b_{1,2},b_{2,2}\dots b_{k_2,2})\dots(b_{1,l},b_{2,l}\dots b_{k_l,l})$$

for some b_{ij}. Then

$$f:\quad I\to I,\quad a_{ij}\mapsto b_{ij}$$

is a well-defined bijection from I to I. Hence $f\in\mathrm{Sym}(I)$ and (a) shows that $f\circ g\circ f^{-1}=h$. □

Example 1.8.14. (1) Consider $g=(1,4,2)(3,6)(7,8,9,5)$ and $f=(1,7,3)(2,6)$ in Sym(9). Then

$$f\circ g\circ f^{-1} = (7,4,6)(1,2)(3,8,9,5)$$

(2) Find all conjugates of $(1,2)(3,4)$ in Sym(4).

The conjugates of $(1,2)(3,4)$ are the elements of cycle type $(2,2)$, that is

$$(1,2)(3,4),\quad (1,3)(2,4)\quad (1,4)(2,3).$$

(3) Let $g=(1,3,5)(2,4,6)$ and $h=(1,2,5)(3,4,6)$. Find $f\in\mathrm{Sym}(6)$ with $f\circ g\circ f^{-1}=h$.

$$f = \begin{pmatrix} 1 & 3 & 5 & 2 & 4 & 6\\ 1 & 2 & 5 & 3 & 4 & 6\end{pmatrix} = (3,5)$$

1.9 The Isomorphism Theorems

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

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

Kerϕ *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 1.8.8. Let $g \in G$. The definition of $\mathrm{Ker}\phi$ shows that

$$(*) \qquad g \in \mathrm{Ker}\phi \quad \Longleftrightarrow \quad \phi(g) = e_H$$

Let $a, b \in \mathrm{Ker}\phi$. Then $(*)$ shows that

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

(i) $\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H$ and so $ab \in \mathrm{Ker}\phi$.
(ii) By 1.6.5(a), $\phi(e_G) = e_H$ and so $e_G \in \mathrm{Ker}\phi$.
(iii) By 1.6.5(b), $\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H$ and so $a^{-1} \in \mathrm{Ker}\phi$.
(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 $dad^{-1} \in \mathrm{Ker}\phi$.

By (i)-(iv) and 1.8.8 $\mathrm{Ker}\phi$ is a normal subgroup of G. □

Lemma 1.9.3. *Let $\phi : G \to H$ be a homomorphism of groups.*

(a) *Let $a, b \in G$. Then*

$$\phi(a) = \phi(b) \quad \Longleftrightarrow \quad a^{-1}b \in \mathrm{Ker}\phi \quad \Longleftrightarrow \quad a\mathrm{Ker}\phi = b\mathrm{Ker}\phi \quad \Longleftrightarrow \quad a \in b\mathrm{Ker}\Phi$$

(b) *ϕ is 1-1 if and only if* $\mathrm{Ker}\phi = \{e_G\}$.

Proof. (a)

$$\begin{array}{lll} & \phi(a) = \phi(b) & \\ \Longleftrightarrow & \phi(a)^{-1}\phi(b) = e_H & - \text{Cancellation law} \\ \Longleftrightarrow & \phi(a^{-1})\phi(b) = e_H & - 1.6.5(b) \\ \Longleftrightarrow & \phi(a^{-1}b) = e_H & - \phi \text{ is a homomorphism} \\ \Longleftrightarrow & a^{-1}b \in \mathrm{Ker}\phi & - \text{Definition of } \mathrm{Ker}\phi \end{array}$$

Hence the first equivalence holds. The other two follow from 1.7.6.

(b) Suppose ϕ is 1-1 and let $a \in \mathrm{Ker}\phi$. Then $\phi(a) = e_H = \phi(e_G)$ and since ϕ is 1-1 we get $a = e_G$. So $\mathrm{Ker}\phi = \{e_G\}$.

Suppose $\mathrm{Ker}\phi = \{e_G\}$. Let $a, b \in G$ with $\phi(a) = \phi(b)$. Then by (a)

$$a \in b\mathrm{Ker}\phi = b\{e_G\} = \{be_G\} = \{b\}$$

and so $a = b$. Thus ϕ is 1-1. □

Lemma 1.9.4. *Let N be a normal subgroup of G and define*

$$\pi: \quad G \to G/N, \quad a \mapsto aN.$$

Then π is an onto group homomorphism with $\mathrm{Ker}\pi = N$*. π is called the* natural homomorphism *from G to G/N.*

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

$$\pi(ab) = abN \overset{1.8.9(a)}{=} (aN)(bN) = \pi(a)\phi(b),$$

and so ϕ is a homomorphism.

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

$$\begin{array}{rcll} & a \in \mathrm{Ker}\phi & & \\ \Longleftrightarrow & \phi(a) = e_{G/N} & - & \text{definition of } \mathrm{Ker}\phi \\ \Longleftrightarrow & aN = N & - & \text{definition of } \phi, 1.8.11 \\ \Longleftrightarrow & a \in N & - & 1.7.7(a) \end{array}$$

So $\mathrm{Ker}\pi = N$. □

Corollary 1.9.5. *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 of groups with domain G.*

Proof. By 1.9.2 the kernel of a homomorphism is a normal subgroup; and by 1.9.4 any normal subgroup is the kernel of a homomorphism. □

Theorem 1.9.6 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism of groups. Then*

$$\overline{\phi}: \quad G/\mathrm{Ker}\phi \to \mathrm{Im}\,\phi, \quad a\mathrm{Ker}\phi \mapsto \phi(a)$$

is well-defined isomorphism of groups. In particular

$$G/\mathrm{Ker}\phi \cong \mathrm{Im}\,\phi.$$

Proof. Put $N := \mathrm{Ker}\phi$ and $a, b \in G$. By 1.9.3 we have

$$(*) \qquad aN = bN \Longleftrightarrow \phi(a) = \phi(b).$$

The forward direction shows that ϕ is well-defined and the backward direction shows that ϕ is 1-1.

Let $d \in \mathrm{Im}\,\phi$. Then $d = \phi(a)$ for some $a \in G$ and so $\overline{\phi}(aN) = \phi(a) = d$. Thus $\overline{\phi}$ is onto.

Let $S, T \in G/N$. The $S = aN$ and $T = bN$ for some $a, b \in G$. Thus

$$\overline{\phi}(ST) = \overline{\phi}(gNhN) \overset{1.8.9(a)}{=} \overline{\phi}(ghN) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(gN)\overline{\phi}(hN) = \overline{\phi}(S)\overline{\phi}(T)$$

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

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

$$\begin{tikzcd}
 & G \arrow[dddl, "\phi"'] \arrow[dddr, "\pi"] & \\
 & g \arrow[ddl] \arrow[ddr] & \\
 & & \\
\phi(g) & & g\mathrm{Ker}\phi \arrow[ll] \\
\mathrm{Im}\,\phi & & G/\mathrm{Ker}\phi \arrow[ll, "\cong", "\overline{\phi}"']
\end{tikzcd}$$

Lemma 1.9.7. *Let G be a group and $g \in G$. If g has finite order put $n := |g|$, otherwise put $n = 0$. Consider the homomorphism*

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

from Example 1.6.4(1). Then

$$\mathrm{Ker}\Phi = n\mathbb{Z} \qquad \textit{and} \quad \mathrm{Im}\,\phi = \langle g \rangle.$$

In particular,

$$\mathbb{Z}_n \cong \langle g \rangle$$

and, if g has infinite order, then

$$\mathbb{Z} \cong \langle g \rangle$$

Proof. By 1.6.4(1) we already know that

$$\mathrm{Im}\,\phi = \{g^m \mid m \in \mathbb{Z}\} = \langle g \rangle.$$

We compute

$$\mathrm{Ker}\phi = \{m \in \mathbb{Z} \mid \phi(m) = e\} = \{m \in \mathbb{Z} \mid g^m = e\}.$$

Suppose that ϕ has finite order n. By 1.5.10(4) we have $g^m = e$ if and only if $n \mid m$. So $\mathrm{Ker}\Phi = n\mathbb{Z}$.

Suppose ϕ has infinite order. Then $g^m \neq e$ for all $m \in \mathbb{Z}^+$. Since $g^{-m} = (g^m)^{-1}$ we conclude that $g^m = e$ if and only if $m = 0$. Hence $\mathrm{Ker}\phi = \{0\} = 0\mathbb{Z} = n\mathbb{Z}$.

The First Isomorphism Theorem says

$$\mathbb{Z}/\mathrm{Ker}\phi \cong \mathrm{Im}\,\phi$$

and so

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

If g has infinite order, then $\mathrm{Ker}\phi = \{0\}$. So by 1.9.3 ϕ is 1-1 and hence $\mathbb{Z} \cong \mathrm{Im}\,\phi = \langle g\rangle$. □

Corollary 1.9.8. (a) *Let G be a cyclic group of finite order n. Then $G \cong \mathbb{Z}_n$.*

(b) *Let G be an infinite cyclic group. Then $G \cong \mathbb{Z}$.*

(c) *Two cyclic groups are isomorphic if and only if they have the same order.*

(d) *Let G be a finite group of prime order p. Then $G \cong \mathbb{Z}_p$.*

Proof. Let G be a cyclic group. Then by definition there exists $g \in G$ with $G = \langle g\rangle$. Let

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

be the homomorphism from 1.9.7.Then

$$\mathrm{Im}\,\phi = \langle g\rangle = G.$$

(a) Suppose G has finite order n. Then $|g| \overset{1.6.4(1)}{=} |\langle g\rangle| = |G|$. Hence 1.9.7 shows that $\mathbb{Z}_n \cong \mathrm{Im}\,\phi = G$.

(b) If G has infinite order, then 1.9.7 shows $\mathbb{Z} \cong \mathrm{Im}\,\phi = G$.

(c) follows from (a) and (b).

(d) By 1.7.18 any group of prime order is cyclic. So (d) follows from (a). □

Definition 1.9.9. (a) *Let $(A_i)_{i\in I}$ be a family of sets, that is I is a set and for each $i \in I$, A_i is a set. Then $\times_{i\in I} A_i$ denotes the sets of all functions*

$$f : I \to \bigcup_{i\in I} A_i, \quad \textit{with} \quad f(i) \in A_i \textit{ for all } i \in I$$

We denote such a function by $\big(f(i)\big)_{i\in I}$. The set $\times_{i\in I} A_i$ is called the direct product of the family of sets $(A_i)_{i\in I}$.

(b) *Let $(A_i, *_i)$ be a family of pairs such that $*_i$ is a binary operation on A_i. Define a binary operation $*$ on $\times_{i\in I} A_i$ by*

$$(f * g)(i) = f(i) *_i g(i) \quad \textit{for all } i \in I$$

or equivalently in tuple notation by

$$(a_i)_{i\in I} * (b_i)_{i\in I} = (a_i *_i b_i)_{i\in I}$$

This binary operation is called the direct product of the family of binary operations $(*_i)_{i\in I}$ *and is denoted by*

$$\bigtimes_{i\in I} *_i.$$

(c) *If* $(A_i)_{i=1}^n$ *is a finite family of sets, we write*

$$A_1 \times A_2 \times \ldots \times A_n$$

for $\bigtimes_{i=1}^n A_i$.

Lemma 1.9.10. *Let* $(G_i, *_i)_{i\in I}$ *be a family of groups. Then*

$$\left(\bigtimes_{i\in I} G_i,\ \bigtimes_{i\in I} *_i\right)$$

is a group with identity

$$\left(e_{G_i}\right)_{i\in I}.$$

Moreover,

$$(g_i)_{i\in I}^{-1} = (g_i^{-1})_{i\in I}.$$

for all $(g_i)_{i\in I} \in \bigtimes_{i\in I} G_i$.

Proof. Define $G := \bigtimes_{i\in U}$ and $* := (\bigtimes_{i\in I} *_i)$. Let $a, b, c \in G$.

$$a = (a_i)_{i\in I}, \quad b = (b_i)_{i\in I} \quad (c_i)_{i\in I}$$

with $a_i, b_i, c_i \in G_i$ for all $i \in I$.

$$\begin{aligned}
(a * b) * c &= \Big((a_i)_{i\in I} * (b_i)_{i\in I}\Big) * (c_i)_{i\in I} \\
&= (a_i *_i b_i)_{i\in I} * (c_i)_{i\in I} \\
&= \left((a_i *_i b_i) *_i c_i\right)_{i\in I} \\
&= \left(a_i *_i (b_i *_i c_i)\right)_{i\in I} \\
&= (a_i)_{i\in I} * \left(b_i *_i c_i\right)_{i\in I} \\
&= (a_i)_{i\in I} * \Big((b_i)_{i\in I} * (c_i)_{i\in I}\Big) \\
&= a * (b * c).
\end{aligned}$$

So $*$ is associative.

Put $e := \left(e_{G_i}\right)_{i\in I}$ and $a^{-1} := \left(a_i^{-1}\right)_{i\in I}$. Then

$$
\begin{aligned}
e * a &= \big(e_{G_i}\big)_{i\in I} * (a_i)_{i\in I} = \big(e_{G_i} *_i a_i\big)_{i\in I} = (a_i)_{i\in I} = a, \\
a * e &= (a_i)_{i\in I} * \big(e_{G_i}\big)_{i\in I} = \big(a_i *_i e_{G_i}\big)_{i\in I} = (a_i)_{i\in I} = a, \\
a^{-1} * a &= \big(a_i^{-1}\big)_{i\in I} * (a_i)_{i\in I} = \big(a_i^{-1} *_i a_i\big)_{i\in I} = \big(e_{G_i}\big)_{i\in I} = e \\
a * a^{-1} &= (a_i)_{i\in I} * \big(a_i^{-1}\big)_{i\in I} = \big(a_i *_i a_i^{-1}\big)_{i\in I} = \big(e_{G_i}\big)_{i\in I} = e
\end{aligned}
$$

Thus e is an identity of $*$ and a^{-1} is an inverse of a. Hence $(G, *)$ is a group and the lemma is proved. □

Example 1.9.11. Let A and B be groups and define

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

Show that π is a homomorphism and apply the First Isomorphism Theorem to π.

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

and so π is an homomorphism.

$$\operatorname{Im}\pi = \{\pi(a,b) \mid (a,b) \in A \times B\} = \{b \mid a \in A, b \in B\} = B,$$

$$\operatorname{Ker}\pi = \{(a,b) \in A \times B \mid \pi(a,b) = e_B\} = \{(a,b) \in A \times B \mid b = e_B\} = \{(a, e_B) \mid a \in A\} = A \times \{e_B\}.$$

The First Isomorphism Theorem 1.9.6 now shows that

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

Example 1.9.12. Consider the subgroups

$$A := \langle (13) \rangle = \{(1), (13)\} \quad \text{and} \quad B := \langle (13), (24) \rangle = \langle (1), (13), (24), (13)(24) \rangle$$

of D_4. Then $|A| = 2, |B| = 4$ and $|D_4| = 8$. So by 1.8.3(2) we have $A \trianglelefteq B$ and $B \trianglelefteq D_4$. But

$$((14)(23))^{-1} \circ (13) \circ (14)(23) = (2,4) \notin A$$

and so A is not a normal subgroup of D_4, see 1.8.6

Lemma 1.9.13. *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) *Let $\alpha : G \to F$ be a homomorphism of groups. Then the restriction*

$$\alpha_H : \quad H \to F, \quad h \mapsto \alpha(h).$$

is a a homomorphism of groups. Moreover,

$$\mathrm{Ker}\alpha_H = H \cap \mathrm{Ker}\alpha \quad \textit{and} \quad \mathrm{Im}\,\alpha_H = \alpha(H)$$

and if α is 1-1, then also α_H is 1-1.

Proof. (a) Follow immediately from the Subgroup Group Proposition.

(b) Suppose $T \trianglelefteq G$. Then $T \leq G$ and (a) shows that $T \leq H$. Let $h \in H$. Then $h \in G$ and since $T \trianglelefteq G$ we get $hT = Th$. So $T \trianglelefteq H$.

(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

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

So $\mathrm{Ker}\alpha_H = H \cap \mathrm{Ker}\alpha$. Also $\mathrm{Im}\,\alpha_H = \{\alpha_H(h) \mid h \in H\} = \{\alpha(h) \mid h \in H\} = \alpha(H)$.
Suppose α is 1-1. If $\alpha_H(a) = \alpha_H(b)$, then $\alpha(a) = \alpha(b)$ and so $a = b$. Thus α_H is 1-1. □

Theorem 1.9.14 (Second Isomorphism Theorem)**.** *Let G be a group, $N \trianglelefteq G$ and $A \leq G$. Then*

(a) *AN is a subgroup of G.*

(b) *N is a normal subgroup of AN.*

(c) *$A \cap N$ is a normal subgroup of A.*

(d) *The function*

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

is a well-defined isomorphism.

(e) *$A/A \cap N \cong AN/N$.*

Proof. (a) 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.
(b) Since $N \trianglelefteq G$ 1.9.13(b) implies that $N \trianglelefteq AN$.
(c) By 1.9.4

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

is homomorphism with $\mathrm{Ker}\pi = N$. Hence by 1.9.13(c) the restriction

$$\pi_A : A \to G/N, \quad a \to aN$$

is a homomorphism with

$$(*) \qquad \mathrm{Ker}\pi_A = A \cap \mathrm{Ker}\pi = A \cap N$$

By 1.9.2 $\mathrm{Ker}\pi_A \trianglelefteq A$, so $A \cap N$ is a normal subgroup of A.

(d) We will apply the First Isomorphism Theorem to π_A. For this we compute

$$\begin{aligned}
\mathrm{Im}\,\pi_A &= \{\pi_A(a) \mid a \in A\} && -\text{ definition of } \mathrm{Im} \\
&= \{aN \mid a \in A\} && -\text{ definition of } \pi_A \\
&= \{a(nN) \mid n \in N, a \in A\} && - nN = N \text{ for all } n \in N, \text{ see } 1.7.7(b) \\
&= \{(an)N) \mid n \in N, a \in A\} && - 1.8.1(c) \\
&= \{dN \mid d \in AN\} && -\text{ definition of } AN \\
&= AN/N && -\text{ definition of } AN/N
\end{aligned}$$

So

$$(**) \qquad \mathrm{Im}\,\pi_A = AN/N.$$

From the First Isomorphism Theorem 1.9.6 we know that

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

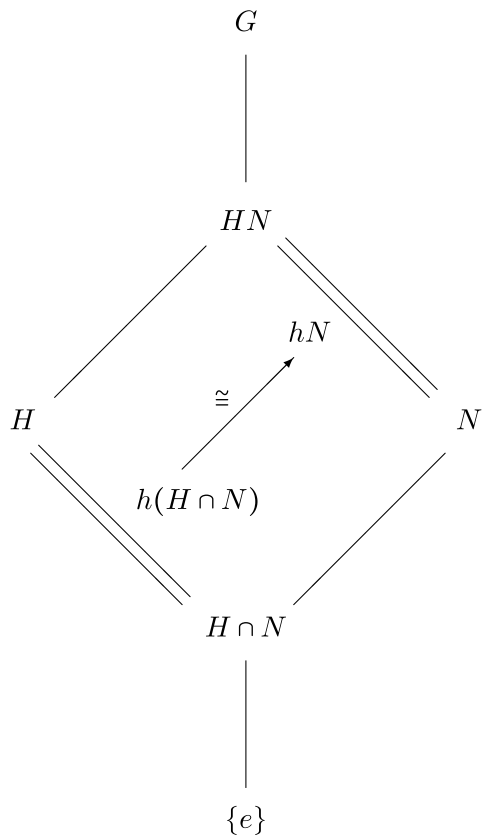
is a well-defined isomorphism. Thus by$(*)$ and $(**)$

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

is a well-defined isomorphism.

(e) follows from (d). $\square$

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



Example 1.9.15. Let

$$H := \{f \in \mathrm{Sym}(4) \mid f(4) = 4$$

and note that $H \cong \mathrm{Sym}(3)$.

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

By Homework 4 N is a normal subgroup of G. By Lagrange

$$|G/N| = \frac{|G|}{|N|} = \frac{24}{4} = 6.$$

The only element f in N with $f(4) = 4$ is $f = (1)$. Thus

$$(*) \qquad H \cap N = 1$$

Hence

$$\begin{aligned} HN/N &\cong H/H\cap N && \text{– Second Isomorphism Theorem}\\ &\cong H/\{(1)\} && \text{– }(*)\\ &\cong H && \text{– First Isomorphism Theorem applied to } \mathrm{id}_H : H \to H, h \mapsto h \end{aligned}$$

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

(a) *If $A \le G$ 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, then $\phi(A) \trianglelefteq H$.*

(c) *If $B \le H$, 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) Consider the restriction $\phi_A : A \to H, a \mapsto \phi(a)$. By 1.9.13(c) ϕ_A is a homomorphism and and $\mathrm{Im}\,\phi_A = \phi(A)$. By 1.6.5(c), $\mathrm{Im}\,\phi_A \le H$, so $\phi(A) \le H$.

(b) By (a) $\phi(A) \le H$. Hence by 1.8.6(f) 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

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

Since $A \trianglelefteq G$, 1.8.6(f) implies $aga^{-1} \in A$. So $(*)$ shows that $hbh^{-1} \in \phi(A)$. 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

$$(**) \qquad \phi(x) \in B \text{ and } \phi(y) \in B.$$

In particular, since $\phi(xy) = \phi(x)\phi(y)$ and B is closed under multiplication we conclude 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) $\phi(x^{-1}) = \phi(x)^{-1}$. As $\phi(x) \in B$ and B is closed under inverses we get $\phi(x)^{-1} \in B$. 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 $\phi^{-1}(B) \le G$.

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

$$(***) \qquad \phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1}.$$

As $B \trianglelefteq H$ we know that B is invariant under conjugation in H. Since $\phi(x) \in B$ we get $\phi(g)\phi(x)\phi(g)^{-1} \in B$. Hence $(***)$ gives $gxg^{-1} \in \phi^{-1}(B)$. Thus $\phi^{-1}(B)$ is invariant under conjugation and so 1.8.6(f) shows that $\phi^{-1}(B) \trianglelefteq G$. □

Theorem 1.9.17 (Correspondence Theorem)**.** *Let N be a normal subgroup of the group G. Put*

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

Let

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

be the natural homomorphism.

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

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

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

(d) *The function*

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

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 $N \le K \le G$, 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 $N \le K$ and $F = K/N$. Moreover, $K = \pi^{-1}(F)$.*

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

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

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

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

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

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

(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 $g \in gN = kN \subseteq K$. Thus $g \in K$ if and only if $gN \in K/N$.

(d) Let $N \leq H \leq G$ and $F \leq G/N$. We will first show that β and α are well-defined, that is $H/N \leq G/N$ and $N \leq \pi^{-1}(F) \leq G$.

By (a) $H/N = \pi(H)$ and so by 1.9.16(a) $H/N \leq G/N$.

By 1.9.16(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 $N \leq \pi^{-1}(N)$.

So β and α are well-defined. We compute

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

Since π onto, A.2.5 implies $\pi\big(\pi^{-1}(F)\big) = F$ 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, 1.9.16(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 1.9.16(d) $K \trianglelefteq N$.

(f) We have

$$\begin{array}{lll} & H \subseteq K & \\ \iff & h \in K \text{ for all } h \in H & - \text{definition of } \subseteq \\ \iff & hN \in K/N \text{ for all } h \in H & - \text{(c)} \\ \iff & T \in K/N \text{ for all } T \in H/N & - H/N = \{hN \mid h \in H\} \\ \iff & H/N \subseteq K/N & - \text{definition of } \subseteq \end{array}$$

(g) Let

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

be the natural homomorphism. Consider the composition:

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

Since η and π are homomorphism, also $\eta \circ \pi$ is homomorphism (see Homework 3). 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 $\operatorname{Ker}(\eta \circ \pi)$:

$$\begin{array}{rcl}
 & g \in \operatorname{Ker}(\eta \circ \pi) & \\
\iff & (\eta \circ \pi)(g) = e_{(G/N)/(H/N)} & - \ \text{Definition of } \operatorname{Ker}(\eta \circ \pi) \\
\iff & \eta(\pi(g)) = e_{(G/N)/(H/N)} & - \ \text{Definition of } \circ \\
\iff & \pi(g) \in \operatorname{Ker}\eta & - \ \text{Definition of } \operatorname{Ker}\eta \\
\iff & \pi(g) \in H/N & - \ 1.9.4 \\
\iff & gN \in H/N & - \ \text{Definition of } \pi \\
\iff & g \in H & - \ (c)
\end{array}$$

Thus

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

By the First Isomorphism Theorem 1.9.6

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

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.

□

Lemma 1.9.18. *Consider the infinite cyclic group $(\mathbb{Z}, +)$ and observe that the k'th power of n in $(\mathbb{Z}, +)$ is nk.*

(a) *Let $n \in \mathbb{Z}$. Then $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.*

(b) *Let $m \in \mathbb{Z}$ with $m \neq 0$. Then $\mathbb{Z} \to m\mathbb{Z}, k \mapsto mk$ is an isomorphism of groups.*

(c) *Let* $H \leq \mathbb{Z}$*. Then* $H = m\mathbb{Z}$ *for a unique* $m \in \mathbb{N}$*.*

(d) *Let* $n, m \in \mathbb{Z}$*. Then* $n\mathbb{Z} \leq m\mathbb{Z}$ *if and only if* $m|n$ *in* $\mathbb{Z}$*.*

Proof. (a) follows from 1.5.10(4).

(b): By (a) $n\mathbb{Z}$ is an infinite cyclic group with generator n. Hence (a) follows from 1.9.7

(c) Note that $0 = e_{\mathbb{Z}} \in H$. If $H = \{0\}$, then $H = 0\mathbb{Z}$ and (b) holds. So suppose $H \neq \{0\}$. 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 (c) is proved.

(d) By (a) $n\mathbb{Z}$ is the smallest subgroup of $\mathbb{Z}$ containing n. Thus $n\mathbb{Z} \subseteq \mathbb{Z}$ if and only if $n \in m\mathbb{Z}$ and so if and only of $n = mk$ for some $k \in \mathbb{Z}$.

□

Lemma 1.9.19. *Let* n *be a positive integer and consider the cyclic group* $(\mathbb{Z}_n, +)$ *of order* n*. Let* $F \leq (\mathbb{Z}_n, +)$*.*

(a) $F = \mathbb{Z}_m/\mathbb{Z}_n$ *for a unique* $m \in \mathbb{Z}^+$ *with* $m|n$*.*

(b) $F = \langle m + \mathbb{Z}_n \rangle$

(c) $\mathbb{Z}_n/F \cong \mathbb{Z}_m$*.*

(d) $F \cong \mathbb{Z}_{\frac{n}{m}}$*.*

Proof. (a) By the Correspondence Theorem $F = H/n\mathbb{Z}$ for some subgroup H of $\mathbb{Z}$ with $n\mathbb{Z} \leq H$. By 1.9.18(b) we have $H = m\mathbb{Z}$ for a unique $m \in \mathbb{N}$. Since $n\mathbb{Z} \leq H = m\mathbb{Z}$ we get $m \neq 0$ and $m \mid n$, see 1.9.18(c). Thus (a) holds.

(b) Follows from $m\mathbb{Z} = \langle m \rangle$ and (a).

(c) By the Third Isomorphism Theorem

$$\mathbb{Z}_n/F = \mathbb{Z}/nZ \Big/ m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

(d) From (c) we get $\left|\mathbb{Z}/n\mathbb{Z} \Big/ m\mathbb{Z}/n\mathbb{Z}\right| = \left|\mathbb{Z}/m\mathbb{Z}\right| = m$. Note also that $|\mathbb{Z}/n\mathbb{Z}| = n$. By Lagrange Theorem applied to the subgroup $m\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$,

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

Thus

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

and so

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

By (b) H is cyclic and so by 1.9.7

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

□

Example 1.9.20. Determine all subgroups and the corresponding quotients of $\mathbb{Z}_{12}$.

The divisors of 12 are $1, 2, 3, 4, 6$, and 12 and so the subgroups are $\mathbb{Z}_{12}$ are

$$1\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_{12}, \quad 2\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_6, \quad 3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_4 \quad 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_3, \quad 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_2, \quad 12\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_1$$

The corresponding quotient groups are isomorphic to

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

Example 1.9.21. Find all subgroups of $\mathrm{Sym}(3)$. Which ones are normal?

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

If $|K| = 2$, then by 1.7.18 K is cyclic and so by 1.7.16(a), $K = \langle g \rangle$ for some $g \in K$. The elements of order 2 in $\mathrm{Sym}(3)$ 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 $\mathrm{Sym}(3)$ 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 $\mathrm{Sym}(3)$ are

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

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

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

Example 1.9.22. Let $N = \langle(1,2)(3,4), (1,3)(2,4)\rangle \le \mathrm{Sym}(4)$. Find all subgroups of $\mathrm{Sym}(4)$ containing N. Which ones are normal?

Put

$$H := \{f \in \mathrm{Sym}(4) \mid f(4) = 4\} \cong \mathrm{Sym}(3)$$

By Example 1.9.15 $N \trianglelefteq \mathrm{Sym}(4)$ and

$$\begin{array}{rcl} \mathrm{Sym}(4)/N = HN/N & \xrightarrow{\cong} H/H \cap N = H/\{(1)\} \xrightarrow{\cong} & H \\ hN & \longrightarrow h(H \cap N) = h\{(1)\} = \{h\} \longrightarrow & h \end{array}$$

Thus

$$\phi : \quad H \to \mathrm{Sym}(4)/N, \quad h \mapsto hN.$$

is an isomorphism. So we can obtain the subgroups of G/N by computing $\phi(K)$ for each subgroups K of H:

$$\begin{aligned}
\phi(\{1\}) &= \{(1)N\} \\
&= \Big\{\{(1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}\Big\}
\end{aligned}$$

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

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

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

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

$$\phi(H) = \mathrm{Sym}(4)/N$$

By the Correspondence Theorem 1.9.17 the function

$$\mathcal{S}(\mathrm{Sym}(4)/N) \to \mathcal{S}(\mathrm{Sym}(4),N), \quad F \to \pi^{-1}(F)$$

is a bijection and

$$\pi^{-1}(F) = \bigcup_{T\in F} T$$

So taking the unions of the above sets of cosets gives us the subgroups of Sym(4) containing N:

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

By the 1.9.17 $F \trianglelefteq \mathrm{Sym}(4)/N$ if and only if $\pi^{-1}(F) \trianglelefteq \mathrm{Sym}(4)$. So the normal subgroups of Sym(4) containing N are

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

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*

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

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

$$* : \quad G \times G \to G, \quad (a,g) \mapsto a * g$$

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) Let I be a set. We claim that

$$\diamond : \quad \mathrm{Sym}(I) \times I \to I, \quad (f,i) \mapsto f(i)$$

is an action of $\mathrm{Sym}(I)$ on I. Indeed, $\mathrm{id}_I \diamond i = \mathrm{id}_I(i) = i$ and so (act:i) holds. Moreover,

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

for all $f,g \in \mathrm{Sym}(I)$ and $i \in I$ and so (act:ii) holds.

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

$$\begin{aligned} \diamond: \qquad \mathrm{GL}_2(\mathbb{F}) \times \mathbb{F}^2 &\to \mathbb{F}^2 \\ (A, v) &\mapsto Av \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \right) &\mapsto \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \end{aligned}$$

is an action of $\mathrm{GL}_2(\mathbb{F})$ on $\mathbb{F}^2$. Recall that the identity element in $GL_2(\mathbb{F})$ is the identity matrix $\begin{bmatrix} 1_{\mathbb{F}} & 0_{\mathbb{F}} \\ 0_{\mathbb{F}} & 1_{\mathbb{F}} \end{bmatrix}$. Since

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

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) *Let $\diamond$ be an action of G on I. For $a \in G$ define*

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

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

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

is a homomorphism with $\Phi_\diamond(a)(i) = a \diamond i$ for all $a \in G$ and $i \in I$. $\Phi_\diamond$ is called the homomorphism associated to the action of *G on I.*

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

$$\diamond_\Phi: \quad G \times I \to I, \quad (g, i) \mapsto \Phi(g)(i).$$

Then $\diamond_\Phi$ is an action of G on I, called the action of G on I associated to Φ.

(c) *Let $\diamond$ be an action of G on I. Then $\diamond_{\Phi_\diamond} = \diamond$.*

(d) *$\Phi : G \to \mathrm{Sym}(I)$ be a homomorphisms of groups. Then $\Phi_{\diamond_\Phi} = \Phi$.*

Proof. Let $a, b \in G$ and $i \in I$.

(a) Since $f_e(i) = e \diamond i = i$ we have

$$(*) \qquad f_e = \mathrm{id}_I.$$

Note that

$$f_{ab}(i) = (ab) \diamond i = a \diamond (b \diamond i) = f_a\big(f_b(i)\big) = (f_a \circ f_b)(i)$$

and so

$$(**) \qquad f_{ab} = f_a \circ f_b.$$

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

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

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

Write Φ for $\Phi_\diamond$. Then

$$\Phi(ab) = f_{ab} \overset{(**)}{=} f_a \circ f_b = \Phi(a) \circ \Phi(b)$$

and so Φ is a homomorphism. Also $\Phi(a)(i) = f_a(i) = a \diamond i$ and so (a) holds.

(b) We will write $\diamond$ for $\diamond_\Phi$. By 1.6.5(a), $\Phi(e) = e_{\mathrm{Sym}(I)} = \mathrm{id}_I$. Thus

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

and (act:i) holds.

Also

$$(ab) \diamond i = \Phi(ab)(i) \overset{\Phi \text{ hom}}{=} (\Phi(a) \circ \Phi(b)(i) = \Phi(a)\big(\Phi(b)(i)\big) = a \diamond (b \diamond i),$$

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

(c) Let $g \in G$ and $i \in I$. Then

$$g \diamond_{\Phi_\diamond} i = \Phi_\diamond(g)(i) = g \diamond i.$$

So $\diamond_{\Phi_\diamond} = \diamond$

(d) Let $g \in G$ and $i \in I$. Then

$$\Phi_{\diamond_\Phi}(g)(i) = g \diamond_\Phi i = \Phi(g)(i)$$

Since this holds for all $i \in I$ we have $\Phi_{\diamond_\Phi}(g) = \Phi(g)$. So $\Phi_{\diamond_\Phi} = \Phi$. □

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

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

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. Recall first that

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

Put

$$a := D_4, \quad b := (1,2)D_4, \quad \text{and} \quad c := (2,3)D_4.$$

Since $(1,2) \notin D_4$, $a \neq b$. Since $(2,3) \notin D_4$, $a \neq c$ and since $(1,2)^{-1} \circ (2,3) = (1,2) \circ (2,3) = (1,2,3) \notin D_4$, $b \neq c$. By Lagrange's Theorem $|G/D_4| = \frac{|G|}{|D_4|} = \frac{24}{8} = 3$. Hence

$$G/D_4 = \{a, b, c\}.$$

We now compute how $(1,2),(2,3)$ and $(3,4)$ act on G/D_4. We start with $(1,2)$:

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

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

and

$$(1,2)c = (1,2)(2,3)D_4 = (1,2,3)D_4.$$

Is $(1,2,3)D_4$ equal to a, b or c? Since the function $f_{(1,2)} : G/D_4 \to G/D_4, T \mapsto (1,2)T$ is a bijection we must have

(1.3) $$(1,2)c = c.$$

So $(1,2,3)D_4 = (2,3)D_4$. This can also be verified directly: $(2,3)^{-1} \circ (1,2,3) = (1,3) \in D_4$ and so $(2,3)D_4 = (1,2,3)D_4$.

Let Φ be the homomorphism from G to $\mathrm{Sym}(G/D_4)$ associated to the action of G on $G/D_4 = \{a,b,c\}$. From (1.1),(1.2) and (1.3):

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

Next we consider $(2,3)$:

(2.1) $$(2,3)a = (2,3)D_4 = c,$$

(2.2) $$(2,3)c = (2,3)(2,3)D_4 = D_4 = a,$$

and since $f_{(2,3)}$ is a bijection

(2.3) $$(2,3)b = b.$$

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

(2) $$\Phi\big((2,3)\big) = f_{(2,3)} = (a,c).$$

(3.1) $$(3,4)b = (3,4)(1,2) \circ D_4 = D_4 = a$$

(3.2) $$(3,4)a = (3,4)(3,4)b = b$$

and since $f_{(3,4)}$ is a bijection,

(3.3) $$(3,4)c = c.$$

From (3.1),(3.2) and (3.3):

(3) $$\Phi\big((3,4)\big) = f_{(3,4)} = (a,b).$$

What is $\mathrm{Im}\,\Phi$? We will compute $\Phi(g)$ for a few elements $g \in \mathrm{Sym}(4)$.

Since $(1,2)(2,3) = (1,2,3)$ and Φ is a homomorphism, we have

(4) $$\Phi\big((1,2,3)\big) = \Phi\big((1,2)\big)\Phi\big((2,3)\big) = (a,b)\circ(a,c) = (a,b,c),$$

and

(5) $$\Phi\big((1,3,2)\big) = \Phi\left((1,2,3)^{-1}\right) = \Phi\big(((1,2,3)\big)^{-1} = (a,b,c)^{-1} = (a,c,b).$$

Clearly

(6) $$\Phi\big((1)\big) = (a).$$

From (1)-(6), Φ is onto and so the First Isomorphism Theorem shows that

$$G/\mathrm{Ker}\Phi = \mathrm{Im}\,\Phi = \mathrm{Sym}\big(\{a,b,c\}\big) \cong \mathrm{Sym}(3).$$

In particular, $|G/\mathrm{Ker}\Phi| = |\mathrm{Sym}(3)| = 6$. By Lagrange's $|G/\mathrm{Ker}\Phi| = \frac{|G|}{|\mathrm{Ker}\Phi|} = \frac{24}{|\mathrm{Ker}\Phi|}$ and so $|\mathrm{Ker}\Phi| = 4$. What is $\mathrm{Ker}\phi$? Note that $\Phi(1,2) = (a,b) = \Phi(3,4)$ and so

$$(1,2)(3,4) = (1,2)^{-1}\circ(3,4) \in \mathrm{Ker}\Phi$$

Since $\mathrm{Ker}\Phi$ is a normal subgroup of G, all conjugates of $(1,2)(3,4)$ are in $\mathrm{Ker}\Phi$. Hence all elements of cycle type $(2,2)$ are in $\mathrm{Ker}\Phi$, so

$$N := \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \subseteq \mathrm{Ker}\Phi.$$

Since $|N| = 4 = |\mathrm{Ker}\Phi|$ this gives $N = \mathrm{Ker}\Phi$. In particular, $N \trianglelefteq G$ and

$$\mathrm{Sym}(4)/N = \mathrm{Sym}(4)/\mathrm{Ker}\Phi = \mathrm{Sym}\big(\{a,b,c\}\big) \cong \mathrm{Sym}(3).$$

Of course we already proved this once before in Example 1.9.15.

Lemma 2.1.7 (Cancellation Law for Action)**.** *Let G be a group acting on the set I, $a \in G$ and $i,j \in I$. Then*

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

(b) $i = j \quad\Longleftrightarrow\quad ai = aj$.

(c) $j = ai \quad\Longleftrightarrow\quad i = a^{-1}j$.

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)

$$\begin{aligned} & j = ai \\ \iff & a^{-1}j = a^{-1}(ai) \quad - \quad (b) \\ \iff & a^{-1}j = i \quad - \quad (a) \end{aligned}$$

$\square$

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 Homework 4 N is a normal subgroup of G. Hence by Homework 6,

$$\diamond : \quad \mathrm{Sym}(4) \times N \to N, (g, n) \to gng^{-1}$$

is an action of $\mathrm{Sym}(4)$ on N. Let $n \in N$, then

$$\mathrm{Sym}(4) \diamond n = \{g \diamond n \mid g \in \mathrm{Sym}(4)\} = \{gng^{-1} \mid \mathrm{Sym}(4)\}.$$

Thus $\mathrm{Sym}(4) \diamond n$ consists of all conjugates of n under $\mathrm{Sym}(4)$, that is all the elements of the same cycle type as n. Thus

$$\mathrm{Sym}(4) \diamond e = \{e\}.$$

and

$$\mathrm{Sym}(4) \diamond (1,2)(3,4) = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Lemma 2.1.10. *Let $\diamond$ be an action of the group G on the set I.*

(a) '$\equiv_\diamond \pmod{G}$ ' *an equivalence relation on I.*

(b) *Let $i \in I$ and let $[i]_\diamond$ the equivalence class of '$\equiv_\diamond \pmod{G}$' containing i. Then $[i]_\diamond = G \diamond i$.*

Proof. Let $i, j, k \in I$. From $ei = i$ we conclude that $i \equiv i \pmod{G}$. So '$\equiv \pmod{G}$' is reflexive.

Suppose $i \equiv j \pmod{G}$. Then $j = gi$ for some $g \in G$. Hence 2.1.7(c) shows that $g^{-1}j = i$. Thus $j \equiv i \pmod{G}$, so '$\equiv \pmod{G}$' is symmetric.

Suppose $i \equiv j \pmod{G}$ 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.

$$[i]_\diamond = \{j \in I \mid i \equiv j \pmod{G}\} = \{j \in I \mid j = gi \text{ for some } g \in G\} = \{gi \mid g \in G\} = Gi$$

□

Proposition 2.1.11. *Let G be a group acting on the set I and $i, j \in I$. Then following are equivalent.*

(a) *$j = gi$ for some $g \in G$.*

(b) *$i \equiv j \pmod{G}$*

(c) *$j \in Gi$.*

(d) *$Gi \cap Gj \neq \varnothing$*

(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 of $\equiv \pmod{G}$ 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 $i, j \in I$ 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 statements 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 of 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): Suppose G acts transitively on I and let $i, j \in I$. Then $j = gi$ for some $g \in G$. Thus $j \in Gi$ and so $Gi = I$.

(b) $\Longrightarrow$ (c): Suppose $Gi = I$ for all $i \in I$. Since I is not empty, there exists $i \in I$. Then $I = Gi$ and (c) holds.

(c) $\Longrightarrow$ (d): Suppose $I = Gi$ for some $i \in I$. By definition, Gi is an orbit of G on I and so (d) holds.

(d) $\Longrightarrow$ (e): Suppose I is an orbit of G on I. Let O be any orbit of G on I. Then both O and I are orbits for G on I and $O \cap I = O \neq \varnothing$. Thus 2.1.11 shows that $O = I$. Thus I is the only orbit for G on I and (e) holds.

(e) $\Longrightarrow$ (f): Suppose G has exactly one orbit, say O, on I and let $i, j \in I$. Both Gi and Gj are orbits for G on I and $Gi = O = Gj$.

(f) $\Longrightarrow$ (g): Suppose $Gi = Gj$ for all $i, j \in I$. Let $i, j \in I$. Then $Gi = Gj$ and so by 2.1.11 $i \equiv j \pmod G$.

(g) $\Longrightarrow$ (a): Suppose $i \equiv j \pmod G$ for all $i, j \in I$. Let $i, j \in I$. . Then $i \equiv j \pmod G$ and so $j = gi$ for some $g \in G$. Hence G acts transitively 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 a bijective G-homomorphism. We say that I and J are isomorphic G-sets and write*

$$I \cong_G J$$

if there exists a 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 $\diamond$.*

Example 2.1.15. (1) Recall that by 2.1.2(2), $\mathrm{Sym}(n)$ acts on $\{1,2,3,\dots,n\}$ 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

$$\mathrm{Stab}^{\diamond}_{\mathrm{Sym}(5)}(\{2,3\}) = \{f \in \mathrm{Sym}(5) \mid f(2) = 2 \text{ and } f(3) = 3\} \cong \mathrm{Sym}(\{1,4,5\}) \cong \mathrm{Sym}(3).$$

(2) Consider the action

$$\diamond : \quad G \times G \to G, \quad (g,h) \mapsto ghg^{-1}$$

if G on G by conjugation. Then

$$\mathrm{Stab}^{\diamond}_{G}(h) = \{g \in G \mid g \diamond h = h\} = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = \mathrm{C}_G(h)$$

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*

$$\phi : \quad G/H \to Gi, \quad aH \mapsto ai$$

is a well-defined G-isomorphism

In particular

$$G/H \cong_G Gi, \quad |Gi| = |G/\mathrm{Stab}_G(i)| \quad \text{and} \quad |Gi| \text{ divides } |G|$$

Proof. Let a, b in G. Then

$$\begin{array}{rcll} & ai = bi & & \\ \iff & a^{-1}(ai) = a^{-1}(bi) & - & 2.1.7(c) \\ \iff & i = (a^{-1}b)i & - & 2.1.7(a), \text{(act ii)} \\ \iff & a^{-1}b \in H & - & H = \mathrm{Stab}(i), \text{ Definition of Stab} \\ \iff & aH = bH & - & 1.7.6(c),(g) \end{array}$$

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. □

Corollary 2.1.17. *Let G be a group.*

(a) *Let $H \le G$. Then the action*

$$G \times G/H \to H/H \quad (g, T) \to gT$$

of G on G/H is transitive.

(b) *Suppose G acts transitively on the non-empty set I. Let $i \in I$ and put $H = \mathrm{Stab}_G(i)$. Then G/H and I are isomorphic G-sets.*

Proof. (a) Let $T \in G/H$. Then $T = gH = g \diamond H$ for some $g \in G$. Thus $G \diamond H = G/H$ and 2.1.13 shows that G acts transtively on G/H.

(b) By 2.1.16 G/H and Gi are isomorphic G-sets. Since G acts transitively, we know that $I = Gi$, see 2.1.13. Thus $G/H \cong_H I$. □

Example 2.1.18. 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

$$(*) \qquad H = \{f \in \mathrm{Sym}(n) \mid f(n) = n\} \cong \mathrm{Sym}(n-1).$$

Then by 2.1.16

$$(**) \qquad \mathrm{Sym}(n)/H \cong \{1, 2, 3 \ldots, n\} \text{ as } \mathrm{Sym}(n)\text{-sets}.$$

Thus

$$\frac{|\mathrm{Sym}(n)|}{|\mathrm{Sym}(n-1)|} \overset{(*)}{=} \frac{|\mathrm{Sym}(n)|}{|H|} \overset{(**)}{=} |\{1, 2, 3 \ldots, n\}| = n,$$

so

$$|\mathrm{Sym}(n)| = n \cdot |\mathrm{Sym}(n-1)|$$

Since $|\mathrm{Sym}(1)| = 1 = 1!$, induction on n shows that $|\mathrm{Sym}(n)| = n!$.

Theorem 2.1.19 (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 of G on I. For each $1 \le k \le n$ let i_k be an element of I_k. Then*

$$|I| = \sum_{i=1}^{n} |I_k| = \sum_{i=1}^{n} |G/\mathrm{Stab}_G(i_k)|.$$

Proof. By 2.1.11 I is the disjoint union of the I_k's. Hence

$$(*) \qquad |I| = \sum_{k=1}^{n} |I_k|.$$

By 2.1.11 $I_k = Gi_k$ and so 2.1.16 implies

$$(**) \qquad |I_k| = |Gi| = |G/\mathrm{Stab}_G(i_k)| \quad \text{for all } 1 \le k \le n.$$

Substituting $(**)$ into $(*)$ gives the theorem. □

Example 2.1.20. Define

$$H := \left\{ f \in \mathrm{Sym}(5) \;\middle|\; f\big(\{1,2\}\big) = \{1,2\} \right\}.$$

For example $(1,2)$, $(3,4)$, and $(1,2)(3,5,4)$ are elements of H, but $(1,3)(2,5)$ is not.

Let $f \in H$. Then $f\big(\{1,2\}\big) = \{1,2\}$ and since f is a bijection we conclude that $f\big(\{3,4,5\}\big) = \{3,4,5\}$. Hence the function

$$H \to \mathrm{Sym}(\{1,2\}) \times \mathrm{Sym}(\{3,4,5\}), \quad f \mapsto \left(f|_{\{1,2\}} \,, f|_{\{3,4,5\}} \right)$$

is an isomorphism. In particular, $H \cong \mathrm{Sym}(2) \times \mathrm{Sym}(3)$ and $|H| = 2 \cdot 6 = 12$.

What are the orbits of H on $\{1,2,3,4,5\}$ with respect to the action

$$\diamond : \quad H \times \{1,2,3,4,5\} \to \{1,2,3,4,5\}, \quad (f,i) \mapsto f(i)$$

Let $f \in H$. 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.

Note that $f \in \mathrm{Stab}_H(1)$ if and only if $f(1) = 1$. Since $f\big(\{1,2\}\big) = \{1,2\}$, we see that $f(1) = 1$ implies $f(2) = 2$, but $f|_{\{3,4,5\}}$ is still an arbitrary element of $\mathrm{Sym}(\{3,4,5\})$. It follows that

$$\mathrm{Stab}_H(1) \cong \mathrm{Sym}(\{3,4,5\}) \cong \mathrm{Sym}(3).$$

In particular, $|\mathrm{Stab}_H(1)| = 3! = 6$.

Also $f \in \mathrm{Stab}_H(3)$ if and only if $f(3) = 3$. Since $f\big(\{3,4,5\}\big) = \{3,4,5\}$, we see that $f(3) = 3$ implies that $f\big(\{4,5\}\big) = \{4,5\}$, thus

$$\mathrm{Stab}_H(3) \cong \mathrm{Sym}(\{1,2\}) \times \mathrm{Sym}(\{4,5\}) \cong \mathrm{Sym}(2) \times \mathrm{Sym}(2).$$

In particular, $|\mathrm{Stab}_H(3)| = 2! \cdot 2! = 4$.

The Orbit Equation 2.1.19 implies that

$$|H/\mathrm{Stab}_H(1)| + |H/\mathrm{Stab}_H(3)| = |\{1,2,3,4,5\}|.$$

As seen above $|H| = 12$, $|\mathrm{Stab}_H(1)| = 6$ and $|H/\mathrm{Stab}_H(3)| = 4$. So using Lagrange's Theorem the orbit equation becomes

$$\frac{12}{6} + \frac{12}{4} = 5,$$

that is

$$2 + 3 = 5.$$

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. Let $n \in \mathbb{Z}^+$. Then $|\mathbb{Z}_n| = n$. So $\mathbb{Z}_n$ is a p-group if and only if n is a power of p. So
$\mathbb{Z}_1$ is a p-group for every prime p.
$\mathbb{Z}_2$ 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, and*

(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 $|G| = p^k l$ for some $k \in \mathbb{N}$ and $l \in \mathbb{Z}^+$ with $p \nmid l$.*

(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 2.2.4(b) shows $\langle (1,2) \rangle$ is a Sylow 2-subgroup of $\mathrm{Sym}(3)$.

$\langle (1,2,3) \rangle$ has order 3 and so is a Sylow 3-subgroup of $\mathrm{Sym}(3)$.

(b) $|\mathrm{Sym}(4)| = 4! = 24 = 2^3 \cdot 3$.

D_4 is a subgroup of order eight of $\mathrm{Sym}(4)$ and so D_4 is a Sylow 2-subgroup of $\mathrm{Sym}(4)$.

$\langle (1,2,3) \rangle$ is a Sylow 3-subgroup of $\mathrm{Sym}(4)$.

(c) $|\mathrm{Sym}(5)| = 5! = 5 \cdot 24 = 2^3 \cdot 3 \cdot 5$.

So D_4 is a Sylow 2-subgroup of $\mathrm{Sym}(5)$,

$\langle(1,2,3)\rangle$ is a Sylow 3-subgroup of $\mathrm{Sym}(5)$, and

$\langle(1,2,3,4,5)\rangle$ is a Sylow 5-subgroup of $\mathrm{Sym}(5)$.

(d) $|\mathrm{Sym}(6)| = 6! = 6 \cdot 5! = 2^4 \cdot 3^2 \cdot 5$.

Note that $D_4 \times \langle(5,6)\rangle$ is a subgroup of order 16 of $\mathrm{Sym}(6)$ and so is a Sylow 2-subgroup of $\mathrm{Sym}(6)$.

$\langle(1,2,3)\rangle \times \langle(4,5,6)\rangle$ is a group of order 9, and so is a Sylow 3-subgroup of $\mathrm{Sym}(6)$.

$\langle(1,2,3,4,5)\rangle$ is a Sylow 5-subgroup of $\mathrm{Sym}(6)$.

Proposition 2.2.6. *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. Define

$$m := \max\{\, |Q| \mid Q \text{ is a } p\text{-subgroup of } G \text{ with } P \le Q\}.$$

Choose a p-subgroup S of G with $P \le S$ and $|S| = m$. Let Q be a p-subgroup of G with $S \le Q$. Then $P \le Q$ and so $|Q| \le m$ by definition of m. Since $S \le Q$ we have $m = |S| \le |Q|$. Thus $|Q| = m = |S|$ and since $S \le Q$ we get $Q = S$. Thus S is indeed a maximal p-subgroup of G, that is a Sylow p-subgroup.

In particular, the p-subgroup $\{e\}$ of G is contained in a Sylow p-subgroup of G and so G has Sylow p-subgroup. $\square$

Definition 2.2.7. *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*

$$\mathrm{Fix}_I(G) = \{i \in I \mid gi = i \textit{ for all } g \in G\}.$$

Lemma 2.2.8 (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 $I_1, I_2, \dots, I_n$ be the distinct orbits of P on I. Let m be the number of orbits of size 1 and choose notation such that

$$(*) \qquad |I_l| = 1 \text{ for } 1 \le l \le m \quad \text{and} \quad |I_l| > 1 \text{ for } m+1 \le l \le n.$$

Fix $i \in I$ and pick $1 \le l \le n$ with $i \in I_l$. By 2.1.11

$$(**) \qquad I_l = Gi.$$

We have

$$\begin{array}{rcll} & i \in \mathrm{Fix}_I(P) & & \\ \iff & gi = i \text{ for all } g \in G & - & \text{Definition of } \mathrm{Fix}_I(P) \\ \iff & Gi = \{i\} & - & \text{Definition of } Gi \\ \iff & |Gi| = 1 & - & \text{since } i \in Gi \\ \iff & |I_l| = 1 & - & (**) \\ \iff & l \le m & - & (*) \end{array}$$

Thus

$$(***) \qquad \mathrm{Fix}_I(P) = \bigcup_{l=1}^{m} I_l.$$

Let $m+1 \le l \le n$. By 2.1.16 $|I_l|$ divides $|P|$. Since $|P|$ is a power of p, we conclude that $|I_l| = p^t$ for some $t \in \mathbb{N}$. As $|I_l| \ne 1$ we have $t \ge 1$. Thus $p \big| |I_l|$ and so

$$(+) \qquad |I_l| \equiv 0 \pmod p \quad \text{for all } m+1 \le l \le n.$$

We compute

$$|I| \overset{2.1.19}{=} \sum_{l=1}^{n} |I_l| = \sum_{l=1}^{m} |I_l| + \sum_{l=m+1}^{n} |I_l| \overset{(***)}{=} |\mathrm{Fix}_I(P)| + \sum_{l=m+1}^{n} |I_l|,$$

and so by (+)

$$|I| \equiv |\mathrm{Fix}_I(P)| \pmod p.$$

□

Example 2.2.9. Let $P = \langle (1,2,3),(4,5,6) \rangle \le \mathrm{Sym}(8) \rangle$. Then P has order 9 and so P is a 3-group. The orbits of P on $I := \{1,2,3,\dots,8\}$ are $\{1,2,3\}$, $\{4,5,6\}$, $\{7\},\{8\}$. The fixed-points of P on I are 7 and 8. So $|\mathrm{Fix}_I(P)| = 2$, $|I| = 8$ and $8 \equiv 2 \pmod 3$, as predicted by 2.2.8.

Definition 2.2.10. *Let $\diamond$ be an action of the group G on the set I.*

(a) *$\mathcal{P}(I)$ is the set of all subsets of I. $\mathcal{P}(I)$ is called the* power set *of I.*

(b) *For $a \in G$ and $J \subseteq I$ define $a \diamond J := \{a \diamond j \mid j \in J\}$.*

(c) $\diamond_{\mathcal{P}}$ *denotes the function*

$$\diamond_{\mathcal{P}}: \quad G \times \mathcal{P}(I) \to \mathcal{P}(I), \quad (a, J) \mapsto a \diamond J$$

(d) *Let* $J \subseteq I$ *and* $H \subseteq G$*. Then* J *is called* H-invariant *if*

$$h \diamond j \in J$$

for all $h \in H, j \in J$*.*

(e) *Let* $H \leq G$ *and* J *an* H*-invariant subset of* I*. Then* $\diamond_{H,J}$ *denotes the function*

$$\diamond_{H,J}: \quad H \times J \to J, \quad (h, j) \to h \diamond j$$

Lemma 2.2.11. *Let* $\diamond$ *be an action of the group* G *on the set* I*.*

(a) $\diamond_{\mathcal{P}}$ *is an action of* G *on* $\mathcal{P}(I)$*.*

(b) *Let* $H \leq G$ *and let* J *be a* H*-invariant subset of* I*. Then* $\diamond_{H,J}$ *is an action of* H *on* J*. In particular,* $h \diamond J = J$ *for all* $h \in H$*.*

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 1.5.4 $e_H = e_G$ 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. □

Lemma 2.2.12. *Let* $\alpha : G \to K$ *be an isomorphism of groups and* $H \leq G$*. Let* p *be a prime.*

(a) $\alpha(H)$ *is a subgroup of* K *isomorphic to* H*.*

(b) *Suppose* H *is a* p*-subgroup of* G*. Then* $\alpha(H)$ *is a* p*-subgroup of* K*.*

(c) *Suppose* H *is a Sylow* p*-subgroup of* G*. Then* $\alpha(H)$ *is a Sylow* p*-subgroup of* K*.*

Proof. (a) See Homework 6#3.

(b) By (b) we have $|\alpha(H)| = |H| = p^k$ for some $k \in \mathbb{N}$. So $\alpha(H)$ is a p-group.

(c) By (b) we know that $\alpha(H)$ is a p-subgroup of H. Let Q be p-subgroup of K with $\alpha(H) \leq Q$. By Homework 6#3, α^{-1} is an isomorphism, so (b) applied to α^{-1} shows that $\alpha^{-1}(Q)$ is a p-subgroup of H. Since $\alpha(H) \leq Q$ we get $H \leq \alpha^{-1}(Q)$. As H is a Sylow p-subgroup of G this gives $H = \alpha^{-1}(Q)$ and so $\alpha(H) = \alpha(\alpha^{-1}(Q)) = Q$. Thus $\alpha(H)$ is a Sylow p-subgroup of G. □

Definition 2.2.13. *Let A and B be subsets of the group G.*

(a) *We say that A is* conjugate *to B in G if there exists $g \in G$ with $A = gBg^{-1}$.*

(b) $\mathrm{N}_G(B) := \{g \in G \mid B = gBg^{-1}\}$. *$\mathrm{N}_G(B)$ is called the normalizer of B in G.*

Corollary 2.2.14. *Let G be a group, H a subgroup of G and $a \in G$. Let p be a prime.*

(a) *aHa^{-1} is a subgroup of G isomorphic to H. In other words, conjugate subgroups of G are isomorphic.*

(b) *Suppose H is a p-subgroup of G. Then aHa^{-1} is p-subgroup of G.*

(c) *Suppose H is a Sylow p-subgroup of G. Then aHa^{-1} is Sylow p-subgroup of G*

Proof. By Homework 3#2 $\alpha : G \to G, g \mapsto aga^{-1}$ is an isomorphism. Observe that

$$\alpha(H) = \{\alpha(h) \mid h \in H\} = \{aha^{-1} \mid h \in H\} = aHa^{-1},$$

so the Corollary follows from 2.2.12 □

Lemma 2.2.15. *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 2.2.11(a), G acts on $\mathcal{P}(G)$ by conjugation. By 2.2.14(c) we know that $aHa^{-1} \in \mathrm{Syl}_p(G)$ for all $H \in \mathrm{Syl}_p(G)$. Thus $\mathrm{Syl}_p(G)$ is a G-invariant subset of $\mathcal{P}(G)$. Hence the lemma follows from 2.2.11(b) □

Lemma 2.2.16. *Let G be a group.*

(a) *Let $B \subseteq G$. Then $\mathrm{N}_G(B) = \mathrm{Stab}_G^\diamond(B)$, where $\diamond$ is the action of G on $\mathcal{P}(G)$ by conjugation. In particular, $\mathrm{N}_G(B)$ is a subgroup of G.*

(b) *Let $B \leq G$. Then $B \trianglelefteq \mathrm{N}_G(B)$.*

(c) *Let $B \leq G$ and $A \leq \mathrm{N}_G(B)$. Then $AB \leq \mathrm{N}_G(B)$ and, if G is finite, $|AB| = \frac{|A||B|}{|A \cap B|}$.*

Proof. (a) $\mathrm{N}_G(B) = \{g \in G \mid gBg^{-1} = B\} = \{g \in G \mid g \diamond B = B\} = \mathrm{Stab}_G^\diamond(B)$.

(b) By definition $gBg^{-1} = B$ for all $g \in \mathrm{N}_G(B)$. So $B \trianglelefteq \mathrm{N}_G(B)$ by 1.8.6.

(c) Let $a \in A$. Then $aBa^{-1} = B$. So $aB = Ba$. Hence

$$AB = \{ab \mid b \in B\} = \bigcup_{a \in A} \{ab \mid b \in B\} = \bigcup_{a \in A} aB = \bigcup_{a \in A} Ba = BA.$$

So Homework 4#4 shows that $AB \leq \mathrm{N}_G(B)$. We compute

$$\begin{aligned}
|AB| &= |AB/B||B| && \text{– Lagrange's Theorem} \\
&= |A/A \cap B||B| && \text{– Second Isomorphism Theorem} \\
&= \frac{|A|}{|A \cap B|}|B| && \text{– Lagrange's Theorem}
\end{aligned}$$

□

Theorem 2.2.17. *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 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.*

(c) *Let $S \in \mathrm{Syl}_p(G)$. Then $|\mathrm{Syl}_p(G)| = |G/\mathrm{N}_G(S)|$.*

Proof. By 2.2.15 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

$(*)$ *P has a unique fixed-point on $\mathrm{Syl}_p(G)$, 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 $P \leq \mathrm{N}_G(Q)$. Thus 2.2.16 implies that PQ is a subgroup of G and

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}.$$

Since P and Q are p-groups, we conclude that $|P|$, $|Q|$ and $|P \cap Q|$ 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 we get $P = PQ$. Similarly, since $Q \leq PQ$ and Q is a maximal p-subgroup of G we have $Q = PQ$. Thus $P = Q$ and $(*)$ is proved.

Next we show:

$(**)$ $$|I| \equiv 1 \pmod p.$$

By $(*)$ $\mathrm{Fix}_I(P) = \{P\}$. Hence $|\mathrm{Fix}_I(P)| = 1$. By 2.2.8 $|I| \equiv |\mathrm{Fix}_I(P)| \pmod p$ and so $(**)$ holds.

Finally we prove:

$(***)$ *I is the unique orbit of G on $\mathrm{Syl}_p(G)$.*

For this let J be an orbit for G on $\mathrm{Syl}_p(G)$. By $(**)$ applied to J in place of I we have

$$|J| \equiv 1 \pmod p$$

Hence $p \nmid |J|$ and 2.2.8 shows that $\mathrm{Fix}_J(P) \neq \varnothing$. Pick $Q \in \mathrm{Fix}_J(P)$. Then $(*)$ implies $P = Q \in J$. As $P \in I$ we get $I \cap J \neq \varnothing$ and 2.1.11 gives $J = I$.

Thus $(***)$ holds.

By $(***)$ and 2.1.13 we conclude that G acts transitively on $\mathrm{Syl}_p(G)$ and $I = \mathrm{Syl}_p(G)$. In particular, (a) holds.

By $(**)$ $|I| \equiv 1 \pmod p$ and so also $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$.

By 2.2.16, $\mathrm{N}_G(S) = \mathrm{Stab}_G^{\diamond}(S)$, where $\diamond$ is the action of G on $\mathrm{Syl}_p(G)$ by conjugation. Since G acts transitively on $\mathrm{Syl}_p(G)$, the Corollary 2.1.17 to the Isomorphism Theorem for G-sets shows that $\mathrm{Syl}_p(G)$ and $G/\mathrm{Stab}^{\diamond}(S)$ are isomorphic G-sets. Thus $|\mathrm{Syl}_p(G)| = |G/\mathrm{Stab}_G^{\diamond}(S)| = |G/\mathrm{N}_G(S)|$. Now Lagrange's Theorem implies that $|\mathrm{Syl}_p(G)|$ divides $|G|$. □

Lemma 2.2.18. *Let X be a set and $n \in \mathbb{N}$. Then $\mathrm{Sym}(n)$ acts on X^n via*

$$a \diamond (x_1, x_2, \ldots x_n) = (x_{a^{-1}(1)}, x_{a^{-1}(2)}, \ldots, x_{a^{-1}(n)}).$$

Proof. Let $e = e_{\mathrm{Sym}(n)}$. Then $e^{-1}(i) = i$ for all $1 \leq i \leq n$ and so also $e \diamond x = x$ for all $x \in X^n$. Thus (act:i) holds.

Let $a, b \in \mathrm{Sym}(n)$ and $x = (x_1, \ldots, x_n) \in X^n$. Put $y := b \diamond x$ and $z := a \diamond (b \diamond x) = a \diamond y$. Let $1 \leq i \leq n$. Then

$$y_i = x_{b^{-1}(i)}$$

and

$$z_i = y_{a^{-1}(i)} = x_{b^{-1}(a^{-1}(i))} = x_{(b^{-1} \circ a^{-1})(i)} = x_{(a \circ b)^{-1}(i)}.$$

Hence $a \diamond (b \diamond x) = z = (a \circ b) \diamond x$ and also (act:ii) holds. □

Example 2.2.19. Consider $n = 5$ and $X = \{a, b, c, d, e, f\}$. Compute $(1, 5, 3) \diamond (b, a, e, f, d)$.

Put $x = (b, a, e, f, d)$ and $h = (1, 5, 3)$. Then $h^{-1} = (1, 3, 5)$.

i	1	2	3	4	5
$h^{-1}(i)$	3	2	5	4	1
$x_{h^{-1}(i)}$	e	a	d	f	b

Thus

$$(1, 5, 3) \diamond (b, a, e, f, d) = (e, a, d, f, b).$$

So the b in the first position is moved to the fifth position, the a in the second position stays in the second position, the e in the third position is moved to the first position and so on.

Theorem 2.2.20 (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 2.2.18. Let $h := (p, p-1, \ldots, 2, 1) \in \mathrm{Sym}(p)$ and $H := \langle h \rangle$. Then H is a subgroup of order p of $\mathrm{Sym}(p)$. Observe that

$$h^{-1} = (1, 2, \ldots, p) = \frac{1 \quad 2 \quad \ldots \quad p-1 \quad p}{2 \quad 3 \quad \ldots \quad p \quad 1}$$

and so

$$(*) \qquad h \diamond (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

Hence h fixes $(g_1, g_2, \ldots, g_p)$ if and only if $(g_2, g_3, \ldots, g_p, g_1) = (g_1, g_2, \ldots, g_{p-1}, g_p)$ and so if and only if $g_1 = g_2, g_2 = g_3, \ldots, g_{p-1} = g_p, g_p = g_1$. Thus

$$(**) \qquad \mathrm{Fix}_{G^p}(h) = \{(g, g, \ldots, g) \mid g \in G\}.$$

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 $(**)$

$$(***) \qquad \mathrm{Fix}_J(H) = \{(g, g, \ldots, g) \mid g \in G, g^p = e\}.$$

In particular

$$(+) \qquad (e, \ldots, e) \in \mathrm{Fix}_J(H).$$

Our goal is now to show that $|\mathrm{Fix}_J(H)| > 1$. For this we will use the Fixed-Point-Formula 2.2.8 for H on acting on J. But we first must make sure that H acts on J. By 2.2.11(b), we need to verify that J is H-invariant. Let $(g_1, g_2, \ldots g_p) \in J$. Then

$$g_1 g_2 \ldots g_p = e.$$

Multiplying with g_1^{-1} from the left and g_1 from the right gives

$$g_2 g_3 \ldots g_p g_1 = e,$$

and so

$$(g_2, g_3, \ldots, g_p, g_1) \in J.$$

Thus $h \diamond x \in J$ for all $x \in J$. Hence $h \diamond J \subseteq J$. Note that $h^{n+1} \diamond J = h^n \diamond (h \diamond J) \subseteq h^n \diamond J$. So induction on n shows that $h^n \diamond J \subseteq J$ for all $n \in \mathbb{N}$. As $H = \langle h \rangle = \{h^i \mid 0 \le i < p\}$ we conclude that J is an H-invariant subset of G^n. Thus by 2.2.11(b), H acts on J and so by 2.2.8

$$(++) \qquad |J| \equiv |\mathrm{Fix}_J(H)| \pmod p.$$

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, namely $g_p = (g_1 \dots g_p)^{-1}$. Since p divides $|G|$ we conclude that $p \,\Big|\, |J|$ and so (++) implies

$$p \,\Big|\, |\mathrm{Fix}_J(H)|.$$

By (+) $(e, \dots, e) \in \mathrm{Fix}_J(H)$. Hence $|\mathrm{Fix}_J(H)| \ge 1$ and so $|\mathrm{Fix}_J(H)| \ge p \ge 2$. Thus we can choose $x \in \mathrm{Fix}_J(H)$ with $x \ne (e, \dots, e)$. By $(***)$ there exists $g \in G$ with $x = (g, \dots, g)$ and $g^p = e$. As $x \ne (e, \dots, e)$ we have $g \ne e$. Since $g^p = e$ we get $|g| \,\big|\, p$, see 1.5.10(4). As p is a prime and $|g| \ne 1$, this gives $|g| = p$. □

Theorem 2.2.21 (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,*

$$\mathrm{Syl}_p(G) = \{P \le G \mid |P| = p^k\}$$

and G has a subgroup of order p^k.

Proof. Let $S \in \mathrm{Syl}_p(G)$. Since S is a p-group we have $|S| = p^m$ for some $m \in \mathbb{N}$. Put $N := \mathrm{N}_G(S)$. By 2.2.16 we have $S \trianglelefteq N$.

Suppose for a contradiction that p divides $|N/S|$. Then by Cauchy's Theorem N/S has a subgroup P of order p. By the Correspondence Theorem, there exists a subgroup Q of N with $S \le Q$ and $P = Q/S$. Lagrange's Theorem shows that

$$|Q| = |Q/S||S| = |P||S| = pp^m = p^{m+1}.$$

Thus Q is a p-subgroup of G with $S \le Q$ and $S \ne Q$. But this a contradicts $S \in \mathrm{Syl}_p(G)$.

Thus p does not divide $|N/S|$. By 2.2.17 we have

$$|G/N| = |\mathrm{Syl}_P(G)| \equiv 1 \pmod p.$$

So p does not divide $|G/N|$. Two application of Lagrange's Theorem give

$$|G| = |G/N||N| = |G/N||N/S||S| = p^m n, \quad \text{where}\, n := |G/N||N/S|$$

Since p divides neither G/N nor N/S, we get $p \nmid n$. Since $p^m n = |G| = p^k l$ conclude that $p^n = p^k$. Thus $|S| = p^k$.

We proved that any p-Sylow subgroup of G has order p^k. Conversely by 2.2.4(b) any subgroup of order p^k of G is a Sylow p-subgroup of G, so

$$\mathrm{Syl}_p(G) = \{P \le G \mid |P| = p^k\}.$$

□

Example 2.2.22. (1) Find the Sylow 2-subgroups of Sym(3).

We have $|\mathrm{Sym}(3)| = 3! = 2 \cdot 3$. The subgroups of order 2 of Sym(3) are $\langle(1,2)\rangle, \langle(1,3)\rangle$ and $\langle(2,3)\rangle$ and so by the First Sylow Theorem

$$\mathrm{Syl}_2\big(\mathrm{Sym}(3)\big) = \{\langle(1,2)\rangle, \langle(1,3)\rangle, \langle(2,3)\rangle\}.$$

(2) Find and count the Sylow 5-subgroups of Sym(5)

We have $|\mathrm{Sym}(5)| = 5! = 2^3 \cdot 3 \cdot 5$. So the Sylow 5-subgroups are the subgroups of order 5. Let $H \le \mathrm{Sym}(5)$ with $|H| = 5$. Let $(1) \ne h \in H$. Then $|h| = 5$ and so $h = (a,b,c,d,e)$ is five cycle. There are 120 choices for the tuple (a,b,c,d,e). But any of the five cycles

$$(a,b,c,d,e),\ (b,c,d,e,a),\ (c,d,e,a,b),\ (d,e,a,b,c),\ (e,a,b,c,d)$$

is also equal to h. Hence there are $\frac{120}{5} = 24$ elements of order five in Sym(5). Since $H = \langle h\rangle$ any of the four elements of order five in H uniquely determines 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 Theorem.

(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 2.2.23. *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 and if and only if $|\mathrm{Syl}_p(G)| = 1$.*

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(e) if and only if S is normal in G. □

Example 2.2.24. (1) $\langle(1,2,3)\rangle$ is the only Sylow 3-subgroup of Sym(3) and so $\langle(1,2,3)\rangle \trianglelefteq \mathrm{Sym}(3)$ by 2.2.23.

(2) Sym(3) has three Sylow 2-subgroups, and so $\langle(1,2)\rangle \ntrianglelefteq \mathrm{Sym}(3)$ by 2.2.23.

Definition 2.2.25. *A group G is called* simple *if $\{e\}$ and G are the only normal subgroups of G.*

Example 2.2.26. Let G be a simple group of order 168. We will show that G is isomorphic to a subgroup of $\mathrm{Sym}(8)$.

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 2.2.23 $s_7 \neq 1$. Since $|G| = 168 = 7 \cdot 24$, the Third Sylow Theorem implies that $s_7 \equiv 1 \pmod 7$ and $s_7 \big| |G|$. Hence $s_7 \mid 24$. 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 $s_7 = 8$.

Put $I := \mathrm{Syl}_7(G)$ and let $\phi : G \to \mathrm{Sym}(I)$ be the homomorphism associated to the action of G on I by conjugation (see 2.1.3(a)). So for g in G we have $\phi(g)(S) = gSg^{-1}$.

Suppose that $\mathrm{Ker}\phi = G$. Then $\phi(g) = e_{\mathrm{Sym}(I)} = \mathrm{id}_I$ for all $g \in G$ and so

$$S = \phi(g)(S) = gSg^{-1}.$$

for all $g \in G$. Thus by 1.8.6(e), $S \trianglelefteq G$, a contradiction, since G is simple.

Hence $\mathrm{Ker}\phi \neq G$. By 1.9.2 $\mathrm{Ker}\phi \trianglelefteq G$. Since G is simple we get $\mathrm{Ker}\phi = \{e\}$. Thus by 1.9.3 ϕ is 1-1 and so by 1.6.5(d),

$$(*) \qquad G \cong \mathrm{Im}\,\phi \leq \mathrm{Sym}(I)$$

Since $|I| = |\mathrm{Syl}_7(G)| = s_7 = 8$, there exist a bijection $\beta : I \to \{1, 2, \dots, 8\}$. Hence by Homework 3#6 there exists an isomorphism $\alpha : \mathrm{Sym}(I) \to \mathrm{Sym}(8)$.

Thus Homework 6#3 shows that $\mathrm{Im}\,\phi \cong \alpha(\mathrm{Im}\,\phi) \leq \mathrm{Sym}(8)$. Since $G \cong \mathrm{Im}\,\phi$ we conclude $G \cong \alpha(\mathrm{Im}\,\phi)$, see Homework 6#1, and so G is isomorphic to a subgroup of $\mathrm{Sym}(8)$.

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* $k \diamond v$.

Notation 3.1.2. $\mathbb{K}$ *be field and* $(V, +, \diamond)$ *be vector space.*

(a) 0_V *denotes the identity of* $+$ *in* V.

(b) *Let* $v \in V$. *Then* $-v$ *denotes the inverse of* v *with respect to* $+$.

(c) *Let* $n \in \mathbb{Z}$ *and* $v \in V$. *Then* nv *denotes the* n*'th power of* v *with respect to* $+$.

Example 3.1.3. 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

$$k \diamond (a_0 + a_1 x + \dots a_n x^n) = (ka_0) + (ka_1)x + \dots (ka_n x^n)$$

for all $k, a_0, \dots, a_n \in \mathbb{K}$.

Lemma 3.1.4. *Let $\mathbb{K}$ be a field and V a field.*

(a) $0_{\mathbb{K}} v = v$ *for all* $v \in \mathbb{K}$.

(b) $(-1_{\mathbb{K}})v = -v$ *for all* $v \in V$.

(c) $k0_V = 0_V$ *for all* $k \in \mathbb{K}$.

(d) *Let $n \in \mathbb{N}$, let $a \in \mathbb{K}$, let $(k_1, \dots, k_n)$ and $(l_1 \dots, l_n)$ be lists in $\mathbb{K}$ and let $(v_1, \dots, v_n)$ be a list in V. Then*

$$a \sum_{i=1}^{n} k_i v_i = \sum_{i=1}^{n} (ak_i) v_i$$

and

$$\sum_{i=1}^{n} k_i v_i \ + \ \sum_{i=1}^{n} l_i v_i = \sum_{i=1}^{n} (k_i + l_i) v_i$$

Proof. I will just write 1 for $1_{\mathbb{K}}$ and 0 for $0_{\mathbb{K}}$.

(a) :

$$0 \diamond v + 0_V = 0 \diamond v = (0+0) \diamond v = (0 \diamond v) + (0 \diamond v).$$

So by the Cancellation Law 1.4.7, $0 \diamond v = 0_V$.

(b):

$$0_V = 0 \diamond v = (1 + (-1)) \diamond v = (1 \diamond v) + (-1) \diamond v = v + (-1) \diamond v.$$

So by 1.4.8(c), $(-1) \diamond v = -v$.

(c)

$$0_V + k \diamond 0_V = k \diamond 0_V = k \diamond (0_V + 0_V) = k \diamond 0_V + k \diamond 0_V$$

and so by the Cancellation Law 1.4.7, $k \diamond 0_V = 0_V$.

(d) Is readily verified. □

Definition 3.1.5. *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 for all $a_1, a_2, \dots, a_n \in \mathbb{K}$:*

$$a_1 v_1 + a v_2 + \dots a v_n = 0_V \quad \Longrightarrow \quad a_1 = a_2 = \dots = a_n = 0_{\mathbb{K}}.$$

(b) *Let* $(a_1, a_2 \ldots, a_n) \in \mathbb{K}^n$. *Then* $a_1v_1 + a_2v_2 + \ldots + a_nv_n$ *is called a* $\mathbb{K}$-linear combination *of* $\mathcal{L}$.

$$\mathrm{Span}_{\mathbb{K}}(\mathcal{L}) = \{a_1v_1 + a_2v_2 + \ldots a_nv_n \mid (a_1, \ldots, a_n) \in \mathbb{K}^n\}$$

is called the $\mathbb{K}$-span *of* $\mathcal{L}$. *In other words,* $\mathrm{Span}_{\mathbb{K}}(\mathcal{L})$ *consists of all the* $\mathbb{K}$*-linear combination of* $\mathcal{L}$. *Recall that an empty sum is defined to be* 0_V, *so* 0_V *is linear combination of the empty list* $()$ *and* $\mathrm{Span}_{\mathbb{K}}\big(()\big) = \{0_V\}$.

(c) *We say that* $\mathcal{L}$ spans V *over* $\mathbb{K}$, *if* $V = \mathrm{Span}_{\mathbb{K}}(\mathcal{L})$, *that for all* $v \in V$ *there exists* $k_1, \ldots, k_n \in \mathbb{K}$ *with*

$$v = k_1v_1 + \ldots k_nv_n.$$

(d) *We say that* $\mathcal{L}$ *is a* basis *of* V *if* $\mathcal{L}$ *is* $\mathbb{K}$*-linearly independent and spans* V *over* $\mathbb{K}$.

(e) *We say that* $\mathcal{L}$ *is a* $\mathbb{K}$-linearly dependent *if it's not linearly independent, that is, if there exist* $k_1, \ldots, k_n \in \mathbb{K}$, *not all* $0_{\mathbb{K}}$ *such that*

$$k_1v_1 + kv_2 + \ldots kv_n = 0_V.$$

Example 3.1.6. (1) Put $e_i = (0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \ldots, 0_{\mathbb{K}}) \in \mathbb{K}^n$ where the $1_{\mathbb{K}}$ is in the i-position. Then $(e_1, e_2, \ldots, e_n)$ is a basis for $\mathbb{K}^n$, called the *standard basis* of $\mathbb{K}^n$.

(2) $(1_{\mathbb{K}}, x, x^2, \ldots x^n)$ 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 3.1.7. *Let* $\mathbb{K}$ *be a field,* V *a* $\mathbb{K}$*-space and* $\mathcal{L} = (v_1, \ldots, v_n)$ *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* $k_1, \ldots, k_n \in \mathbb{K}$ *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 $k_1, \ldots, k_n$ with

$$v = \sum_{i=1}^{m} k_iv_i.$$

Suppose that also $l_1, \ldots, l_n \in \mathbb{K}$ with

$$v = \sum_{i=1}^{m} l_iv_i.$$

Then

$$\sum_{i=1}^{m}(k_i - l_i)v_i = \sum_{i=1}^{m} k_iv_i - \sum_{i=1}^{m} l_iv_i = 0_V.$$

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 $k_1, \dots, k_n \in \mathbb{K}$ 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 $k_1 = k_2 = \dots = k_n = 0_{\mathbb{K}}$. Hence $\mathcal{L}$ is linearly independent and thus a basis for V. □

Lemma 3.1.8. *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. The $\mathcal{L}$ is linearly dependent if and only if there exists $1 \le i \le n$ such that v_i is linear combination of $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$.*

Proof. $\Longrightarrow$: Suppose $\mathcal{L}$ is linearly dependent. Then there exists $k_1, \dots, k_n \in \mathbb{K}$, not all $0\mathbb{K}$ such that

$$\sum_{i=1}^{n} k_i v_i = 0_V.$$

Choose $1 \le i \le i$ with $k_i \ne 0$. Then

$$k_i v_i = -\sum_{\substack{j=1 \\ j \ne i}}^{n} k_j v_j$$

and so

$$v_i = \sum_{\substack{j=1 \\ j \ne i}}^{n} (k_i^{-1} k_j) v_j$$

is a linear combination of $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$.

$\Longleftarrow$: Suppose next that $1 \le i \le n$ and v_i is linear combination of $(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$. Then

$$v_i = k_1 v_1 + \dots + k_{i-1} v_{i-1} + k_{i+1} v_{i+1} + \dots + k_n v_n$$

for some $k_j \in \mathbb{K}$. Thus

$$k_1 v_1 + \dots + k_{i-1} v_{i-1} + (-1_{\mathbb{K}}) v_i + k_{i+1} v_{i+1} + \dots + k_n v_n = 0_V.$$

Since $-1_{\mathbb{K}} \ne 0_K$ this shows that $\mathcal{L}$ is linearly dependent. □

Lemma 3.1.9. *Let $\mathbb{K}$ be field, V an $\mathbb{K}$-space and $\mathcal{L} = (v_1, v_2, \dots v_n)$ a 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. We will show that $(a) \Longleftrightarrow (b)$ and that $(a) \Longleftrightarrow (c)$.

(a) $\Longrightarrow$ (b): Suppose $\mathcal{L}$ is basis. Then $\mathcal{L}$ spans V and $\mathcal{L}$ is linearly independent. By 3.1.8 the latter implies that v_i is not a linear combination of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. So $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ does not span V. Thus $\mathcal{L}$ is a minimal spanning list.

(b) $\Longrightarrow$ (a): Suppose $\mathcal{L}$ is a minimal spanning list. Then $\mathcal{L}$ spans V so we only need to show that $\mathcal{L}$ is linearly independent. Suppose not. Then by 3.1.8 there exists $1 \leq i \leq n$ such that v_i is linear combination of $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. Without loss, $i = 1$. Then

$$v_1 = \sum_{i=2}^{n} k_i v_i).$$

for some $k_i \in \mathbb{K}$. Let $v \in V$. Since $\mathcal{L}$ spans V we know that

$$v = \sum_{i=1}^{n} a_i v_i$$

for some $a_i \in \mathbb{K}$. Thus

$$v = a_1 \left(\sum_{i=2}^{n} k_i v_i \right) + \sum_{i=2}^{n} a_i v_i = \sum_{i=2}^{n} (a_1 k_i + a_i) v_i.$$

Thus $v \in \operatorname{Span}(v_2, \ldots, v_n)$. Hence $(v_2, \ldots, v_n)$ spans V, a contradiction to the definition of a minimal spanning list.

(a) $\Longrightarrow$ (c): Suppose $\mathcal{L}$ is basis of V and let $v \in V$. Then $\mathcal{L}$ spans V, so v is a linear combination of $\mathcal{L}$. Thus 3.1.8 shows that $(v_1, v_2, \ldots, v_n, v)$ is linearly dependent, so $\mathcal{L}$ is maximal linear independent list.

(c) $\Longrightarrow$ (a): Suppose $\mathcal{L}$ is maximal linear independent list. Then $\mathcal{L}$ 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. □

Definition 3.1.10. *Let $\mathbb{K}$ be a field and V and W $\mathbb{K}$-spaces. A* $\mathbb{K}$-linear function *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 function 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 3.1.11. (1) The function $\mathbb{K}^2 \to \mathbb{K}$, $(a, b) \mapsto a$ is $\mathbb{K}$-linear.

(2) The function $\mathbb{K}^3 \to \mathbb{K}^2$, $(a, b, c) \mapsto (a + 2b, b - c)$ is $\mathbb{K}$-linear.

(3) We claim that the function $f : \mathbb{K} \to \mathbb{K}$, $k \mapsto k^2$ 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 $k = k - 1_{\mathbb{K}}$. Hence $k = 0_K$ or $k = 1_K$ and thus $\mathbb{K} = \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}$.

(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

$$D : \quad \mathbb{K}[x] \to \mathbb{K}[x], \quad f \mapsto f'$$

is a $\mathbb{K}$-linear function.

Lemma 3.1.12. *Let $\mathbb{K}$ be a field and V and W be $\mathbb{K}$-spaces. Suppose that $(v_1, v_2, \dots, v_n)$ is basis of V and let $w_1, w_2, \dots w_n \in W$. Then*

(a) *There exists a unique $\mathbb{K}$-linear function $f : V \to W$ with $f(v_i) = w_i$ for each $1 \le i \le n$.*

(b) $f(\sum_{i=1}^{n} k_i v_i) = \sum_{i=1}^{n} k_i w_i$. *for all $k_1, \dots, k_n \in \mathbb{K}$.*

(c) *f is 1-1 if and only if $(w_1, w_2, \dots, w_n)$ is linearly independent.*

(d) *f is onto if and only if $(w_1, w_2, \dots, w_n)$ spans W.*

(e) *f is an isomorphism if and only if $(w_1, w_2, \dots, w_n)$ 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

$$(*) \qquad f\left(\sum_{i=1}^{n} k_i v_i\right) = \sum_{i=1}^{n} k_i f(v_i) = \sum_{i=1}^{n} k_i w_i.$$

for all $k_1, \dots, k_n \in \mathbb{K}$.

So (b) holds. Moreover, since $(v_1, \dots v_n)$ spans V, each v in V is of the form $\sum_{i=1}^{n} k_i v_i$ and so by $(*)$, $f(v)$ is uniquely determined. Thus f is unique.

It remains to show the existence of f. Since $(v_1, \dots, v_n)$ is a basis for V, any $v \in V$ can by uniquely written as $v = \sum_{i=1} k_i v_i$. So we obtain a well-defined function

$$f : \quad V \to W, \quad \sum_{i=1}^{n} k_i v_i \to \sum_{i=1}^{n} k_i w_i.$$

It is now readily verified that f is $\mathbb{K}$-linear and $f(v_i) = w_i$. So f exists.

(c)

$$\begin{array}{llllll}
 & & f \text{ is 1-1} & & & \\
\iff & & \mathrm{Ker} f = \{0_V\} & & & -\ 1.9.3 \\
\iff & \text{for all } v \in V : & f(v) = 0_W & \Longrightarrow & v = 0_V & -\ \text{Definition of Ker} f \\
\iff & \text{for all } k_1, \dots, k_n \in \mathbb{K} : & f(\sum_{i=1}^{n} k_i v_i) = 0_W & \Longrightarrow & \sum_{i=1}^{n} k_i v_i = 0_V & -\ (v_1, \dots, v_n) \text{ spans } V \\
\iff & \text{for all } k_1, \dots, k_n \in \mathbb{K} : & f(\sum_{i=1}^{n} k_i v_i) = 0_W & \Longrightarrow & k_1 = \dots = k_n = 0_{\mathbb{K}} & -\ (v_1, \dots, v_n) \text{ is lin. indep.} \\
\iff & \text{for all } k_1, \dots, k_n \in \mathbb{K} : & \sum_{i=1}^{n} k_i w_i = 0_W & \Longrightarrow & k_1 = \dots k_n = 0_{\mathbb{K}} & -\ \text{(b)} \\
\iff & & (w_1, \dots, w_n) & \text{is linearly indep.} & & -\ \text{Definition of lin. indep.}
\end{array}$$

So (c) holds.

(d) We compute

$$\begin{aligned}
\mathrm{Im}\, f &= \{f(v) \mid v \in V\} && -\ \text{Defintion of Im}\, f \\
&= \left\{ f(\sum_{i=1}^{n} k_i v_i) \;\middle|\; k_1, \dots k_n \in \mathbb{K} \right\} && -\ (v_1, \dots, v_n) \text{ spans } V \\
&= \left\{ \sum_{i=1}^{n} a_i w_i \;\middle|\; k_1, \dots k_n \in \mathbb{K} \right\} && -\ \text{(b)} \\
&= \mathrm{Span}(w_1, w_2, \dots, w_n) && -\ \text{Definition of Span}
\end{aligned}$$

Note that f is onto if and only if $\operatorname{Im} f = W$, if and only of $\operatorname{Span}(w_1, \ldots, w_n) = W$, and if and only if $(w_1, \ldots, w_n)$ spans W.

(e) follows from (c) and (d). $\square$

Corollary 3.1.13. *Let $\mathbb{K}$ be a field and W a $\mathbb{K}$-space with basis $(w_1, w_2 \ldots, w_n)$. Then the function*

$$f: \quad \mathbb{K}^n \to W, \quad (a_1, \ldots a_n) \mapsto \sum_{i=1}^{n} a_i w_i$$

is a $\mathbb{K}$-isomorphism. In particular,

$$W \cong_{\mathbb{K}} \mathbb{K}^n.$$

Proof. By Example 3.1.6(1), $(e_1, e_2, \ldots, e_n)$ is basis for $\mathbb{K}^n$. Also $f(e_i) = w_i$ and so by 3.1.12 f is an isomorphism. $\square$

Definition 3.1.14. *Let $\mathbb{K}$ be a field and $(V, +, \diamond)$ a $\mathbb{K}$-space. A $\mathbb{K}$-subspace of $(V, +, \diamond)$ is a $\mathbb{K}$-space $(W, \oplus, \square)$ such that and $W \subseteq V$. Then W is called a* $\mathbb{K}$-subspace *of V provided that*

(I) $W \subseteq V$.

(II) $u \oplus w = u + w$ *for all* $u, w \in W$.

(III) $k \square w = k \diamond w$ *for all* $k \in \mathbb{K}$ *and* $w \in W$.

Proposition 3.1.15 (Subspace Proposition)**.** *Let $\mathbb{K}$ be a field, V a $\mathbb{K}$-space and W a subset of V. Define*

$$\oplus : W \times W \to W, \quad (u, w) \to u + w$$

and

$$\square : \mathbb{K} \times W \to W, \quad (k, w) \to k \diamond w.$$

Then $(W, \oplus, \square)$ is well-defined $\mathbb{K}$-subspace of $(V, +, \square)$ if and only if

(i) $0_V \in W$.

(ii) $v + w \in W$ *for all* $v, w \in W$.

(iii) $kw \in W$ *for all* $k \in \mathbb{K}$, $w \in W$.

Proof. Observe first that $\oplus$ and $\square$ are well-defined if and only if (ii) and (iii) holds. So we may assume that (ii) and (iii) hold and that $\oplus$ and $\square$ are well-defined.

$\Longrightarrow$: Suppose $(W, \oplus, \square)$ is a $\mathbb{K}$-subspace of $(V, \oplus, \square)$. Then $(W, \oplus)$ is a subgroup of $(V, +)$ and the Subgroup Proposition 1.5.4 shows that $0_V \in W$.

$\Longleftarrow$: Suppose that (iii) holds. Let $w \in W$. Then $-w = (-1_K)w \in W$ and the the Subgroup Proposition shows that $(W, \oplus)$ is a subgroup of $(V, +)$. In particular, $(W, \oplus)$ is a groups. Since $(V, +)$ is abelian, also $(W, \oplus)$ is abelian, indeed:

$$u \oplus w = u + w = w + u = w \oplus v$$

for all $u, w \in W$. Similarly, all the remaining Axioms of a vector space holds for $(W, \oplus, \square)$ since they hold for $(V,, \diamond)$. We leave the details to the reader. $\square$

Proposition 3.1.16 (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*

$$+_{V/W} : \quad V/W \times V/W \to V/W, \quad (u + V, v + W) \mapsto (u + v) + W$$

and scalar multiplication

$$\diamond_{V/W} : \quad \mathbb{K} \times V/W \to V/W, \quad (k, v + W) \mapsto kv + W$$

is a well-defined vector space.

(b) *The function*

$$\pi : \quad V \to V/W, \quad v \mapsto v + W$$

is an onto and $\mathbb{K}$-linear. Moreover, $\mathrm{Ker}\phi = W$.

Proof. (a) By Theorem 1.8.11 $(V/W, +_{V/W})$ 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 1.9.4 π is an onto homomorphism of groups and $\mathrm{Ker}\pi = W$. Let $k \in \mathbb{K}$ and $v \in V$. Then

$$\pi(kv) = kv + W = k(v + W),$$

and so π is a $\mathbb{K}$-linear function. $\square$

Lemma 3.1.17. *Let $\mathbb{K}$ be field, V a $\mathbb{K}$-space, W a subspace of V. Let $(w_1, \dots, w_l)$ be a basis for W and let $(v_1, \dots, v_l)$ be a list of vectors in V. Then the following statements 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.*

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 list 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. □

Lemma 3.1.18. *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 $n \geq 1$ and $m \geq 1$. Without loss $n \leq m$. Put $W = \operatorname{Span}(w_1)$. 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 3.1.9(a), $(v_1 + W, \ldots, v_k + W)$ is a basis for V/W.

By 3.1.9(b) the basis $(v_1, \ldots, v_n)$ is a maximal linearly independent list. Hence $(w_1, v_1, \ldots, v_n)$ is linearly dependent , and so cannot be a basis for V. As w_1 is basis for W we conclude from 3.1.17 that $(v_1 + W, \ldots, v_n + W)$ is not basis for V/W. It follows that $k \neq n$ and so $k < n$. The induction assumption now implies that 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, 3.1.17 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 $n = m$. □

Definition 3.1.19. *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 3.1.18).*

Lemma 3.1.20. *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 $\mathcal{B}$ is a minimal spanning list and 3.1.9(b) shows that $\mathcal{B}$ is basis for V. □

The next lemma is the analogue of Lagrange's Theorem for vector spaces:

Theorem 3.1.21 (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 W and V/W are finite dimensional. Let $(w_1, w_2 \dots w_k)$ be basis for W and $(v_1 + W, \dots v_l + W)$ a basis for V/W.

Then by 3.1.17 $(w_1, \dots, w_l, v_1, \dots, v_l)$ 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 $(z_1, \dots, z_n)$ be a basis for V. Then $(z_1 + W, z_2 + W, \dots, z_n + W)$ is a spanning list for V/W. So by 3.1.20

$$(**) \qquad V/W \text{ is finite dimensional.}$$

It remains to show that W is finite dimensional. Let $(z_1, \dots, z_k)$ be a linear independent list in W and put $Z := \mathrm{Span}(z_1, \dots, l_k)$.. Then $(z_1, \dots, z_k)$ is a basis for Z. By (**) know that V/Z is finite dimensional, so (*) gives

$$\dim V = \dim Z + \dim V/Z \geq k$$

Thus we can choose $k \in \mathbb{N}$ maximal such that there exists a linearly independent list $(z_1, \dots, z_k)$ in W. Then $(z_1, \dots, z_k)$ is a maximal linear independent list in W and so 3.1.9 shows that $(z_1, \dots, z_k)$ is a basis for W. □

Corollary 3.1.22. *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 a sublist of basis of V. In particular, $\mathcal{L}$ has length at most $\dim_{\mathbb{K}} V$.*

Proof. Let $W = \mathrm{Span}(\mathcal{L})$. Then $\mathcal{L}$ is a basis for W. By 3.1.21 V/W is finite dimensional and so has a basis $(v_1 + W, v_2 + W, \dots, v_l + W)$ for some list $(v_1, \dots, v_l)$ in V. Let $\mathcal{L} = (w_1, \dots w_k)$. Then 3.1.17 shows that $(w_1, \dots, w_k, v_1, \dots v_l)$ is a basis for V. □

3.2 Simple Field Extensions

Definition 3.2.1. *Let $(\mathbb{K}, +, \cdot)$ be a field. A subfield of $(\mathbb{K}, +, \cdot)$ is a field $(\mathbb{F}, \oplus, \odot)$ such that*

(i) $\mathbb{F} \subseteq \mathbb{K}$,

(ii) $a \oplus b = a + b$ *for all* $a, b \in \mathbb{K}$.

(iii) $a \odot b = a \cdot b$ *for all* $a, b \in \mathbb{K}$.

If $\mathbb{F}$ *is a subfield of* $\mathbb{K}$ *we also say that* $\mathbb{K}$ *is an* extension field *of* $\mathbb{F}$ *and that* $F \leq \mathbb{K}$ *is a field extension.*

Proposition 3.2.2 (Subfield Proposition)**.** *Let* $(\mathbb{K}, +, \cdot)$ *be a field and* $\mathbb{F}$ *a subset of* $\mathbb{K}$. *Define*

$$\oplus : \quad \mathbb{F} \times \mathbb{F} \to \mathbb{F}, \quad (a, b) \mapsto a + b.$$

and

$$\odot : \quad \mathbb{F} \times \mathbb{F} \to \mathbb{F}, \quad (a, b) \mapsto a \cdot b.$$

Then $(\mathbb{F}, \oplus, \odot)$ *is a well-defined subfield of* $(\mathbb{K}, +, \cdot)$ *if and only of*

(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* $a \neq 0_{\mathbb{K}}$.

Proof. Readily verified. □

Example 3.2.3. $\mathbb{Q} \leq \mathbb{R}$ and $\mathbb{R} \leq \mathbb{C}$ are field extensions.

Lemma 3.2.4. *Let* $\mathbb{F} \leq \mathbb{K}$ *be a field extension. Then* $\mathbb{K}$ *is vector space over* $\mathbb{F}$, *where the scalar multiplication is given by*

$$\mathbb{F} \times \mathbb{K} \to \mathbb{K}, \quad (f, k) \mapsto fk$$

Proof. Using the axioms of a field it is easy to verify the axioms of a vector space. □

Definition 3.2.5. *A field extension* $\mathbb{F} \leq \mathbb{K}$ *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* $\mathbb{F} \leq \mathbb{K}$.

Example 3.2.6. $(1, i)$ is an $\mathbb{R}$-basis for $\mathbb{C}$ and so $\mathbb{R} \leq \mathbb{C}$ is a finite field extension of degree 2. We claim that $\mathbb{Q} \leq \mathbb{R}$ is not finite. Indeed, by 3.1.13 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 3.2.7. *Let* $\mathbb{F} \leq \mathbb{K}$ *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* $\mathbb{F} \leq \mathbb{K}$ *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 $\mathbb{F} \leq \mathbb{K}$ 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 $(v_1, \dots, v_n)$ spans V over $\mathbb{K}$ there exists $l_1, \dots, l_n \in \mathbb{K}$ with

$$(*) \qquad v = \sum_{j=1}^{n} l_j v_j.$$

Let $1 \le j \le n$. Since $(k_1, \dots, k_m)$ spans $\mathbb{K}$ over $\mathbb{F}$ there exists $a_{1j}, \dots a_{mj} \in \mathbb{F}$ with

$$(**) \qquad l_i = \sum_{i=1}^{m} a_{ij} k_i.$$

Substituting $(**)$ into $(*)$ 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 $1 \le i \le m$ and $i \le j \le n$ 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 $(v_1, \dots, v_n)$ is linearly independent over $\mathbb{K}$ we conclude that for all $1 \le j \le n$:

$$\sum_{i=1}^{m} a_{ij} k_i = 0_{\mathbb{K}}.$$

Since $(k_1, k_2, \dots, k_m)$ is linearly independent over $\mathbb{F}$ this implies $a_{ij} = 0_{\mathbb{F}}$ for all $1 \le i \le m$ and all $1 \le j \le m$. 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 3.2.8. *Let $\mathbb{F} \le \mathbb{K}$ and $\mathbb{K} \le \mathbb{E}$ be finite field extensions. Then also $\mathbb{F} \le \mathbb{E}$ is a finite field extension and*

$$\dim_{\mathbb{F}} \mathbb{E} = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{K}} \mathbb{E}.$$

Proof. By 3.2.4 $\mathbb{E}$ is a $\mathbb{K}$-space. So the corollary follows from 3.2.7 applied with $V = \mathbb{E}$. □

Before proceeding we recall a few definition and facts from ring theory.

Definition 3.2.9. *Let R be a ring.*

(a) *Let I be 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 $i \in I$.*

(b) *Let $a \in R$. Then $(\!(a)\!) := \bigcap\{I \subseteq R \mid I \text{ is an ideal in } R, a \in I\}$.*

(c) *Let $a \in R$. Then $Ra := \{ra \mid r \in R\}$*

Lemma 3.2.10. *Let R is a commutative ring with identity and $a \in R$. Then $Ra = (\!(a)\!)$. In particular, Ra is the smallest ideal of R containing a, that is*

(a) *Ra is an ideal of R.*

(b) *$a \in Ra$.*

(c) *If I is an ideal of R with $a \in R$, then $Ra \subseteq I$.*

Proof. See [Hung, Theorem 6.2]. □

Lemma 3.2.11. *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 $I = (\!(p)\!) = \mathbb{F}[x]p$.*

(b) *$\mathbb{F}[x]/I$ is an integral domain if and only if p is irreducible and if and only if $\mathbb{F}[x]/I$ is field.*

Proof. (a) We will first show the existence of p. Since $I \neq \{0_\mathbb{F}\}$ we can choose $s \in I$ of minimal degree with respect to $s \neq 0_\mathbb{F}$. Put $p := \mathrm{lead}(s)^{-1} \cdot s$. Then s is monic, $\deg p = \deg q$ and, since I is an ideal, $p \in I$.

Let $f \in I$. . By the Division Algorithm [Hung, Theorem 4.4], $f = qp + r$ where $q, r \in \mathbb{F}[x]$ with $\deg r < \deg p$. Since I is an ideal and $f, p \in I$ we get $r = f - qp \in I$. Since $\deg r < \deg p = \deg q$, the minimal choice of $\deg q$ shows that $r = 0_F$. Thus $f = qp \in (\!(p)\!)$. Hence $I \subseteq (\!(p)\!)$. As $p \in I$ and I is an ideal, $(\!(p)\!) \subseteq I$. Thus $I = (\!(p)\!)$.

Suppose that also $\tilde{p} \in \mathbb{F}[x]$ is monic with $I = \mathbb{F}[x]\tilde{p}$. Then $\tilde{p} \in \mathbb{F}[x]p$ 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 3.2.12. *Let R be a commutative ring with identity, S a subring of R with $1_R \in S$ and a in R.*

(a) *Then $S[a] := \{f(a) \mid f \in S[x]\} \subseteq R$.*

(b) *a is called* algebraic *over S, if there exists a non-zero $f \in S[x]$ with $f(a) = 0_S$. Otherwise a is called transcendental over S.*

Example 3.2.13. Consider the field extension $\mathbb{Q} \leq \mathbb{C}$.

(1) $\sqrt{2}$ is the a root of $x^2 - 2$ and so $\sqrt{2}$ is algebraic over $\mathbb{Q}$.

(2) i is a root of $x^2 + 1$ so i is algebraic over $\mathbb{Q}$.

(3) 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 3.2.14. *Let R be a commutative ring with identity, S a subring of R with $1_R \in S$ and a in R*

(a) *The function $\phi_a : S[x] \to R, f \mapsto f(a)$ is a ring homomorphism.*

(b) $\operatorname{Im}\phi_a = S[a]$ *is a subring of R with $S \subseteq R$ and $a \in S[a]$.*

(c) *ϕ_a is 1-1 if and only if* $\operatorname{Ker}\phi_a = \{0_S\}$ *and if and only if a is transcendental over S.*

Proof. (a) Let $f, g \in S[x]$. Then

$$\phi_a(f+g) = (f+g)(a) = f(a) + g(a) = \phi_a(f) + \phi_a(g)$$

and similarly $\phi_a(fg) = \phi_a(f)\phi_a(g)$. We remark that the assertion $(f+g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$ really needs a justification, but leave the the details to the reader.

(b) $\operatorname{Im}\phi_a = \{\phi_a(f) \mid f \in S[x]\} = \{f(a) \mid f \in S[x]\} = S[a]$. By Corollary 3.13 in Hungerford [Hung] the image of a homomorphism is a subring and so $S[a]$ is a subring of S.

Let $s \in S$ and put $f = s$. Then $f \in S[x]$ and $s = f(a) \in S[a]$.

Let $g = 1_R x$. Then $g \in S[x]$ and $a = g(a) \in S[a]$.

(c) By 1.9.3 ϕ_a is 1-1 if and only if $\operatorname{Ker}\phi_a = \{0_{\mathbb{F}}\}$. Now

$$\operatorname{Ker}\phi_a = \{f \in S[x] \mid \phi_a(f) = 0_R\} = \{f \in \mathbb{F}[x] \mid f(a) = 0_R\},$$

and so $\operatorname{Ker}\phi_a = \{0_S\}$ if and only if there does not exist a non-zero polynomial $f \in S[x]$ with $f(a) = 0_R$, that is if and only if a is transcendental. □

Theorem 3.2.15. *Let $\mathbb{F} \leq \mathbb{K}$ 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* $\operatorname{Ker}\phi_a = (\!(p_a)\!)$.

(b) $\overline{\phi}_a : \quad \mathbb{F}[x]/(\!(p_a)\!) \to \mathbb{F}[a], \quad f + (\!(p_a)\!) \mapsto f(a)$ *is a well-defined isomorphism of rings.*

(c) *p_a is irreducible.*

(d) *$\mathbb{F}[a]$ is a subfield of $\mathbb{K}$.*

(e) *Put $n := \deg p_a$. Then $(1, a, \ldots, a^{n-1})$ is an $\mathbb{F}$-basis for $\mathbb{F}[a]$*

(f) *$\mathbb{F} \leq \mathbb{F}[a]$ is finite and $\dim_{\mathbb{F}} \mathbb{F}[a] = \deg p_a$.*

(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 3.2.14(c), $\mathrm{Ker}\phi_a \neq \{0_{\mathbb{F}}\}$. By 3.2.14(a) is a ring homomorphism and so by Theorem 6.10 in Hungerford [Hung], $\mathrm{Ker}\phi_a$ is an ideal in $\mathbb{F}[x]$. Thus by 3.2.11, $\mathrm{Ker}\phi_a = (\!(p_a)\!)$ for a unique monic polynomial $p_a \in \mathbb{F}[x]$.

(b): By definition of p_a, $\mathrm{Ker}\phi_a = (\!(p_a)\!)$. By 3.2.14(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): As $\mathbb{K}$ is a field we know that $\mathbb{K}$ is an integral domain. Since $\mathbb{F}[a]$ is a subring of $\mathbb{K}$ this shows that $\mathbb{F}[a]$ is an integral domain. By (b) $\mathbb{F}[a] \cong \mathbb{F}[x]/(\!(p_a)\!)$ and so also $\mathbb{F}[x]/(\!(p_a)\!)$ is an integral domain. Hence by 3.2.11(b), p_a is irreducible and $\mathbb{F}[x]/(\!(p_a)\!)$ is a field. Since $\mathbb{F}[a] \cong \mathbb{F}[x]/(\!(p_a)\!)$ also $\mathbb{F}[a]$ is a field. Thus (c) and (d) are proved.

(e) Let $T \in \mathbb{F}[x]/(\!(p_a)\!)$. Then $T = f + (\!(p_a)\!)$ for some $f \in \mathbb{F}[x]$. Let $r \in \mathbb{F}[x]$. By 1.7.6 $f + (\!(p_a)\!) = r + (\!(p_a)\!)$ if and only $f = r + g$ for some $g \in (\!(p_a)\!)$ and so if and only if $f = r + qp_a$ for some $q \in \mathbb{F}[x]$. By the Division Algorithm there exist unique $q, r \in \mathbb{F}[x]$ with

$$f = qp_a + r, \quad \text{and} \quad \deg r < \deg p_a$$

and we conclude that there exists a unique $r \in \mathbb{F}[x]$ with

$$T = r + (\!(p_a)\!) \quad \text{and} \quad \deg r < n.$$

Any $r \in \mathbb{F}[x]$ with $\deg r < n$ can be uniquely written as $r = \sum_{i=0}^{n} b_i x^i$, where $b_i \in \mathbb{F}$. Hence there exist unique $b_0, \ldots, b_{n-1} \in \mathbb{F}$ with

$$T = \sum_{i=0}^{n-1} b_i x^i \; + \; (\!(p_a)\!),$$

that is with

$$T = \sum_{i=0}^{n-1} b_i \left(x^i + (\!(p_a)\!) \right).$$

Thus by 3.1.7

$$\left(\, 1 + (\!(p_a)\!), \; x + (\!(p_a)\!), \; \ldots, \; x^{n-1} + (\!(p_a)\!) \, \right)$$

is a $\mathbb{F}$-basis for $\mathbb{F}[x]/(\!(p_a)\!)$. Since $\overline{\phi}_a$ is an isomorphism and $\overline{\phi}_a\big(x^i + (\!(p_a)\!)\big) = a^i$ we conclude from 3.1.12(e) that

$$(\, 1, \; a, \; a^2, \; \ldots, \; a^{n-1})$$

is a basis for $\mathbb{F}[a]$.

(f) Follows from (e).

(g) Note that $g(a) = 0_{\mathbb{K}}$ if and only if $\phi_a(g) = 0_{\mathbb{K}}$, if and only if $g \in \mathrm{Ker}\phi_a$, if and only if $g \in (\!(p_a)\!)$, if and only if $g = qp_a$ for some $q \in \mathbb{F}[x]$, and if and only if $p_a \mid g$ in $\mathbb{F}[x]$. □

Definition 3.2.16. *Let* $\mathbb{F} \leq \mathbb{K}$ *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* $\mathrm{Ker}\phi_a = (\!(p_a)\!)$ *is called the* minimal polynomial *of* a *over* $\mathbb{F}$.

Lemma 3.2.17. *Let $\mathbb{F} \le \mathbb{K}$ be a field extension and $a \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then p_a is the unique monic irreducible polynomial in $\mathbb{F}[x]$ with $p_a(a) = 0_F$.*

Proof. Note that $p_a \,|\, p_a$ in $\mathbb{F}[x]$ and so 3.2.15(g) shows that $p_a(a) = 0_F$. By definition p_a is monic and by 3.2.15(c), p_a is irreducible.

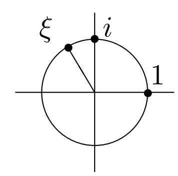
Suppose now that p is a monic, irreducible polynomial in $\mathbb{F}[x]$ with $p(a) = 0$. Then 3.2.15(g) shows that $p_a \mid p$. Since p is irreducible, the only monic polynomials dividing p are $1_{\mathbb{F}}$ and p. As p has a root, (namely a), $p_a \neq 1_{\mathbb{F}}$. Thus $p = p_a$. □

Example 3.2.18. (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 3.2.17 implies that $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. Hence by 3.2.15(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 3.2.19. (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 functions 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*

$$R[x] \to S[x], \quad \sum_{i=1}^{n} f_i x^i \mapsto \sum_{i=1}^{n} \sigma(i) x^i$$

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. □

Corollary 3.2.20. *Let $\sigma : \mathbb{K}_1 \to \mathbb{K}_2$ be a field isomorphism. For $i = 1, 2$ let $\mathbb{K}_i \le \mathbb{E}_i$ be a field extension and suppose $a_i \in \mathbb{E}_i$ 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

$$\rho(a_1) = a_2 \text{ and } \rho|_{\mathbb{K}_1} = \sigma$$

Proof. By 3.2.19(c)

$$\sigma : \mathbb{K}_1[x] \to \mathbb{K}_2[x], \quad f \mapsto \sigma(f)$$

is a ring isomorphism. By 3.2.19(b:a)

$$\sigma\big((\!(p_1)\!)\big) = (\!(\sigma(p_1))\!) = (\!(p_2)\!)$$

and so by 3.2.19(b:c)

$$(*) \qquad \mathbb{K}_1[x]/(\!(p_1)\!) \to \mathbb{K}_2[x]/(\!(p_2)\!), \quad f + (\!(p_1)\!) \mapsto \sigma(f) + (\!(p_2)\!)$$

is an isomorphism

By 3.2.15(b)

$$(**) \qquad \begin{aligned} \mathbb{K}_1[x]/(\!(p_1)\!) \to \mathbb{K}_1[a_1], \quad f + (\!(p_1)\!) \mapsto f(a_1) \\ \mathbb{K}_2[x]/(\!(p_2)\!) \to \mathbb{K}_2[a_2], \quad f + (\!(p_2)\!) \mapsto f(a_2) \end{aligned}$$

both are isomorphism. Hence we obtain an isomorphism

$$\begin{array}{ccccccccc} \rho : & \mathbb{K}_1[x] & \to & \mathbb{K}_1[x]/(\!(p_1)\!) & \to & \mathbb{K}_2[x]/(\!(p_2)\!) & \to & \mathbb{K}_2[x] \\ & f(a_1) & \mapsto & f + (\!(p_1)\!) & \mapsto & \sigma(f) + (\!(p_2)\!) & \mapsto & \sigma(f)(a_2) \end{array}$$

Let $k \in \mathbb{F}_1$. To compute $\rho(k)$, choose $f = k \in \mathbb{K}_1[x]$. Then

$$f(a_1) = k, \quad \sigma(f) = \sigma(k) \in K_2, \quad \sigma(f)(a_2) = \sigma(k)$$

Thus
$$\rho(k) = \sigma(k).$$

To compute $\rho(a_1)$, choose $f = x \in \mathbb{K}_1[x]$. Then
$$f(a_1) = a_1, \quad \sigma(f) = \sigma(x) = x, \quad \sigma(f)(a_2) = a_2.$$
So
$$\rho(a_1) = a_2.$$

□

3.3 Splitting Fields

Definition 3.3.1. *A field extension $\mathbb{F} \le \mathbb{K}$ is called* algebraic *if each $k \in \mathbb{K}$ is algebraic over $\mathbb{F}$.*

Lemma 3.3.2. *Any finite field extension is algebraic.*

Proof. Let $\mathbb{F} \le \mathbb{K}$ be a finite field extension. Put $n := \dim_{\mathbb{F}} \mathbb{K}$ and let $a \in \mathbb{K}$. By 3.1.20 any $\mathbb{F}$-linearly independent list in $\mathbb{K}$ has lengthy at most n. Thus $(1_{\mathbb{F}}, a, \dots, a^n)$ is $\mathbb{F}$-linearly dependent and so there exist $f_0, \dots, f_n \in \mathbb{F}$, not all 0_F, with $\sum_{i=1}^n f_i a^i = 0_{\mathbb{F}}$. Put $f = \sum_{i=1}^n f_i x^i \in \mathbb{F}[x]$. Then $f \neq 0_F$ and $f(a) = 0_F$. Thus a is algebraic over $\mathbb{F}$. □

Example 3.3.3. $\mathbb{R} \le \mathbb{C}$ is algebraic but $\mathbb{Q} \le \mathbb{R}$ is not.

Definition 3.3.4. *Let R be a commutative ring with identity, S a subring of R with $1_R \in S$, $n \in \mathbb{N}$ and $a_1, a_2 \dots, a_n \in \mathbb{K}$. For $n = 0$ define $S[] = S$, and for $n \ge 1$, inductively define*
$$S[a_1, a_2, \dots, a_k] := S[a_1, a_2, \dots, a_{k-1}][a_k] \subseteq R$$

Definition 3.3.5. *Let $\mathbb{F} \le \mathbb{K}$ be field extensions and $f \in \mathbb{F}[x]$. We say that f* splits *in $\mathbb{K}$ if there exist $a_1 \dots a_n \in \mathbb{K}$ with*

(i) $f = \mathrm{lead}(f)(x - a_1)(x - a_2)\dots(x - a_n)$.

We say that $\mathbb{K}$ is a splitting field *for f over $\mathbb{F}$ if f splits in $\mathbb{K}$ and*

(ii) $\mathbb{K} = \mathbb{F}[a_1, a_2, \dots, a_n]$.

Example 3.3.6. Consider the extension $\mathbb{R} \le \mathbb{C}$.

(1) $x^2 + 1 = (x - i)(x - (-i))$ and $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[i, -i]$. So $\mathbb{C}$ is splitting field of $x^2 + 1$ over $\mathbb{C}$.

(2) $x^2 = (x - 0)(x - 0)$, but $\mathbb{C} \neq \mathbb{R} = \mathbb{R}[0]$. So x^2 splits over $\mathbb{C}$, but $\mathbb{C}$ is not a splitting field of $\mathbb{C}$ over $\mathbb{R}$.

Proposition 3.3.7. *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, $\mathbb{F} \le \mathbb{K}$ is finite of degree at most $n!$.*

Proof. The proof is by induction on $\deg f$. If $\deg f \le 0$, 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 3.2.11 $\mathbb{E}$ 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 $b := x + (\!(p)\!) \in \mathbb{F}$ and $n = \deg f$. Then $\mathbb{E} = \mathbb{F}[b]$. Since $p \mid f$ we have $f \in (\!(p)\!)$ and so $f + (\!(p)\!) = (\!(p)\!) = 0_{\mathbb{E}}$. Hence

$$f(b) = \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} f_i\big(x + (\!(p)\!)\big)^i = \sum_{i=0}^{n} f_i x^i + (\!(p)\!) = f + (\!(p)\!) = (\!(p)\!) = 0_{\mathbb{E}},$$

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 $g \in \mathbb{E}[x]$. As $deg f = k+1$ we have $\deg g = k$. So by the induction assumption there exists a splitting field $\mathbb{K}$ for g over $\mathbb{E}$ with $\dim_{\mathbb{E}} \mathbb{K} \le k!$. By 3.2.11

$$\dim_{\mathbb{F}} \mathbb{E} = \deg p \le \deg f = k+1$$

and so by 3.2.8

$$\dim_{\mathbb{F}} \mathbb{K} = \dim_{\mathbb{F}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{K} \le (k+1)\cdot k! = (k+1)!$$

Moreover, there exist $a_1, \dots, a_k \in \mathbb{K}$ with

(i) $g = \mathrm{lead}(g)(x-a_1)(x-a_2)\dots(x-a_k)$;

(ii) $\mathbb{K} = \mathbb{E}[a_1, a_2, \dots, a_k]$; and

Note that $\mathrm{lead} f = \mathrm{lead} g$, $f = (x-b)\cdot g$ and $\mathbb{E} = \mathbb{K}[b]$. Hence

(iv) $g = \mathrm{lead}(f)(x-b)(x-a_1)(x-a_2)\dots(x-a_k)$, and

(v) $\mathbb{K} = \mathbb{F}[b][a_1, a_2, \dots, a_b] = \mathbb{F}[b, a_1, \dots, a_n]$.

Thus $\mathbb{K}$ is a splitting field for f over $\mathbb{F}$.

So the theorem also holds for polynomials of degree $k+1$ and, by the Principal of Mathematical Induction, for all polynomials. □

Lemma 3.3.8. *Let $\mathbb{F}$ be a field, $f \in \mathbb{F}[x]$ and $\mathbb{K}$ a splitting field for f over $\mathbb{F}$. Suppose a is a root of f in $\mathbb{K}$ and put $\mathbb{E} := \mathbb{F}[a]$. Then there exists a unique $g \in \mathbb{E}[x]$ with $f = (x-a)\cdot g$ and, $\mathbb{K}$ is a splitting field for g over $\mathbb{E}$.*

Proof. Note that a is a root of f in $\mathbb{E}$ and so the factor theorem shows that $f = (x-a)g$ for some $g \in \mathbb{E}$. Since $\mathbb{E}[x]$ is an integral domain, g is unique. Since $\mathbb{K}$ is a splitting field for f there exists $b, a_1, \dots, a_n \in \mathbb{K}$ with

$$f_1 = b\cdot(x-a_1)(x-a_2)\dots(x-a_n)$$

Since a is a root of f we may assume that $a = a_1$. Since

$$(x-a_1)g = (x-a)g = f = (x-a_1)\cdot b\cdot(x-a_2)\dots(x-a_n)$$

we get

$$g = b \cdot (x - a_2) \dots (x - a_n)$$

Note that

$$\mathbb{K} = \mathbb{F}[a_1, \dots, a_n] = \mathbb{F}[a][a_2, \dots, a_n] = \mathbb{E}[a_2, \dots a_n]$$

and so $\mathbb{K}$ is a splitting field for g over $\mathbb{E}$. □

Theorem 3.3.9. *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

$$\breve{\sigma} : \mathbb{K}_1 \to \mathbb{K}_2 \textit{ with } \breve{\sigma} \mid_{\mathbb{F}_1} = \sigma.$$

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*

$$\sigma(a_1) = a_2.$$

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 $\sigma = \breve{\sigma}$.

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 divisor of f_1 in $\mathbb{F}_1[x]$. Put $p_2 := \sigma(p_1)$. By 3.2.19(c), $\sigma : \mathbb{K}_1[x] \to \mathbb{K}_2[x]$ is a ring isomorphism. Thus p_2 is a irreducible divisor of 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 3.2.20 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 $f_1 = (x - a_1) \cdot g_1$ for some $g_1 \in \mathbb{E}_1[x]$. Put $g_2 := \rho(g_1) \in \mathbb{E}_2[x]$. Since $\rho(a_1) = a_2$ we get

$$f_2 = \rho(f_1) = \rho((x - a_1) \cdot g_1) = \rho(x - a_1)\rho(f_1) = (x - a_2) \cdot g_2.$$

For 3.3.8 we conclude that $\mathbb{E}_i$ is a splitting field for g_i over $\mathbb{E}_i$. So by the induction assumption there exists a field isomorphism $\breve{\sigma} : \mathbb{K}_1 \to \mathbb{K}_2$ with $\breve{\sigma} \mid_{\mathbb{E}_i} = \rho$. We have $\breve{\sigma}(a_1) = \rho(a_1) = a_2$ and $\breve{\sigma} \mid_{\mathbb{F}_1} = \rho \mid_{\mathbb{F}_1} = \sigma$.

Thus the theorem holds for polynomials of degree $k+1$ and so by induction for all polynomials. □

Corollary 3.3.10. *Let $\mathbb{F}$ be a field, $f \in \mathbb{F}[x]$ and let $\mathbb{K}, \mathbb{K}_1, \mathbb{K}_2$ be splitting fields of f over $\mathbb{F}$.*

(a) *There exists a field isomorphism $\rho : \mathbb{K}_1 \to \mathbb{K}_2$ with $\rho\,|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$. .*

(b) *Let p be an irreducible divisor of f in $\mathbb{F}[x]$ and let $a_1$and a_2 be roots of p in $\mathbb{K}$. Then there exists a field isomorphisms $\rho : \mathbb{K} \to \mathbb{K}$ with $\rho\,|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ and $\sigma(a_1) = a_2$.*

Proof. (a): Apply 3.3.9 with

$$\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}, \quad \sigma = \mathrm{id}_{\mathbb{F}}, \quad f_1 = f_2 = f$$

(b): Apply 3.3.9 with

$$\mathbb{F}_1 = \mathbb{F}_2 = \mathbb{F}, \quad \mathbb{K}_1 = \mathbb{K}_2 = \mathbb{K}, \sigma = \mathrm{id}_{\mathbb{F}}, \quad f_1 = f_2 = f, \quad p_1 = p_2 = p$$

□

Example 3.3.11. By Example 3.3.6(1) $\mathbb{C}$ is splitting field of $x^2 + 1$ over $\mathbb{R}$. Moreover $x^2 + 1$ is irreducible over $\mathbb{R}$ and i and $-i$ are roots of $x^2 + 1$. Hence 3.3.10(b) shows that there exists a field isomorphism $\rho : \mathbb{C} \to \mathbb{C}$ with

$$\rho\,|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}} \quad \text{and} \quad \rho(i) = -i.$$

Let $a, b \in \mathbb{R}$. Then

$$\rho(a + bi) = \rho(a) + \rho(b)\rho(-i) = a + b(-i) = a - bi$$

This shows ρ is complex conjugation. In particular, complex conjugation is an isomorphism of fields.

3.4 Separable Extension

Definition 3.4.1. *Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$.*

(a) *Let $\mathbb{K}$ be a splitting field for f over $\mathbb{K}$ and $a_1, \ldots, a_n \in \mathbb{K}$ with*

$$f = \mathrm{lead}(f)(x - a_1)\ldots(x - a_n)$$

We say that f has a double root if $a_i = a_j$ for some $1 \le i < j \le n$.

(b) *If f is irreducible in $\mathbb{F}[x]$, then f is called* separable *over $\mathbb{F}$ provided that f does not have a double root. In general, f is called separable over $\mathbb{F}$ provided that all irreducible divisors of f in $\mathbb{F}[x]$ are separable over $\mathbb{F}$.*

(c) *Let $\mathbb{F} \le \mathbb{K}$ be a field extension. Then $a \in \mathbb{K}$ 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 $\mathbb{F}$.*

(d) *A field extension $\mathbb{F} \le \mathbb{K}$ is called separable if each $a \in \mathbb{K}$ is separable over $\mathbb{F}$.*

Example 3.4.2. Let $\mathbb{Z}_2 \leq \mathbb{E}$ 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 3.2.17 $x^2 - t^2$ 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 $\mathbb{F} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{K}$ be 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 $\mathbb{F} \leq \mathbb{K}$ is separable, then also $\mathbb{F} \leq \mathbb{E}$ and $\mathbb{E} \leq \mathbb{K}$ are separable.*

Proof. (a) Since $p_a^{\mathbb{F}}(a) = 0_{\mathbb{F}}$ and $p_a^{\mathbb{E}} \in \mathbb{F}[x] \subseteq \mathbb{E}[x]$ we see that a is algebraic over $\mathbb{E}$. Moreover, as a is a root of $p_a^{\mathbb{F}}$. we know that $p_a^{\mathbb{F}}$ divides $p_a^{\mathbb{E}}$ by 3.2.15(g).

(b) Let $f \in \mathbb{F}[x]$ be separable over $\mathbb{F}$. Then $f = p_1 p_2 \dots p_k$ for some irreducible $p_i \in \mathbb{F}[x]$. Moreover, $p_i = q_{i1} q_{i2} \dots q_{il_i}$ 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 $\mathbb{F} \leq \mathbb{K}$ is separable, a is separable over $\mathbb{F}$. So by (c), a is separable over $\mathbb{E}$. Thus $\mathbb{E} \leq \mathbb{K}$ is separable. Let $a \in \mathbb{E}$. Then $a \in \mathbb{K}$ and so a is separable over $\mathbb{F}$. Hence $\mathbb{F} \leq \mathbb{E}$ is separable. □

3.5 Galois Theory

Definition 3.5.1. *Let $\mathbb{F} \leq \mathbb{K}$ be field extension.* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ *is the set of all field isomorphism $\alpha : \mathbb{K} \to \mathbb{K}$ with $\alpha|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$.*

Lemma 3.5.2. *Let $\mathbb{F} \le \mathbb{K}$ 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 3.2.19(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 3.2.19(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 1.5.4, $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ 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 3.3.11, 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 $\mathbb{F} \le \mathbb{K}$ 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 $\mathbb{F} \le \mathbb{K}$ 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 $a^{-1} \in \mathrm{Fix}_{\mathbb{K}}(H)$.

Thus $\mathrm{Fix}_{\mathbb{K}}(H)$ is a subfield of $\mathbb{K}$ by the Subfield Proposition. □

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

$$\mathrm{Fix}_{\mathbb{C}}(\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})) = \mathbb{R}.$$

Lemma 3.5.7. *Let $\mathbb{F} \leq \mathbb{K}$ be a field extension and $a \in \mathbb{K}$.*

(a) *Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ and $f \in \mathbb{F}[x]$. Then $\sigma\big(f(a)\big) = f\big(\sigma(a)\big)$.*

(b) *$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ acts on $\mathbb{K}$ via $\sigma \diamond k = \sigma(k)$.*

(c) *Define $\mathbb{F}(a) := \{de^{-1} \mid, d, e \in \mathbb{F}[a], e \neq 0_{\mathbb{F}}|\}$. Then $\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a) = \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$*

Proof. (a) Let $f = \sum_{i=0}^{n} f_i x^i$ with $f_i \in \mathbb{F}$. Then $\sigma(f_i) = f_i$, so

$$\sigma\big(f(a)\big) = \sigma\left(\sum_{i=0}^{n} f_i a^i\right) = \sum_{i=0}^{n} \sigma(f_i)\sigma(a)^i = \sum_{i=0}^{n} f_i \sigma(a)^i = f\big(\sigma(a)\big).$$

(b) Just recall from 3.5.2 that $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \subseteq \mathrm{Sym}(\mathbb{K})$ and from Example 2.1.2(2) that $\mathrm{Sym}(\mathbb{K})$ acts in $\mathbb{K}$ via $\sigma \diamond k = \sigma(k)$.

(c) Put

$$H := \mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a) = \{\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \mid \sigma(a) = a\}.$$

Since $\mathbb{F} \subseteq \mathbb{F}(a)$ and $a \in \mathbb{F}(a)$ we have

$$\mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K}) \subseteq H.$$

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 10#8, $\mathbb{F}(a) \subseteq \mathrm{Fix}_{\mathbb{K}}(H)$. Thus $H \subseteq \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$, so $H = \mathrm{Aut}_{\mathbb{F}(a)}(\mathbb{K})$. □

Proposition 3.5.8. *Let $\mathbb{F} \leq \mathbb{K}$ be a field extension and $0_{\mathbb{F}} \neq f \in \mathbb{F}[x]$. Let R be the set of roots of f in $\mathbb{K}$, let $a \in R$ and let*

$$S := \{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(K)\}.$$

(a) *$S \subseteq R$. In particular, R is $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ invariant and $\mathrm{Aut}_{\mathbb{F}}(K)$ acts in $\mathbb{R}$.*

(b) *$\mathbb{F}[a] = \mathbb{F}(a)$,*

(c)

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a])}(\mathbb{K})| = |S|$$

Proof. (a) Let $b \in S$. Then $b = \sigma(a)$ for some $\sigma \in \mathrm{Aut}_{\mathbb{F}}(K)$. Thus

$$f(b) = f\big(\sigma(a)\big) \overset{3.5.7(a)}{=} \sigma\big(f(a)\big) = \sigma(0_{\mathbb{K}}) = 0_{\mathbb{K}}.$$

So $b \in R$ and $S \subseteq R$.

(b) Since a is a root of f, we know that a is algebraic over $\mathbb{F}$. Hence by 3.2.15(c) $\mathbb{F}[a]$ is a subfield of $\mathbb{K}$, so $\mathbb{F}[a] = \mathbb{F}(a)$.

(c)

$$\begin{aligned}
|S| &= |\{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})\}| && \text{– definition of } S\\
&= |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Stab}_{\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})}(a)| && \text{– 2.1.16}\\
&= |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a])}(\mathbb{K})| && \text{– 3.5.7(c)}\\
&= |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a])}(\mathbb{K})| && \text{– (b)}
\end{aligned}$$

□

Definition 3.5.9. *Let $\mathbb{F} \le \mathbb{K}$ be field extension.*

(a) *$\mathbb{F} \le \mathbb{K}$ is called Galois if there exists a separable polynomial $f \in \mathbb{F}[x]$ such that $\mathbb{K}$ is a splitting field of f over $\mathbb{F}$.*

(b) *An* intermediate *field of $\mathbb{F} \le \mathbb{K}$ is a subfield $\mathbb{E}$ of $\mathbb{K}$ with $\mathbb{F} \subseteq \mathbb{E}$.*

Lemma 3.5.10. *Let $F \le \mathbb{E}$ and $\mathbb{E} \le \mathbb{K}$ be field extension. If $\mathbb{F} \le \mathbb{K}$ is Galois, then also $\mathbb{E} \le \mathbb{K}$ is Galois.*

Proof. Suppose $\mathbb{F} \le \mathbb{K}$ is Galois. Then $\mathbb{K}$ is the splitting field of a separable polynomial $f \in \mathbb{F}[x]$ over $\mathbb{F}$. Hence there exists $a_1, \dots, a_n \in \mathbb{K}$ with

$$f = \mathrm{lead}(f)(x - a_1)\dots(x - a_n), \quad \text{and} \quad \mathbb{K} = \mathbb{F}[a_1, \dots, a_n]$$

Then

$$\mathbb{K} = \mathbb{F}[a_1, \dots, a_n] \subseteq \mathbb{E}[a_1, \dots a_n] \subseteq \mathbb{K}$$

and so $\mathbb{K} = \mathbb{E}[a_1, \dots, a_n]$. Thus $\mathbb{K}$ is a splitting field of f over $\mathbb{E}$. By 3.4.3(b), f is separable over $\mathbb{E}$ and so $\mathbb{E} \le \mathbb{K}$ is Galois. □

Theorem 3.5.11. *Let $\mathbb{F} \le \mathbb{K}$ be a Galois extension. Then*

$$|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{K}.$$

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 $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \{\mathrm{id}_{\mathbb{F}}\}$. So the theorem holds in this case.

Suppose now $\dim_{\mathbb{F}} \mathbb{K} > 1$ and 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 such that $\mathbb{K}$ is the splitting field of f over $\mathbb{F}$. Since $\dim_{\mathbb{K}} \mathbb{K} > 1$ we have $\mathbb{K} \neq \mathbb{F}$. Also $\mathbb{K} = \mathbb{F}[a_1, \dots, a_m]$ where $a_1, \dots, a_m$ are the roots of f in $\mathbb{K}$. So there exists a root a of f in $\mathbb{K}$ with $a \notin \mathbb{F}$. Let p_a be the minimal polynomial of a over $\mathbb{F}$. Since a is a root of f we conclude from 3.2.15 that $p_a | f$ in $\mathbb{F}[x]$, and that p_a is irreducible. Since f is separable this implies that p_a has no double roots. Since f splits over $\mathbb{K}$, also p_a splits over $\mathbb{K}$. Let R be the set of roots of p_a in $\mathbb{K}$. It follows that

$$(*) \qquad |R| = \deg p_a.$$

Put

$$S := \{\sigma(a) \mid \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})\}.$$

We will show that $S = R$.

Let $b \in R$. Then both a and b are roots of p_a. Also p_a is an irreducible divisor of f. Thus by 3.3.10(b) there exists a field isomorphism $\rho : \mathbb{K} \to \mathbb{K}$ with

$$\rho\,|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}} \qquad \text{and} \quad \rho(a) = b.$$

Then $\rho \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ and so $b = \rho(a) \in S$. Hence $R \subseteq S$. By 3.5.8(a) we have $S \subseteq R$, so

$$(**) \qquad R = S.$$

We compute

$$\begin{aligned} |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| &= |S| && - 3.5.8(c) \\ &= |R| && - (**) \\ &= \deg p_a && - (*) \\ &= \dim_{\mathbb{F}} \mathbb{F}[a] && - 3.2.15(e) \end{aligned}$$

Thus

$$(***) \qquad |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = \dim_{\mathbb{F}} \mathbb{F}[a].$$

By 3.5.10 $\mathbb{F}[a] \leq \mathbb{K}$ is Galois. By 3.2.8 we have

$$(+) \qquad \dim_{\mathbb{F}} \mathbb{K} = \dim_{\mathbb{F}} \mathbb{F}[a] \cdot \dim_{\mathbb{F}[a]} \mathbb{K}$$

Since $a \notin \mathbb{F}$ we have $\dim_{\mathbb{F}} \mathbb{F}[a] \geq 2$ and so (+) implies $\dim_{\mathbb{F}[a]} \mathbb{K} < \dim_{\mathbb{F}} \mathbb{K}$. Hence induction assumption shows that

$$(++) \qquad |\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| = \dim_{\mathbb{F}[a]} \mathbb{K}.$$

Hence

$$\begin{aligned}
|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| &= |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| \cdot |\mathrm{Aut}_{\mathbb{F}[a]}(\mathbb{K})| && -\text{Lagrange's} \\
&= \dim_{\mathbb{F}} \mathbb{F}[a] \cdot \dim_{\mathbb{F}[a]} \mathbb{K} && -(*\,*\,*) \text{ and } (++) \\
&= \dim_{\mathbb{F}} \mathbb{K} && -(+)
\end{aligned}$$

□

Example 3.5.12. By Example 3.2.18 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 $\xi := e^{\frac{2\pi}{3}i} \in \mathbb{C}$, $\xi^3 = 1$ and $\xi \neq 1$. Note that $x^3-1 = (x-1)(x^2+x+1)$. So 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 has not root in $\mathbb{Q}[\sqrt[3]{2}]$. It follows that x^2+x+1 is irreducible over $\mathbb{Q}[\sqrt[3]{2}]$ and so 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 $\dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]} \mathbb{K} = \deg(x^2+x+1) = 2$ and so

$$\dim_{\mathbb{Q}} \mathbb{K} = \dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt[3]{2}\right] \cdot \dim_{\mathbb{Q}\left[\sqrt[3]{2}\right]} \mathbb{K} = 3 \cdot 2 = 6.$$

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 $R := \left\{\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\right\}$ be the set of roots of x^3-2. By 3.5.8, R is $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$-invariant and so by 2.2.11(b), $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ acts on R. The homomorphism associated to this action is

$$\Phi: \quad \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \to \mathrm{Sym}(R), \quad \sigma \mapsto \sigma\,|_R\,.$$

By Homework 12, Φ is 1-1. By 3.5.11 $|\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| = \dim_{\mathbb{Q}} \mathbb{K} = 6$. Since also $|\mathrm{Sym}(R)| = 6$ we conclude that Φ is a bijection, so

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \cong \mathrm{Sym}(R) \cong \mathrm{Sym}(3).$$

Lemma 3.5.13. *Let $\mathbb{F} \leq \mathbb{K}$ be a field extension and G a finite subgroup of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ with $\mathrm{Fix}_{\mathbb{K}}(G) = \mathbb{F}$. Then $\mathbb{F} \leq \mathbb{K}$ is finite and $\dim_{\mathbb{F}} \mathbb{K} \leq |G|$.*

Proof. Put $m := |G|$ and let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ with $\sigma_1 = \mathrm{id}_{\mathbb{K}}$.

Let $n \in \mathbb{N}$ and let $(k_1, k_2, \ldots, k_n)$ be an $\mathbb{F}$-linear independent list in $\mathbb{K}$. Let $C_1, C_2, \ldots, C_n$ be the columns of the matrix

$$\left[\sigma_i(k_j)\right]_{\substack{1\le i\le m\\1\le j\le n}} = \begin{bmatrix} k_1 & k_2 & \dots & k_n \\ \sigma_2(k_1) & \sigma_2(k_2) & \dots & \sigma_2(k_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_m(k_1) & \sigma_m(k_2) & \dots & \sigma_m(k_n) \end{bmatrix}.$$

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 $\mathbb{K}$, 3.1.22 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 $n \le m$. In particular, there exists a maximal $\mathbb{F}$-linear independent list $(a_1, a_2, \dots, a_l)$ in $\mathbb{K}$. If follows that $(a_1, \dots, a_l)$ is an $\mathbb{F}$-basis for $\mathbb{K}$ and $l \le m$. Thus $\dim_{\mathbb{F}} \mathbb{K} \le |G|$.

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

$$(1) \qquad \sum_{j=1}^{n} l_k C_j = \vec{0}.$$

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 $l_1 \ne 0_{\mathbb{K}}$. 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 $1 \le j \le n$. 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 $1 \le k \le n$ 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 $\rho(l_2) \ne l_2$. 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

$$\sum_{j=1}^{n} \rho(l_j)C_j = \vec{0}. \tag{2}$$

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

$$\sum_{j=2}^{n} (\rho(l_j) - l_j)C_j = \vec{0}. \tag{3}$$

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. □

Proposition 3.5.14. *Let $\mathbb{F} \leq \mathbb{K}$ be a field extension and let G a finite subgroup of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. Suppose that $\mathrm{Fix}_{\mathbb{K}}(G) = \mathbb{F}$ and let $a \in \mathbb{K}$. Let $a_1, a_2, \dots a_n$ be the distinct elements of $Ga = \{\sigma(a) \mid \sigma \in G\}$. Let p_a be the minimal polynomial of a over $\mathbb{F}$.*

(a) *a is algebraic over $\mathbb{F}$.*

(b) *$p_a = (x - a_1)(x - a_2)\dots(x - a_n)$.*

(c) *p_a splits over $\mathbb{K}$.*

(d) *$\mathbb{F} \leq \mathbb{K}$ is separable.*

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

$$\sigma(q) = \sigma\big((x - a_1)(x - a_2)\dots(x - a_n)\big) = \big(x - \sigma(a_1)\big)\big(x - \sigma(a_2)\big)\dots\big(x - \sigma(a_n)\big). \tag{$*$}$$

By 2.1.11 $\sigma(b) \in Ga$ for all $b \in Ga$. Also σ is injective. It follows that the function

$$\Phi : \quad Ga \to Ga, \quad b \mapsto \sigma(b)$$

is well-defined and injective. Since G is finite, also Ga is finite. Thus Φ is a bijection. It follows that

$$\big(x-\sigma(a_1)\big)\big(x-\sigma(a_2)\big)\dots\big(x-\sigma(a_n)\big) = (x-a_1)(x-a_2)\dots(x-a_n) = q.$$

Thus by $(*)$

$$(**) \qquad \sigma(q) = q.$$

Note that $q = \sum_{i=0}^{n} k_i x^i$ for some $k_0, k_1, \dots, k_n \in \mathbb{K}$. Then

$$\sum_{i=0}^{n} k_i x^i = q \overset{(**)}{=} \sigma(q) = \sigma\left(\sum_{i=0}^{n} k_i x^i\right) = \sum_{i=0}^{n} \sigma(k_i) x^i,$$

and so

$$k_i = \sigma(k_i) \text{ for all} 0 \leq i \leq n \text{and all } \sigma \in G.$$

It follows that for all $0 \leq i \leq n$,

$$k_i \in \mathrm{Fix}_{\mathbb{K}}(G) = \mathbb{F}.$$

Hence $q \in \mathbb{F}[x]$.

Since $a = \mathrm{id}_{\mathbb{K}}(a)$, there exists $1 \leq i \leq n$ with $a = a_i$. Thus $q(a) = 0_{\mathbb{F}}$ and 3.2.15(g) implies that $p_a \mid q$ in $\mathbb{F}[x]$. Note that a is a root of p_a and p_a is irreducible. Hence 3.5.8 shows that each $b \in Ga$ is a root of p_a. In particular, $x - b$ divides p_a in $\mathbb{K}[x]$. Hence also q divides p_a in $\mathbb{K}[x]$. We proved that $p_a|q$ and $q|p_a$. As p_a and q are both monic, we conclude that $p_a = q$. Hence

$$p_a = (x-a_1)(x-a_2)\dots(x-a_n).$$

As $a_i \in \mathbb{K}$ for all $1 \leq i \leq n$ this shows that 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, $\mathbb{F} \leq \mathbb{K}$ is separable. □

Definition 3.5.15. *Let $\mathbb{F} \leq \mathbb{K}$ be algebraic field extension. Then $\mathbb{F} \leq \mathbb{K}$ is called* normal *if for each $a \in \mathbb{K}$, p_a splits over $\mathbb{K}$.*

Theorem 3.5.16. *Let $\mathbb{F} \leq \mathbb{K}$ be a field extension. Then the following statements are equivalent.*

(a) *$\mathbb{F} \leq \mathbb{K}$ is Galois, that is $\mathbb{K}$ is the splitting field of a separable polynomial in $\mathbb{F}[x]$ 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) *$\mathbb{F} \leq \mathbb{K}$ is finite, separable and normal.*

Proof. (a) $\Longrightarrow$ (b): Suppose $\mathbb{F} \leq \mathbb{K}$ is Galois. Then 3.5.11 $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ 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

$$(*) \qquad \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}).$$

By 3.5.10 $\mathbb{E} \leq \mathbb{K}$ is Galois. So we can apply 3.5.11 to $\mathbb{F} \leq \mathbb{K}$ and $\mathbb{E} \leq \mathbb{K}$. Hence

$$\dim_{\mathbb{E}} \mathbb{K} \leq \dim_{\mathbb{F}} \mathbb{E} \cdot \dim_{\mathbb{E}} \mathbb{K} \overset{3.2.8}{=} \dim_{\mathbb{F}} \mathbb{K} \overset{3.5.11}{=} |\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})| \overset{(**)}{=} |\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})| \overset{3.5.11}{=} \dim_{\mathbb{E}} \mathbb{K}.$$

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 choose $G := \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(c) $\Longrightarrow$ (d): By 3.5.13 $\mathbb{F} \leq \mathbb{K}$ is finite. By 3.5.14 $\mathbb{F} \leq \mathbb{K}$ is separable, and p_a splits over $\mathbb{K}$ for all $a \in \mathbb{F}$. Thus $\mathbb{F} \leq \mathbb{K}$ is normal.

(d) $\Longrightarrow$ (a): Since $\mathbb{F} \leq \mathbb{K}$ is finite there exists a $\mathbb{K}$-basis $(a_1, a_2, \ldots, a_n)$ for $\mathbb{K}$. Then $\mathbb{K} \subseteq \mathbb{F}[a_1, a_2 \ldots, a_n] \subseteq \mathbb{K}$. So

$$(**) \qquad \mathbb{K} = \mathbb{F}[a_1, a_2 \ldots, a_n].$$

Let p_i be the minimal polynomial of a_i over $\mathbb{F}$. Since $\mathbb{F} \leq \mathbb{K}$ is separable, p_i is separable over $\mathbb{F}$. Since $\mathbb{F} \leq \mathbb{K}$ is normal, p_i splits over $\mathbb{F}$. Put $f := p_1 p_2 \ldots p_n$. Then f is separable and splits over $\mathbb{K}$. Each a_i, $1 \leq i \leq n$ is a root of p_i and so of f. Let $a_1, a_2, \ldots, a_n, \ldots, a_m$ be all the roots of f in $\mathbb{K}$. Then

$$\mathbb{K} \overset{(**)}{=} \mathbb{F}[a_1, a_2 \ldots, a_n] \subseteq \mathbb{K} \subseteq \mathbb{F}[a_1, a_2 \ldots, a_m] \subseteq \mathbb{K}$$

and so

$$K = \mathbb{F}[a_1, a_2 \ldots, a_m].$$

Thus $\mathbb{K}$ is a splitting field of f over $\mathbb{F}$. □

Lemma 3.5.17. *Let $\mathbb{F} \leq \mathbb{K}$ 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

$$\begin{array}{rcll} & \rho \in \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) & & \\ \Longleftrightarrow & \rho(k) = k \text{ for all } k \in \sigma(\mathbb{E}) & - & \text{Definition of } \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) \\ \Longleftrightarrow & \rho(\sigma(e)) = \sigma(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma(\mathbb{E}) \\ \Longleftrightarrow & \sigma^{-1}(\rho(\sigma(e)) = e \text{ for all } e \in \mathbb{E} & - & \sigma \text{ is a bijection} \\ \Longleftrightarrow & (\sigma^{-1}\rho\sigma)(e) \text{ for all } e \in \mathbb{E} & - & \text{Definition of } \sigma^{-1}\rho\sigma \\ \Longleftrightarrow & \sigma^{-1}\rho\sigma \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) & - & \text{Definition of } \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \\ \Longleftrightarrow & \rho \in \sigma \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} & - & 1.8.1(c) \end{array}$$

□

Lemma 3.5.18. *Let $\mathbb{F} \le \mathbb{K}$ be a Galois extension and $\mathbb{E}$ an intermediate field of $\mathbb{F} \le \mathbb{K}$. The following are equivalent:*

(a) $\mathbb{F} \le \mathbb{E}$ *is normal.*

(b) $\mathbb{F} \le \mathbb{E}$ *is Galois.*

(c) $\mathbb{E}$ *is invariant under* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$*, that is* $\sigma(\mathbb{E}) \subseteq \mathbb{E}$ *for all* $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$*.*

(d) $\mathbb{E} = \sigma(\mathbb{E})$ *for all* $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$*.*

Proof. (a) $\Longrightarrow$ (b): Suppose $\mathbb{F} \le \mathbb{E}$ is normal. Since $\mathbb{F} \le \mathbb{K}$ is separable, 3.4.3(d) implies that $\mathbb{F} \le \mathbb{E}$ is separable. Since $\mathbb{F} \le \mathbb{K}$ is finite, 3.1.21 implies that $\mathbb{F} \le \mathbb{E}$ is finite. Thus $\mathbb{F} \le \mathbb{E}$ is Galois by 3.5.16.

(b) $\Longrightarrow$ (c): Suppose $\mathbb{F} \le \mathbb{E}$ is Galois. Let $a \in \mathbb{E}$ and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. By 3.5.8 $\sigma(a)$ is a root of p_a in $\mathbb{K}$. Since $\mathbb{F} \le \mathbb{E}$ is normal, p_a splits over $\mathbb{E}$. Hence all roots of p_a in $\mathbb{K}$ are in $\mathbb{E}$, so $\sigma(a) \in \mathbb{E}$.

(c) $\Longrightarrow$ (d): See 2.2.11(b).

(d) $\Longrightarrow$ (a): $\sigma(\mathbb{E}) = \mathbb{E}$ for all $\sigma \in \mathrm{Aut}_{\mathbb{F}}(|K)$. Since $\mathbb{F} \le \mathbb{K}$ is Galois we conclude that 3.5.16 $\mathbb{F} = \mathrm{Fix}_{\mathbb{K}}(G)$ for some finite subgroup G of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. So by 3.5.14 p_a splits over $\mathbb{K}$ and if b is a root of p_a, then $b = \sigma(a)$ for some $\sigma \in G$. $b = \sigma(a) = \sigma(\mathbb{E}) = \mathbb{E}$. So p_a splits over $\mathbb{E}$ and $\mathbb{F} \le \mathbb{E}$ is normal. □

Theorem 3.5.19 (Fundamental Theorem of Galois Theory)**.** *Let $\mathbb{F} \le \mathbb{K}$ be a Galois Extension. Let $\mathbb{E}$ be an intermediate field of $\mathbb{F} \le \mathbb{K}$ and $G \le \mathrm{Aut}_{\mathbb{F}}(K)$.*

(a) *The function*

$$\mathbb{E} \to \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$$

is a bijection between to intermediate fields of $\mathbb{F} \le \mathbb{K}$ and the subgroups of $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. The inverse of this function 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) $\mathbb{F} \le \mathbb{E}$ *is normal if and only if* $\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$ *is normal in* $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$.

(d) *If* $\mathbb{F} \le \mathbb{E}$ *is normal, then the function*

$$\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})/\mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \mathrm{Aut}_{\mathbb{F}}(\mathbb{E}), \sigma\mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \to \sigma\mid_{\mathbb{E}}$$

is a well-defined isomorphism of groups.

Proof. Let $\mathbb{E}$ be an intermediate field of $\mathbb{F} \le \mathbb{K}$ and $G \le \mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$. By 3.5.10

$(*)$ $\quad$ *$E \le \mathbb{K}$ is Galois.*

Hence by 3.5.11

$$(**) \qquad \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) = \dim_{\mathbb{E}} \mathbb{K}.$$

(a) Since $\mathbb{E} \le \mathbb{K}$ is Galois, 3.5.16 shows that

$$(***) \qquad \mathrm{Fix}_{\mathbb{K}}(\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})) = \mathbb{E}.$$

Put $\mathbb{L} := \mathrm{Fix}_{\mathbb{K}}(G)$. Then

$$(+) \qquad G \le \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$$

We compute

$$|\mathrm{Aut}_{\mathbb{L}}(\mathbb{K})| \overset{(**)}{=} \dim_{\mathbb{E}} \mathbb{K} \overset{3.5.13}{\le} |G| \overset{(+)}{\le} |\mathrm{Aut}_{L}(\mathbb{K})|$$

It follows that equality holds everywhere. In particular,

$$(++) \qquad |G| = \dim_{\mathcal{L}} \mathbb{K} = \dim_{\mathrm{Fix}_{\mathbb{K}}(G)} \mathbb{K}$$

and $|G| = \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$. As $G \subseteq \mathrm{Aut}_{\mathbb{L}}(|K)$, this gives $G = \mathrm{Aut}_{\mathbb{L}}(\mathbb{K})$, that is

$$(+++) \qquad \mathrm{Aut}_{\mathrm{Fix}_{\mathbb{K}}(G)}(\mathbb{K}) = G.$$

By $(***)$ and $(+++)$ the two functions in (a) are inverse to each other. Thus (a) holds.

(b) The first statement is $(++)$ and the second statement is $(**)$.

(c) We have

$$\begin{array}{clcl} & \mathbb{F} \le \mathbb{E} \text{ is normal} & & \\ \Longleftrightarrow & \sigma(\mathbb{E}) = \mathbb{E} \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 3.5.18 \\ \Longleftrightarrow & \mathrm{Aut}_{\sigma(\mathbb{E})}(\mathbb{K}) = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & (a) \\ \Longleftrightarrow & \sigma\mathrm{Aut}_{\mathbb{E}}(\mathbb{K})\sigma^{-1} = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \text{ for all } \sigma \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 3.5.17 \\ \Longleftrightarrow & \mathrm{Aut}_{\mathbb{E}}(\mathbb{K}) \trianglelefteq \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) & - & 1.8.6(e) \end{array}$$

(d) By 3.5.18 $\mathbb{E}$ is $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$-invariant. So by 2.2.11(b) $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ acts on $\mathbb{E}$. The homomorphism associated to this action is

$$\alpha: \quad \mathrm{Aut}_{\mathbb{F}}(\mathbb{K}) \to \mathrm{Sym}(\mathbb{E}), \quad \sigma \mapsto \sigma\mid_{\mathbb{E}}.$$

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 $\mathrm{Im}\,\alpha \le \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Let $\rho \in \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Then by 3.3.9, 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 $\sigma \in \mathrm{Ker}\alpha$ if and only if $\alpha\mid_{\mathbb{E}} = \mathrm{id}_{\mathbb{E}}$. So $\mathrm{Ker}\alpha = \mathrm{Aut}_{\mathbb{E}}(\mathbb{K})$. Hence (d) follows from the First Isomorphism Theorem.

□

Example 3.5.20. 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 3.5.12

$$\mathbb{K} = \mathbb{Q}[a, \xi], \quad \dim_{\mathbb{Q}} \mathbb{K} = 6 \text{ and } \mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) \cong \mathrm{Sym}(R) \cong \mathrm{Sym}(3),$$

where $R = \{a, b, c\}$ is the set of roots of $x^3 - 2$. For $(x_1, \dots x_n)$ a cycle in $\mathrm{Sym}(R)$ let $\sigma_{x_1 \dots x_n}$ be the corresponding element in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$. So for example σ_{ab} is the unique element of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ with $\sigma_{ab}(a) = b, \sigma_{ab}(b) = a$ and $\sigma_{ab}(c) = c$. Then by 1.9.21 the subgroup of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ are

$$\{\mathrm{id}_{\mathbb{K}}\}, \quad \langle\sigma_{abc}\rangle, \quad \mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}), \quad \langle\sigma_{ab}\rangle, \quad \langle\sigma_{ac}\rangle, \quad \langle\sigma_{bc}\rangle, \quad \langle\sigma_{ac}\rangle.$$

Moreover, the first three (subgroups of order 1,3 or 6) are normal, while the last three (subgroups of order 2) are not normal.

We now compute the corresponding intermediate fields:

Observe that

$$\mathrm{Fix}_{\mathbb{K}}(\{\mathrm{id}_{\mathbb{K}}\}) = \mathbb{K}.$$

$\langle\sigma_{ab}\rangle$ has order 2. Hence by the FTGT 3.5.19(b), $\dim_{\mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle)} \mathbb{K} = 2$. Since $\dim_{\mathbb{Q}} \mathbb{K} = 6$, 3.2.8 implies that $\dim_{\mathbb{Q}} \mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle) = 3$. Since c is fixed by σ_{ab} and $\dim_{\mathbb{Q}} \mathbb{Q}[c] = \deg p_c = \deg(x^3 - 2) = 3$ we have

$$\mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{ab}\rangle) = \mathbb{Q}[c] = \mathbb{Q}\left[\xi^2 \sqrt[3]{2}\right].$$

Similarly,

$$\mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{ac}\rangle) = \mathbb{Q}[b] = \mathbb{Q}\left[\xi \sqrt[3]{2}\right]$$

and

$$\mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{bc}\rangle) = \mathbb{Q}[a] = \mathbb{Q}\left[\sqrt[3]{2}\right].$$

Note that $\dim_{\mathbb{Q}} \mathbb{Q}[\xi] = 2$ and so $\dim_{\mathbb{Q}[\xi]} \mathbb{K} = 3$. Hence $|\mathrm{Aut}_{\mathbb{Q}[\xi]}\mathbb{K}| = 3$. Since $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})$ has a unique subgroup of order 3 we get $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K}) = \langle\sigma_{abc}\rangle$ and so

$$\mathrm{Fix}_{\mathbb{K}}(\langle\sigma_{abc}\rangle) = \mathbb{Q}[\xi].$$

Let us verify that σ_{abc} indeed fixes ξ. From $b = a\xi$ and $c = b\xi$ we have $\xi = a^{-1}b = b^{-1}c$ and so

$$\sigma_{abc}(\xi) = \sigma_{abc}(a^{-1}b) = (\sigma_{abc}(a))^{-1}\sigma_{abc}(b) = b^{-1}c = \xi.$$

Finally by 3.5.16

$$\mathrm{Fix}_{\mathbb{K}}(\mathrm{Aut}_{\mathbb{Q}}(\mathbb{K})) = \mathbb{Q}.$$

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 $\mathbb{Q} \leq \mathbb{Q}[\xi]$ 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 $\mathbb{Q} \leq \mathbb{Q}[a]$ 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.*

(f) *$A/\sim := \{[a]_\sim \mid a \in A\}$.*

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. Let $a,b\in A$. Then the following statements are equivalent:*

(a) $a\sim b$.

(b) $b\in[a]$.

(c) $[a]\cap[b]\neq\varnothing$.

(d) $[a]=[b]$.

(e) $a\in[b]$

(f) $b\sim a$.

Proof. (a) $\Longrightarrow$ (b): Suppose $a\sim b$. Since $[a]=\{b\in A\mid a\sim b\}$ we get $b\in[a]$.

(b) $\Longrightarrow$ (c): Suppose $b\in[a]$. Since $\sim$ is reflexive we have $b\sim b$ and so $b\in[b]$. Thus $b\in[a]\cap[b]$ and $[a]\cap[b]\neq\varnothing$.

(c) $\Longrightarrow$ (d): Suppose $[a]\cap[b]\neq\varnothing$. Then there exists $c\in[a]\cap[b]$. We will first show that $[a]\subseteq[b]$. For this let, $d\in[a]$.

$$c\in[b],\quad c\in[a],\quad\text{and}\quad d\in[a].$$

The definition of an equivalence class implies:

$$b\sim c,\quad a\sim c,\quad\text{and}\quad a\sim d,$$

Since $\sim$ is symmetric, this gives

$$b\sim c,\quad c\sim a,\quad\text{and}\quad a\sim d$$

Since $\sim$ is transitive,

$$b\sim a\quad\text{and}\quad a\sim d$$

and then

$$b\sim d.$$

So $d\in[b]$. This shows that $[a]\subseteq[b]$. The situation is symmetric in a and b, so we also get $[b]\subseteq[a]$. Hence $[a]=[b]$.

(d) $\Longrightarrow$ (e): Since a is reflexive, we have $a\sim a$, so $a\in[a]$. If $[a]=[b]$ we get $a\in[b]$.

(e) $\Longrightarrow$ (f): If $a\in[b]$, the definition of $[a]$ implies $b\sim a$.

(f) $\Longrightarrow$ (a): If $b\sim a$, then $a\sim b$ since $\sim$ is symmetric. □

Corollary A.1.4. *Let $\sim$ be an equivalence relation on the set A.*

(a) *Let $a\in A$. Then a is contained a unique equivalence class X of $\sim$, namely $X=[a]_\sim$.*

(b) *$A/\sim$ is a partition of A, that is each elements of A is contained in a unique element of $A/\sim$.*

Proof. (a) Let $a \in A$ and $X \in A/\sim$. We need to show that $a \in X$ if and only if $X = [a]$. By definition of an equivalence class, $X = [b]$ for some $b \in A$. Hence

$$\begin{array}{lll} & a \in X & \\ \iff & a \in [b] & \text{– Principal of Substitution} \\ \iff & [a] = [b] & \text{– A.1.3(d),(e)} \\ \iff & [a] = X & \text{– Principal of Substitution} \end{array}$$

(b) follows from (a). □

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 $A \neq \varnothing$.*

(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 $b \in \mathrm{Im}\, f$ choose $a_b \in A$ with $f(a_b) = b$. If $b \notin \mathrm{Im}\, f$, 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. □

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 function from C to B shows that $C \prec B$. Since $\prec$ is transitive we get $A \prec B$. $\square$

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, $A \prec B$. $\square$

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 $a \in A \smallsetminus B$ 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 $d \in A \smallsetminus B$ 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 function $\mathbb{Z}^+ \to [0,1, \quad n \to \frac{1}{n}$ 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 $0 \leq r_i \leq 9$, 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. □

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