Introduction to Algebra

H113

Mariusz Wodzicki

September 1, 2010

1 Preliminaries

1.1 The language of sets

1.1.1

The concepts of a *set* and of *being an element* of a set,

$$a \in A \qquad (\text{“}a \text{ belongs to } A\text{”}), \tag{1}$$

are the two foundations on which the edifice of modern Mathematics is built. Nearly everything else is expressed using just these two concepts.

1.1.2

A set A is a subset of set B if

$$\textit{for any } a \in A\textit{, one has } a \in B. \tag{2}$$

We denote this using symbolic notation by $A \subseteq B$ and say that set A is *contained* in set B or, equivalently, that set B *contains* set A.

1.1.3

Sets A and B are declared equal if $A \subseteq B$ and $B \subseteq A$.

1.1.4

A safe guideline is to form new sets only from objects already known to be elements of some sets.

1.1.5

Very few assumptions are made about sets. They are called *axioms* of the Set Theory. Most important for us is the so-called *Separation Axiom* which, for any set A and a well-formed statement $\mathscr{P}(x)$, applicable to an arbitrary element x of A, gurantees the existence of the subset consisting of those $x \in A$ for which $\mathscr{P}(x)$ holds. This subset is denoted as follows

$$\{x \in A \mid \mathscr{P}(x)\}. \tag{3}$$

The name, *Separation Axiom*, signifies the fact that we separate elements $x \in A$ for which $\mathscr{P}(x)$ holds from those for which $\mathscr{P}(x)$ does not hold.

1.1.6

The Separtion Axiom guarantees then the existence of the *singleton* sets $\{a\}$. Indeed, if $a \in A$, then

$$\{a\} = \{x \in A \mid x = a\}. \tag{4}$$

1.1.7 The union of two sets

Another axiom guarantees that, for any two sets A and B, there exists a set containing both A and B. If this is so, then we can guarantee that the union, $A \cup B$, exists. Indeed, let C be a set containing both A and B. Then

$$A \cup B = \{c \in C \mid c \in A \text{ or } c \in B\}. \tag{5}$$

1.1.8

Axiom 1.1.7 then guarantees the existence of the sets $\{a, b\}$. Indeed, if $a \in A$ and $b \in B$, then

$$\{a, b\} = \{x \in A \cup B \mid x = a \text{ or } x = b\}. \tag{6}$$

The following lemma is as simple as useful.

Lemma 1.1 *For any elements a, b, and c of a set A, one has*

$$\{a, b\} = \{a, c\} \quad \textit{if and only if} \quad b = c. \tag{7}$$

Proof. If $b \in \{a, c\}$, then either $b = a$ or $b = c$. If $b = a$, then $c \in \{a, b\} = \{b\}$ which means that $b = c$. □

1.1.9 The power set

The third and the last axiom concerned with formation of sets guarantees, for any set A, the existence of the *set of all subsets of* A. We shall denote this set by $\mathscr{P}(A)$.

1.1.10 The empty set

Finally, we need a guarantee that there is at least one set. If this is so, then there exists a set with no elements. Indeed, if A is a set, then the set

$$\{a \in A \mid a \notin A\} \tag{8}$$

has no elements.[1] Note that, for another set B,

$$\{a \in A \mid a \notin A\} = \{b \in B \mid b \notin B\}$$

since both are subsets of $C = A \cup B$ and two subsets X, X' of a given set C are equal if and only if

$$\textit{for any } c \in C, \textit{ one has } c \in X \textit{ if and only if } c \in X'. \tag{9}$$

The set with no elements is referred to as the *empty set* and denoted $\emptyset$.

1.1.11 Natural numbers

Having the empty set, we can construct *natural numbers* as sets:

$$\mathbf{0} := \emptyset, \quad \mathbf{1} := \{\mathbf{0}\}, \quad \mathbf{2} := \{\mathbf{0}, \mathbf{1}\}, \quad \mathbf{3} := \{\mathbf{0}, \mathbf{1}, \mathbf{2}\}, \quad \ldots \tag{10}$$

or, in expanded form,

$$\mathbf{0} := \emptyset, \quad \mathbf{1} = \{\emptyset\}, \quad \mathbf{2} = \{\emptyset, \{\emptyset\}\}, \quad \mathbf{3} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \ldots .$$

[1] Symbol $\notin$ denotes the negation of $\in$; hence, $a \notin A$ reads "a does not belong to A".

1.2 The product of sets

1.2.1 The ordered pair

For any elements s and t of a set S, let

$$(s,t) := \{\{s\},\{s,t\}\}. \tag{11}$$

Note that (11) guaranteed to exist and is a subset of the power set $\mathscr{P}(S)$.

1.2.2

If

$$(s,t) = (s',t'),$$

then $\{s\} = \{s'\}$, in which case $s = s'$, or $\{s\} = \{s',t'\}$. In the former case, we apply Lemma 1.1 to deduce that

$$\{s,t\} = \{s',t'\}$$

and, since $s = s'$, to apply the same lemma again to deduce that $t = t'$.

In the latter case, both s' and t' would be elements of $\{s\}$, and that would mean that

$$s' = s = t', \qquad \text{and} \qquad (s',t') = \{\{s\}\}.$$

In particular,

$$\{s,t\} \in \{\{s\}\}$$

which means that $\{s,t\} = \{s\}$. This in turn implies that $t \in \{s\}$ which means that

$$s = t = s' = t'.$$

□

1.2.3

The above argument establishes the essential property of (11):

$$(s,t) = (s',t') \quad \text{if and only if} s = s' \text{ and } t = t'. \tag{12}$$

In all the applications of the notion of the ordered pair one uses only this property and not its specific realization. You can consider (11) to provide a proof that such an object indeed exists.

1.2.4 The (Cartesian) product of two sets

Definition 1.2 *For any sets X and Y we define their* Cartesian product *to be*

$$X\times Y := \{A \in \mathscr{P}(\mathscr{P}(X \cup Y)) \mid A = (x,y) \text{ for some } x \in X \text{ and } y \in Y\}. \tag{13}$$

Note that the set defined in (13) is guaranteed to exist and is a subset of $\mathscr{P}(\mathscr{P}(X \cup Y))$.

One can rewrite (13) in an informal way as saying

$$X\times Y = \{(x,y) \mid x \in X \text{ and } y \in Y\}. \tag{14}$$

That, however, would still require demonstrating that the set on the right-hand side of (14) exists. Definition (13) is free of this deficiency.

1.2.5

At this point one could attempt to extend the definition of the Cartesian product from two sets to any family of sets. This can be done however more efficiently by first introducing the concept of a *mapping*.

1.3 Binary Relations

1.3.1

Let X and Y be sets. We shall identify *relations* between elements of X and Y with subsets, $E \subseteq X\times Y$ of the Cartesian product of X and Y.

1.3.2 The inverse relation

We denote by $E^{-1} := \{(y,x) \in Y\times X \mid (x,y) \in E\}$ what we shall the **inverse** relation.

1.3.3 Right and left relatives

Given a binary relation $E \subseteq X\times Y$ and a subset $A \subseteq X$, we define

$$E(A) = \{y \in Y \mid (a,y) \in E \text{ for some } a \in A\} \tag{15}$$

and call $E(A)$ the *set of right E-relatives* of $A \subseteq X$.

Given a subset $B \subseteq Y$, we obtain the set $E^{-1}(B) \subseteq X$ by considering the inverse relation E^{-1}. We refer to it as the *set of left E-relatives* of $B \subseteq Y$.

1.3.4 Mappings

Binary relations $E \subseteq X \times Y$ are called *mappings* if for every $x \in X$, the set $E(\{x\})$ is a singleton set.

1.3.5

This single element is then usually denoted $f(x)$ where f here stands for the *name* of the mapping, usually a single letter of Latin or Greek alphabet, but also can be a word, often abbreviated, like $\log$, $\exp$, or $\sin$, in case of some standard mappings.

1.3.6

The above comment should alert you to the fact that even though mappings between sets form a special kind of binary relations, they come their own notational and terminological conventions.

1.3.7 The identity relation

For any set X, we shall denote by Δ_X the **identity** relation $\{(x, x') \in X \times X \mid x = x'\}$. We shall often omit subscript X when set X is clear from the context.

2 Binary operations

2.1 Idempotents, identity elements, zeros

2.1.1

Let $(X, \cdot)$ be a binary structure.

Definition 2.1 *An element $e \in X$ is an **idempotent** if $e \cdot e = e$.*

2.1.2 Example

In monoids $(\mathscr{P}(S), \cup)$ and $(\mathscr{P}(S), \cap)$ any element is an idempotent.

Definition 2.2 *An element $e \in X$ is a **left identity** if $e \cdot x = x$ for any $x \in X$. Right identities are defined similarly.*

-

2.1.3 Example

Let X be any set. Consider the projection onto the second factor

$$p_2 \colon X \times X \longrightarrow X, \qquad (x_1, x_2) \longmapsto x_2, \tag{16}$$

as a binary operation on X. *Any* element of X is a left identity. Binary structure (16) possesses no right identity except when X is a one-element set. Note that (16) is associative, i.e., $(X, p_2 \colon X \times X \longrightarrow X)$ is a semigroup.

2.1.4

The above example emphatically demonstrates that one-sided identities may be not unique. However, if e is any left identity and e' is any right identity, then they are equal:

$$e = ee' = e'.$$

It follows that in any binary structure with at least one left and at least one right identity, the two coincide, thus there exists a *two-sided* identity and it is necessary unique.

Definition 2.3 *An element $e \in X$ is a **left zero** (also called a **left sink**), if $z \cdot x = z$ for any $x \in X$. Right zeros are defined similarly.*

One-sided zeros need not be unique. In Example 2.1.3 every element is a right zero. If X is not a singleton set, then no element is a left zero in semigroup (2.1.3).

However, if $z \in X$ is a left zero, and $z' \in X$ is a right zero, then they must be equal:

$$z = zz' = z'.$$

Thus, like in the case of one-sided identities, in a binary structure with at least one left zero and at least one right zero, the two coincide, thus there exists a *two-sided* zero, and it is necessarily unique.

2.2 Central elements

2.2.1

Definition 2.4 *An element $c \in X$ is **central** if it commutes with every element of X,*

$$cx = xc \qquad (x \in X).$$

2.2.2 Center

The set of all central elements is called the *center* of $(X, \cdot)$. We will denote it $Z(X, \cdot)$, or simply $Z(X)$ when the binary operation is clear from the context.

Exercise 1 *Prove that the center of a **semigroup** is closed under multiplication and thus is a sub-semigroup.*

2.3 Rings

2.3.1

Definition 2.5 *A set R equipped with two binary operations, $+$ and $\cdot$, which are customarily referred to as **addition** and **multiplication**, is called a **ring**, if:*

$$(X, +) \text{ is an abelian group} \tag{17}$$

and the two operations are compatible in the following natural sense:

$$a(b + c) = ab + ac \qquad (\text{left distributivity}) \tag{18}$$

and

$$(b + c)a = ba + ca \qquad (\text{right distributivity}) \tag{19}$$

for any $a, b, c \in R$.

The group $(R, +)$ is called the *additive* group of the ring, and its identity element is called *zero* and denoted 0.

Exercise 2 *Prove that 0 is indeed a* zero *of the multiplicative structure, $(R, \cdot)$, i.e., that*

$$0 \cdot a = a \cdot 0 = 0$$

for any $a \in R$.

2.3.2

We say that a ring is *associative*, *commutative*, or *unital*, if the *multiplicative* structure is associative, commutative, or, respectively, possesses an identity element.

Exercise 3 *Explain why* $(\mathscr{P}(S), \cup, \cap)$ *is not a ring according to Definition 2.5. Slightly modify* one *of the two operations so that the power set becomes an associative and commutative ring with identity.*

2.4 Congruences

2.4.1

Let $\sim$ denote any congruence relation on a binary structure $(X, \cdot)$. For any element $x \in X$, we shall denote the corresponding equivalence class by $[x]$.

Exercise 4 *Prove that, for any idempotent* $e \in X$*, set* $[e]$ *is closed under multiplication, i.e. defines a substructure of* $(X, \cdot)$

Exercise 5 *Let* $z \in X$ *be any left zero and* I *denote set* $[z]$*. Prove that*

$$IX \subseteq I. \tag{20}$$

Exercise 6 *Let* $c \in X$ *be any central element and* N *denote set* $[c]$*. Prove that*

$$Na = aN, \tag{21}$$

for all $a \in X$*, where* Na *is defined as* $N\{a\}$*,*

$$Na = \{xa \mid x \in N\},$$

and aN *is defined similarly.*

A subset $N \subseteq X$ with property (21) will be called *normal*.

2.4.2

Let $(G, \cdot)$ be a group and $H \subseteq G$ be a subset. By H^{-1} we shall denote the set of inverses of elements of H,

$$H^{-1} := \{h^{-1} \mid h \in H\}. \tag{22}$$

Exercise 7 *Prove that H is a subgroup if and only if $H \cdot H^{-1} = H$.*

Exercise 8 *Consider the family of subsets*

$$\{gH \mid g \in G\}. \tag{23}$$

*Its memebers are called **left cosets** of H in G.*[2] *Prove that* (23) *is a partition of set G if and only if the coset aH which contains the identity element, e, is a subgroup of G.*

Exercise 9 *Consider the following relation on set G:*

$$a \sim_H b \quad \text{if} \quad a \in bH. \tag{24}$$

Prove that

1. *$\sim_H$ is reflexive if and only if H contains the identity element of G;*
2. *the inverse relation, $(\sim_H)^{-1}$, coincides with $\sim_{H^{-1}}$; in particular, $\sim_H$ is symmetric if and only if $H = H^{-1}$;*
3. *$\sim_H$ is transitive if and only if $H \cdot H \subseteq H$;*
4. *$\sim_H$ is an equivalence relation if and only if H is a subgroup of G;*
5. *$\sim_H$ is a congruence if and only if H is a normal subgroup of G.*

Exercise 10 *Prove that any congruence $\sim$ on a group G is of the form $\sim_N$ for some normal subgroup $N \subseteq G$.*

2.5 Notation for normal subgroups

The fact that N is a normal subgroup of a group G is often expressed using the notation

$$N \lhd G \qquad \text{or} \qquad G \rhd N. \tag{25}$$

[2] Subsets Hg, where $g \in G$, are called *right cosets*.

3 Morphisms

3.1 Morphism between relations

3.1.1

Let $(X_1, \ldots, X_n, \mathscr{R})$ and $(Y_1, \ldots, Y_n, \mathscr{S})$ be two n-ary relations.

Definition 3.1 *A collection of maps $\phi = (\phi_1, \ldots, \phi_n)$, where $\phi_i \colon X_i \longrightarrow Y_i$, is called a **morphism** from $\mathscr{R}$ to S if*

$$\mathscr{R}(x_1, \ldots, x_n) \quad \textit{implies} \quad \mathscr{S}(\phi_1(x_1), \ldots, \phi_n(x_n)). \tag{26}$$

We shall extend the arrow notation from maps between sets to morphisms between relations and other structures:

$$\phi \colon \mathscr{R} \longrightarrow \mathscr{S}.$$

3.1.2 The identity morphism

In the case when $X_i = Y_i$, for all $i = 1, \ldots, n$, and $\mathscr{R} = \mathscr{S}$, we can consider the identity morphism

$$\mathrm{id}_{\mathscr{R}} \colon \mathscr{R} \longrightarrow \mathscr{R} \tag{27}$$

where each ϕ_i is the identity map $X_i \longrightarrow X_i$.

3.1.3 Composition of morphisms

If $(W_1, \ldots, W_n, \mathscr{Q})$ is a third n-ary relation and $\psi \colon \mathscr{Q} \longrightarrow \mathscr{R}$ is a morphism,

$$\psi = (\psi_1, \ldots, \psi_n),$$

then the *composite* $\phi \circ \psi$ is defined as:

$$\phi \circ \psi := (\phi_1 \circ \psi_1, \ldots, \phi_n \circ \psi_n).$$

Note that $\phi \circ \psi$ is a morphism from $\mathscr{Q}$ to $\mathscr{S}$.

3.1.4 Isomorphisms

If, for a morphism $\phi\colon \mathscr{R} \longrightarrow \mathscr{S}$, there exists a morphism $\psi\colon \mathscr{S} \longrightarrow \mathscr{R}$ such that $\phi \circ \psi = \mathrm{id}_{\mathscr{S}}$ and $\psi \circ \phi = \mathrm{id}_{\mathscr{R}}$, then we say that ϕ is an *isomorphism* between $\mathscr{R}$ and $\mathscr{S}$, and ψ is the *inverse* of ϕ.

Exercise 11 *Prove that a morphism $\phi = (\phi_1, \ldots, \phi_n)$ is an isomorphism if and only if each $\phi_i\colon X_i \longrightarrow Y_i$ is a bijection.*

3.1.5 Endomorphisms and automorphisms

A morphism $\phi\colon \mathscr{R} \longrightarrow \mathscr{R}$ is often called an *endomorphism of* $\mathscr{R}$. If, additionally, ϕ is an isomorphism, we say that ϕ is an *automorphism* of $\mathscr{R}$.

3.2 Special cases

3.2.1 Morphisms between maps

In view of the fact that maps between sets are special cases of binary relations, it is possible to talk about morphisms between them. A morphism ϕ from a map $f\colon X_1 \longrightarrow X_2$ to a map $g\colon Y_1 \longrightarrow Y_2$ is the same as a pair of maps $\phi_i\colon X_i \longrightarrow Y_i$, where $i = 1$ or 2, such that the following diagram commutes:

$$\begin{array}{ccc} X_1 & \xrightarrow{\ f\ } & X_2 \\ {\scriptstyle \phi_1}\,\vdots\downarrow & & \downarrow\vdots\,{\scriptstyle \phi_2}, \\ Y_1 & \xrightarrow[\ g\ ]{} & Y_2 \end{array}$$

i.e., $\phi_2 \circ f = g \circ \phi_1$.

3.2.2

In the special case when some X_i is always assumed equal to some X_j, one can also restrict attention to morphisms between such relations which satisfy: $\phi_i = \phi_j$. One can then refer to such morphisms as *strict* morphisms.

3.2.3 Morphisms between operations

Given two sets equipped with n-ary operations

$$\mu\colon X\times\cdots\times X\longrightarrow X$$

and

$$\nu\colon Y\times\cdots\times Y\longrightarrow Y,$$

one can consider morphisms between them to be the morphisms between the corresponding $(n+1)$-ary relations, i.e., the $(n+1)$-tuples of maps $(\phi_1,\ldots,\phi_{n+1})$ from X to Y such that, for any $x_1,\ldots,x_n\in X$,

$$\nu(\phi_1(x_1),\ldots,\phi_n(x_n))=\phi_{n+1}(\mu(x_1,\ldots,x_n)). \tag{28}$$

In this case a *strict* morphism is a single map $\phi\colon X\longrightarrow Y$ such that

$$\nu(\phi(x_1),\ldots,\phi(x_n))=\phi(\mu(x_1,\ldots,x_n)). \tag{29}$$

This is what we call a *homomorphism* from (X,μ) to (Y,ν).

3.2.4 Isotopisms and autotopisms

Having a relaxed and a strict versions of a morphism between sets equipped with an n-ary operation we have also two versions of the notion of *isomorphism*. In order to distinguish between the two, it is customary to call isomorphisms in the relaxed sense of (28) *isotopisms*.

Isotopisms whose source and target coincide are called *autotopisms*. Autotopisms of (X,μ) form a group (cf. Exercise 11) which we will denote $A(X,\mu)$. The latter contains two subgroups: the group of *automorphisms* (in the restricted sense), $\mathrm{Aut}(X,\mu)$, and the group of *principal* autotopisms, $A_0(X,\mu)$, i.e., autotopisms of the form:

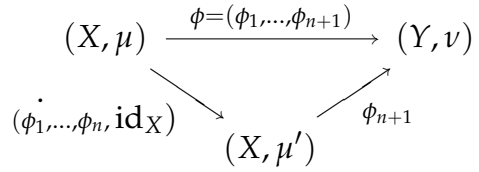
$$(\phi_1,\ldots,\phi_n,\mathrm{id}_X). \tag{30}$$

Exercise 12 *Prove that the group of principal autotopisms, $A_0(X,\mu)$, is a normal subgroup of the group of all autotopisms, $A(X,\mu)$.*

Exercise 13 *Prove that any isotopism*

$$(X,\mu)\xrightarrow{\phi=(\phi_1,\ldots,\phi_{n+1})}(Y,\nu)$$

canonically factorizes as the composition of a principal autotopism and an isomorphism:



for some n-ary operation μ' on X. (Hint: First find μ'.)

Exercise 14 *Prove that any quasigroup, $(Q,\cdot)$, is isotopic to a loop. (Hint: Find two bijections, f_1 and f_2, of set Q onto itself such that Q equipped with the operation*

$$(q_1,q_2) \longmapsto q_1 \circ q_2 := (f_1)^{-1}(q_1)\cdot(f_2)^{-1}(q_2)$$

is a loop.)

Exercise 15 *Let $(X,\cdot)$ be a binary structure. Consider a binary relation on set X:*

$$x \sim y \text{ if } \phi(x)=\phi(y) \text{ for any homomorphism } \phi \text{ into any semigroup.} \quad (31)$$

Show that $\sim$ is a congruence on $(X,\cdot)$ and that, for any homomorphism $\phi\colon X\longrightarrow S$ into a semigroup S, there exists a unique *homomorphism $\tilde{\phi}\colon X/_\sim\longrightarrow S$ such that $\phi=\tilde{\phi}\circ\pi$ where $\pi\colon X\longrightarrow X/_\sim$ is the canonical epimorphism.*

3.2.5 Homomorphisms and antihomomorphisms of binary structures

In the case of binary structures, a homomorphism from $(G,\cdot)$ to $(G',\cdot)$ is a map $\phi\colon G\longrightarrow G'$ such that

$$\phi(gh)=\phi(g)\phi(h) \quad (32)$$

for any $g,h\in G$.

If a map ϕ satisfies instead the identity

$$\phi(gh)=\phi(h)\phi(g) \qquad (g,h\in G), \quad (33)$$

then we say that ϕ is an *antihomomorphism*.

3.2.6

Composition of a homomorphism with an antihomomorphism is an antihomomorphism. Composition of two antihomomorphisms is a homomorphism.

3.2.7 The opposite binary structure

For any binary structure, $(G, \cdot)$ we define the *opposite* binary structure, $(G, \cdot)^{op} = (G^{op}, \cdot^{op})$, by setting G^{op} to be the set G whose elements, however, will be denoted g^{op} in order to clearly indicate which structure are we considering, and multiplication given by

$$g^{op} h^{op} := (hg)^{op}. \tag{34}$$

Then

$$(\ )^{op}_{G} : (G, \cdot) \longrightarrow (G^{op}, \cdot^{op}), \qquad g \longmapsto g^{op}, \tag{35}$$

can be thought of as a canonical *anti*isomorphism of $(G, \cdot)$ onto $(G^{op}, \cdot^{op})$.

3.2.8

One has $(G, \cdot)^{op} = (G, \cdot)$ if and only if $(G, \cdot)$ is commutative.

3.2.9

Note that $((G, \cdot)^{op})^{op} = (G, \cdot)$, and

$$(\ )^{op}_{G^{op}} \circ (\ )^{op}_{G} = id_G. \tag{36}$$

3.2.10 Functoriality of the opposite structure

Any homomorphism $\phi : G \longrightarrow G'$ induces a homomorphism of the corresponding opposite structures, $\phi^{op} : G^{op} \longrightarrow (G')^{op}$,

$$\phi^{op} := (\ )^{op}_{G'} \circ \phi \circ (\ )^{op}_{G^{op}}. \tag{37}$$

3.2.11

If $\phi\colon G \longrightarrow G'$ is an antihomomorphism, then both

$$\phi \circ (\ )^{op}_{G^{op}}\colon G^{op} \longrightarrow G'$$

and

$$(\ )^{op}_{G'} \circ \phi\colon G \longrightarrow (G')^{op}$$

are homomorphisms, and vice-versa.

This allows us to view antihomomorphisms as homomorphisms, except that the source, or the target, has to be replaced by the opposite structure.

3.3 Groups

3.3.1

Any semigroup G is antiisomorphic to G^{op}, cf. (35). Some semigroups are also *isomorphic* to their opposites or, what is the same, antiisomorphic to themselves.

This happens, for example, when G admits an *antiinvolution*, i.e. an antiisomorphism $*\colon G \longrightarrow G$ such that

$$*(*g)) = g \qquad (g \in G).$$

Such semigroups are called $*$-semigroups. They form an important class of $*$-semigroups.

3.3.2

Every group is equipped with a canonical antiinvolution that sends an element to its inverse,

$$g \longmapsto g^{-1}.$$

Exercise 16 *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism. Show that, for any element $g \in G$, the order of $\phi(g)$ divides the order of g.*

Exercise 17 *Prove that any subgroup of a cyclic group is cyclic.*

Exercise 18 *Let C be a cyclic group of order n. Prove that for any positive divisor d of n, there exists a unique subgroup $D \subseteq C$ of that order.*

For any two such sungroups D and E, show that $D \subseteq E$ if and only if $|D|$ divides $|E|$.

Exercise 19 *For any elements a and b in a group G, their* commutator *is defined as*

$$[a, b] := aba^{-1}b^{-1}. \tag{38}$$

Let

$$[G, G] := \{g \in G \mid g = [a_1, b_1] \cdots [a_r, b_r] \text{ for some } a_1, b_1, \ldots, a_r, b_r \in G\}. \tag{39}$$

Show that $[G, G]$ is a normal subgroup (this subgroup is called the commutator subgroup *of G). Show that the factor-group $G/[G, G]$ is abelian, and that every homomorphism $\phi\colon G \longrightarrow A$ into an abelian group factorizes through $G/[G, G]$.*

Exercise 20 *Let G be a group such that $g^2 = e$ for each $g \in G$. Show that G is abelian.*

Exercise 21 *Let G be a group such that $G/Z(G)$ is cyclic. Show that G is abelian. (Hint. Let $g \in G$ be an element that is sent by the canonical factor-map $G \twoheadrightarrow G/Z(G)$ to a generator of $G/Z(G)$. Show that $G = Z(G)\langle g \rangle$ and use this fact.)*

Exercise 22 *Let G be a nonabelian group of order 8. Show that there exists an element $a \in G$ of order 4 and show that, for any element $b \in G \setminus \langle a \rangle$, one has $bab^{-1} = a^{-1}$.*

If every element of $G \setminus \langle a \rangle$ is of order 2, the group is called the dihedral group *of order 8 and denoted D_8 or, in older notation, D_4. It is isomorphic to the group of symmetries of the square.*

If, on the other hand, $G \setminus \langle a \rangle$ contains an element of order 4, then show that it is isomorphic to the multiplicative group of quaternions:

$$Q := \{\pm 1, \pm i, \pm j, \pm k\} \tag{40}$$

where i, j, k are the imaginary quaternions. Because of this isomorphism, the unique up to isomorphism group of order 8 with a pair of noncommuting elements of order 4 is called the quaternion *group and is denoted Q.*

Exercise 23 *For both D_8 and Q, do the following.*

Let a be any element of order 4 and b be any element of $G \setminus \langle a \rangle$. Show that the cyclic subgroup, $\langle a \rangle$, is normal, and every element $g \in G$ has a representation,

$$g = a^i b^j, \tag{41}$$

for unique $i \in \mathscr{Z}/4\mathscr{Z}$ and $j \in \mathscr{Z}/2\mathscr{Z}$, in the dihedral case, and $j \in \mathscr{Z}/4\mathscr{Z}$, in the quaternion case.

Write down all elements, (41), of order 2 in G.

Find all subgroups of G and draw a diagram that displays which subgroup is contained in which one. (Do not forget about the trivial subgroups: $\{e\}$ and G).

Find the center, $Z(G)$, of G and its commutator subgroup, $[G, G]$.

Exercise 24 *Determine the structure of the group of automorphisms of cyclic groups of order 2, 4, 8, 16. Formulate a general hypothesis regarding the group of automorphisms of a cyclic group of order 2^n (and prove it, if you can).*

Exercise 25 *Determine the structure of the group of automorphisms of cyclic groups of order 3, 9, 27. Formulate a general hypothesis regarding the group of automorphisms of a cyclic group of order 3^n (and prove it, if you can).*

3.4 Group extensions

3.4.1

Definition 3.2 *A pair of group homomorphisms*

$$\mathscr{E} \; : \qquad G \xleftarrow{\;\pi\;} E \xleftarrow{\;\iota\;} N \tag{42}$$

is called an extension of G by N *if π is an epimorphism, ι is a monomorphism, and* $\operatorname{Ker} \pi = \operatorname{Im} \iota$.

3.4.2 Notation

When dealing with group extensions usually a special notation is employed:

$$G \xleftarrow{\;\pi\;} E \xleftarrow{\;\iota\;} N$$

or

$$1 \longleftarrow G \overset{\pi}{\twoheadleftarrow} E \overset{\iota}{\hookleftarrow} N \longleftarrow 1$$

Here 1 stands for the trivial, one-element group.

3.4.3 Terminology

By extension, we call the group in the middle, E, an extension of G by N. Group N is called the *kernel* of the extension.

3.4.4 Restriction of an extension to a subgroup

Exercise 26 *If H is a subgroup of G, show that $F := \pi^{-1}(H)$ is a subgroup of E.*

We speak in this case of

$$H \overset{\pi_{|F}}{\twoheadleftarrow} F \overset{\iota}{\hookleftarrow} N$$

as the *restriction* of extension $\mathscr{E}$ to H.

$$G \overset{\pi}{\twoheadleftarrow} E \overset{\iota}{\hookleftarrow} N$$

3.4.5

Exercise 27 *If G and N are finite, show that*

$$|E| = |G|\,|N|.$$

3.4.6 Split extensions

An extension $\mathscr{E}$ is said to be *split* if there exists a homomorphism $\sigma\colon G \longrightarrow E$ such that $\pi \circ \sigma = \mathrm{id}_G$. Such a homomorphism is called a *splitting* of extension $\mathscr{E}$.

Exercise 28 *Show that a group extension, (42), is split if and only if there exists a subgroup $G' \subseteq E$ such that $\pi_{|G'}$ is an isomorphism between G' and G.*

The following theorem is one of the fundamental results of Finite Group Theory.

Theorem 3.3 (Schur–Zassenhaus) *If G and N are finite groups and their orders are relatively prime, then any extension of G by N is split.* □

3.4.7 Morphisms of extensions

A morphism of an extension $\mathscr{E}$ into an extension $\mathscr{E}'$ consists of three group homomorphisms $f_0\colon G\longrightarrow G'$, $f_1\colon E\longrightarrow E'$ and $f_2\colon N\longrightarrow N'$ such that the squares in the following diagram

$$\begin{array}{rccccc} \mathscr{E}\ : & & G & \xleftarrow{\ \pi\ } & E & \xleftarrow{\ \iota\ } & N \\ & & \Big\downarrow{\scriptstyle f_0} & & \Big\downarrow{\scriptstyle f_1} & & \Big\downarrow{\scriptstyle f_2} \\ \mathscr{E}'\ : & & G' & \xleftarrow{\ \pi'\ } & E' & \xleftarrow{\ \iota'\ } & N' \end{array}$$

commute.

3.4.8 Trivial extensions

An extension $\mathscr{E}$ is said to be trivial if it is isomorphic to the extension

$$G \xleftarrow{\ p_2\ } N\times G \xleftarrow{\ i_1\ } N \tag{43}$$

where $p_2\colon N\times G\longrightarrow G$ is the projection onto the second factor, and

$$i_1\colon N\longrightarrow N\times G, \qquad n\longmapsto (n,e)$$

is the inclusion of the first factor, N, into $G\times N$.

3.4.9 Central extensions

If the kernel, N, of extension $\mathscr{E}$ is contained in the center of E, then we say that the extension is *central*.

A central extension is split if and only if it is trivial.

3.4.10

Central extensions play a fundamental role in modern Mathematics and Mathematical Physics.

3.5 Solvable groups

3.5.1 Classes of groups closed under extensions

Definition 3.4 *We say that some class $\mathscr{C}$ of groups is* closed under extensions *if in any extension,* (42)*, where G and N belong to class $\mathscr{C}$, also the middle group, E, belongs to $\mathscr{C}$.*

3.5.2 Classes of groups closed under extensions

The class of finite groups is obviously closed under extensions. A less obvious example is provided by so called torsion groups.

Definition 3.5 *We say that a group G is a* torsion group *if every element $g \in G$ has a finite order.*

Exercise 29 *Show that the class of torsion groups is closed under extensions.*

3.5.3

The class of abelian groups is obviously *not* closed under extensions. We shall explicitly construct the smallest class closed under extensions which contains the class of abelian groups. Denote the latter class by $\mathscr{S}_0$. Groups E that are extensions of an abelian group G by an abelian group N will form the larger class that will be denoted $\mathscr{S}_1$. Groups E that are extensions of an abelian group G by a group N of class $\mathscr{S}_1$ will form even the larger class that will be denoted $\mathscr{S}_2$, and so on: groups E that are extensions of an abelian group G by a group N of class $\mathscr{S}_l$ will form the class denoted $\mathscr{S}_{l+1}$.

Definition 3.6 *We say that a group G is* solvable *if it is of class $\mathscr{S}_l$ for some $l \geq 0$.*

Exercise 30 *Show that class $\mathscr{S}_1$ defined above coincides with the class of groups E whose commutator subgroup $[E, E]$ is abelian.*

3.5.4 Derived series

For any group G, define inductively the sequence of subgroups

$$G^{(0)} := G, \qquad \text{and} \qquad G^{(l+1)} := [G^{(l)}, G^{(l)}]. \tag{44}$$

Exercise 31 *Prove, by induction on l, that any subgroup F of a group E of class $\mathscr{S}_l$ is of class $\mathscr{S}_l$ itself.*

Exercise 32 *Prove, by induction on l, that class $\mathscr{S}_l$ defined above coincides with the class of groups E such that $E^{(l+1)} = 1$ or, equivalently, such that $E^{(l)}$ is abelian. (Hint. Use Exercise 31 and note that $[E, E]^{(l)} = E^{(l+1)}$.)*

3.5.5

It follows that the class of solvable groups coincides with the class of groups for which the *derived series* terminates after finitely many terms in the trivial group

$$E = E^{(0)} \triangleright E^{(1)} \triangleright \cdots \triangleright E^{(l+1)} = 1. \tag{45}$$

4 Actions

4.1 Vocabulary

4.1.1

Definition 4.1 *We say that a semigroup G* acts *on a set X if a map*

$$G \times X \longrightarrow X, \qquad (g, x) \longmapsto gx \tag{46}$$

is given such that

$$(gh)x = g(hx) \tag{47}$$

for all $g, h \in G$ and $x \in G$. The map, (46)*, satisfying* (47) *is called an* action *of G on X and a set equipped with such an action is referred to as a G-*set*.*

4.1.2

A G-action on X induces a homomorphism into the monoid of self-maps, $Map(X, X)$,

$$\lambda \colon (G, \cdot) \longrightarrow (Map(X, X), \circ), \qquad g \longmapsto \lambda_g, \tag{48}$$

where

$$\lambda_g(x) := gx. \tag{49}$$

And vice-versa, any homomorphism of G into $Map(X, X)$. defines a G-action on X:

$$(g, x) \longmapsto \lambda_g(x). \tag{50}$$

4.1.3 Equivariant maps

Given two G-sets, X and Y, a map $f \colon X \longrightarrow Y$ is said to be *equivariant* (or, G-equivariant, for added clarity), if

$$f(gx) = gf(x) \tag{51}$$

for any $g \in G$ and $x \in X$.

Equivariant maps play the role of morphisms in the world of G-sets when G is fixed.

4.1.4 Orbits

For any element $x \in X$, the subset of X

$$Gx := \{gx \mid g \in G\} \tag{52}$$

is called the *orbit* of x.

4.1.5 Stabilizers

For any element $x \in X$, the subset of G

$$G_x := \{g \in G \mid gx = x\} \tag{53}$$

is called the *stabilizer* of x, or the *isotropy* semigroup of x.

The stabilizer of any element $x \in X$ is indeed a semigroup. The stabilizer is also sometimes denoted $\mathrm{stab}_G(x)$. Remember to never confuse G_x with Gx!

4.1.6 Invariant subsets

A subset $A \subseteq X$ of a G-set is said to be *invariant* (under the action of G) if $gx \in A$ for every $x \in X'$. More natural would be to call such subsets G-subsets.

4.1.7 Fixed points

An element x of a G-set is called a *fixed point* (of the action) if

$$gx = x \qquad \text{for every } g \in G. \tag{54}$$

4.1.8 Right actions

What we have defined in Definition 4.1, was, properly speaking, a *left* action of a semigroup G on a set X. There is als a related notion of *right action*.

Definition 4.2 *We say that a semigroup* G acts *on a set* X on the right *if a map*

$$X \times G \longrightarrow X, \qquad (x, g) \longmapsto xg \tag{55}$$

is given such that

$$x(gh) = (xg)h \tag{56}$$

for all $g, h \in G$ *and* $x \in G$. *The map,* (46)*, satisfying* (47) *is called a* right action *of* G *on* X *and a set equipped with such an action is referred to as a* right G-set.

4.1.9 An example: the left and the right regular actions

For any semigroup G, the multiplication map

$$G \times G \longrightarrow G$$

can be thought as a left action of G on itself as well as a right action of G on itself. In the first case, we call it the *left multiplication* action, or the *left regular action* of G. In the second case, we refer to it as the *right multiplication* action, or the *right regular action* of G.

4.1.10

A right G-action on X induces an *anti*homomorphism into the monoid of self-maps, $Map(X,X)$,

$$\rho\colon (G,\cdot)\longrightarrow(Map(X,X),\circ),\qquad g\longmapsto\rho_g, \tag{57}$$

where

$$\rho_g(x) := xg. \tag{58}$$

And vice-versa, any anti-homomorphism of G into $Map(X,X)$. defines a G-action on X:

$$(x,g)\longmapsto\rho_g(x). \tag{59}$$

4.1.11

A right action of G is the same as the left action of G^{op}:

$$(g^{op})x := xg\qquad(g\in G, x\in X).$$

If G is a $*$-semigroup, any right action of G can be converted into a left action with help of the antiinvolution:

$$gx := x(*g)$$

For example, in the case of a group,

$$(G,X)\longrightarrow X,\qquad x\longmapsto xg^{-1},$$

is a (left) action.

4.1.12 Induced actions

An action on a set X may induce a number of related actions. An example is provided by the natural action on the set of all subsets, $\mathscr{P}(X)$ of X,

$$(g,A)\longmapsto gA := \{ga \mid a\in A\}\qquad(A\subseteq X). \tag{60}$$

Note that, invariants subsets of X are precisely the fixed points of this action.

4.1.13

If S is any set and X is a G-set, then G acts naturally on the set of all maps from S to X: a map $F\colon S \longrightarrow X$ is sent under $g \in G$ to the map

$$(gF)(s) := gF(s) \qquad (s \in S). \tag{61}$$

4.1.14

Similarly, the formula

$$(Fg)(x) := F(gx) \qquad (x \in X) \tag{62}$$

defines a natural *right* action on the set of all maps from G to S.

4.1.15 Restriction of an action to an invariant subset

Given an invariant subset $A \subseteq X$ one can *restrict* the action to A to make A into a G-set.

4.1.16 Product of G-sets

Given two G-sets X and Y, there is a natural action of G on $X \times Y$:

$$g(x, y) := (gx, gy) \qquad (g \in G,\ x \in X,\ y \in Y). \tag{63}$$

and similarly for the general case of the product of any family of G-sets.

4.1.17 Equivariant relations

Given G-sets $X_1, \ldots, X_n$, we say that an n-ary relation $(X_1, \ldots, X_n, \mathscr{R})$ is *equivariant* if, for any $x_1 \in X_1, \ldots, x_n \in X_n$, and $g \in G$, one has

$$\mathscr{R}(x_1, \ldots, x_n) \quad \text{implies} \quad \mathscr{R}(gx_1, \ldots, gx_n). \tag{64}$$

4.1.18 Quotient G-sets

If G-subsets of a G-set X are just invariant subsets, then the G-quotients of X are the quotients $X/_\sim$ by equivariant equivalence relations. Note

that the equivalence class $[gx]$ in this case depends only on the equivalence class $[x]$. In particular, the formula

$$g[x] := [gx]$$

defines an induced action of G on $X/\sim$.

4.2 Group actions

4.2.1

When a group G acts on a set X, then any $\lambda_g \colon X \longrightarrow X$ is a bijection since

$$\lambda_e = \mathrm{id}_X \quad \text{and therefore} \quad (\lambda_g)^{-1} = \lambda_{g^{-1}}$$

for any $g \in G$. Hence, a G-action is the same as a homomorphism from G into the group $\mathrm{Bij}\, X$ of self-bijections, otherwise known as *permutations* of X:

$$\lambda \colon G \longrightarrow \mathrm{Bij}_X \,. \tag{65}$$

4.2.2 Orbital decomposition of a G-set

Exercise 33 *Let G be a group acting on a set X. Show that any two orbits $\mathcal{O}$ and $\mathcal{O}'$ are either equal or disjoint.*

In particular, orbits of any group action on X form a partition of X which must correspond to some equivariant equivalence on X. The quotient is denoted X/G in this case. It is the *largest* quotient G-set of X on which G acts trivially.

The set, X/G, is often called the *space of orbits* of the G-action, or the *quotient of X by the action of G*.

4.2.3 The adjoint action

Besides the left and right multiplication actions, group G acts on G also by *conjugation*,

$$(g, x) \longmapsto {}^g x := gxg^{-1} \qquad (g, x \in G). \tag{66}$$

For any $g \in G$, the map

$$\mathrm{ad}_g \colon x \longmapsto {}^g x \qquad (x \in G) \tag{67}$$

is an automorphism of group G. Such automorphisms are called *inner*.

4.2.4

In literature very often one encounters notation $x^g := g^{-1}xg$. Note that,

$$(x, g) \longmapsto x^g$$

is a *right* action.

Exercise 34 *Let $\alpha \in \operatorname{Aut} G$ be any automorphism of group G. Show that the group of inner automorpisms,*

$$\operatorname{Inn} G := \{\mathrm{ad}_g \mid g \in G\}, \tag{68}$$

is a normal subgroup of $\operatorname{Aut} G$. (Hint: prove that

$$\alpha \circ \mathrm{ad}_g \circ \alpha^{-1} = \mathrm{ad}_{\alpha(g)} \tag{69}$$

for any $g \in G$.)

4.2.5 Outer automorphisms

The quotient group

$$\operatorname{Out} G := \operatorname{Aut} G / \operatorname{Inn} G \tag{70}$$

is called the group of *outer* automorphisms of G and denoted $\operatorname{Out} G$. Note that "outer automorphisms" are *not* automorphisms of group G but the cosets in $\operatorname{Aut} G$ of the subgroup of inner automorphisms $\operatorname{Inn} G$.

4.2.6 Conjugacy classes

The orbit of an element $x \in G$ under the adjoint action is called the *conjugacy class* of G.

4.2.7 Centralizers

For any element $a \in G$, the stabilizer of a under the adjoint action of G coincides with the so called centralizer of a,

$$C_G(a) := \{g \in G \mid ga = ag\}. \tag{71}$$

If $A \subseteq G$ is a subset, then its centralizer is the intersection of centralizers of all of its elements,

$$C_G(A) := \bigcap_{a \in A} C_G(a). \tag{72}$$

Exercise 35 *Show that, for any subset A of G, its centralizer $C_G(A)$ is a subgroup of G. Express $C_G({}^gA)$ in terms of $C_G(A)$ and $g \in G$.*

4.2.8 Normalizers

If $A \subseteq G$ is a subset, then its *normalizer*,

$$N_G(A) := \{g \in G \mid {}^gA = A\} \tag{73}$$

is the stabilizer of A with respect to the action on $\mathscr{P}(G)$ induced by the adjoint action.

Exercise 36 *Show that, for any subset A of G, its normalizer $N_G(A)$ is a subgroup of G. Express $N_G({}^gA)$ in terms of $N_G(A)$ and $g \in G$.*

Exercise 37 *Let G be a group acting on a set X and. Show that, for any $x \in X$, the stabilizer, G_x is a subgroup of G, and that*

$$G_{gx} = {}^gG_x. \tag{74}$$

4.2.9

Exercise 38 *Consider the action of a group G on itself by left multiplication. For any subgroup $H \subseteq G$, show that*

$$x \sim_H y \qquad \text{if} \qquad y^{-1}x \in H \tag{75}$$

is an equivariant equivalence on G-set G.

Vice-versa, prove that any *equivariant equivalence on G is of the form,* (75)*, for some subgroup H. (Hint: Find the candidate for H first.)*

Note that the the G-quotient, $G/_{\sim_H}$, is just the set of the left cosets, G/H.

Exercise 39 *Let G be a group and X be any G-set. Show that for any $x \in X$, the map*

$$G/H \longrightarrow Gx, \qquad gH \longmapsto gx, \tag{76}$$

where $H = G_x$, is an isomorphism of G-sets.

In particular, if the orbit of an element $x \in X$ is finite, then its cardinality equals the index of the stabilizer of x in G,

$$|Gx| = |G : G_x|. \tag{77}$$

4.2.10

By combining (77) with Exercise 33 we obtain the following observation.

Observation 4.3 *For any finite G-set X, one has the following identity*

$$|X| = \sum_{\mathscr{O}} |G : G_x|, \tag{78}$$

where the summation extends over all distinct orbits $\mathscr{O} \subseteq X$ and G_x denotes the stabilizer of any single element $x \in \mathscr{O}$.

Exercise 40 *Let H and K be two subgroups of G. Restrict the action of G by left multiplication on G/K to H. Show that the map*

$$H \longrightarrow HK/K, \qquad h \longmapsto hK, \tag{79}$$

induces an isomorphism of H-sets

$$H/H \cap K \simeq HK/K \tag{80}$$

where $HK/K \subseteq G/K$ denotes the subset

$$HK/K := \{hK \in G/K \mid h \in H\}. \tag{81}$$

Exercise 41 *Let H and K be two finite subgroups of G. Show that*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}. \tag{82}$$

Exercise 42 *Let H and K be two subgroups of G. Restrict the action of G by left multiplication on G/K to H. Show that*

$$\mathrm{stab}_H(gK) = H \cap {}^gK. \tag{83}$$

Exercise 43 *Let H a subgroup of G. Show that $H = gH$ is a fixed point of the H-action on G/H if and only if $g \in N_G(H)$. In other words,*

$$\mathrm{Fix}_H(G/H) = N_G(H)/H, \tag{84}$$

and thus the number of fixed points of the H-action on G/H equals the index of H in its normalizer, $N_G(H)$,

$$|\,\mathrm{Fix}_H(G/H)| = |N_G(H) : H|. \tag{85}$$

Exercise 44 *Let H be a subgroup of G. Consider the set of all the conjugate subgroups,*

$$X := \{{}^gH \mid g \in G\} \tag{86}$$

Show that

$$|X| = |G : N_G(H)|. \tag{87}$$

Group G acts on X by conjugation.

$$\mathrm{stab}_G({}^gH) = {}^gN_G(H). \tag{88}$$

4.2.11 Restriction of an action to a subgroup

A G-set X can be viewed as an H-set for any subgriup H of G by restrictiong the action to elements $h \in H$. In this case its orbit structure is different. Any G-orbit $\mathscr{O} = Gx$ is naturally H-invariant but H may not act on $\mathscr{O}$ transitively.

4.2.12

Subgroup H acts on Gx transitively if and only if

$$G = H \cdot \mathrm{stab}_G(x). \tag{89}$$

Note that in this case also $G = {}^gH \cdot \mathrm{stab}_G(x)$ for any $g \in G$.

Exercise 45 *Deduce that that the conjugacy class of $a \in G$ in G equals the conjugacy class of a with respect to H if and only if*

$$G = HC_G(a) \tag{90}$$

4.2.13 Frattini's Argument

Exercise 46 *By looking at the action on the power set $\mathscr{P}(G)$ which is induced by the adjoint action of G, we deduce that the set of G-conjugates of a subset $S \subseteq G$ coincides with the set of H-conjugates,*

$${}^GS = {}^HS, \tag{91}$$

if and only if

$$G = HN_G(S). \tag{92}$$

(Note that both ${}^GS$ and ${}^HS$ are subsets of $\mathscr{P}(G)$, not of G. In other words, they are families *of subsets of G.)*

The above observation is frequently used in Group Theory and it is known under the name of *Frattini's Argument*.

4.3 p-groups

4.3.1

Proposition 4.4 *Let G be a group of order p^n, where p is a prime, and X be a finite G-set. Then*

$$|X| = |\operatorname{Fix}_G(X)| \mod p. \tag{93}$$

Proof. By (78), one has

$$|X| = \sum_{|\mathscr{O}|=1} |G : G_x| + \sum_{|\mathscr{O}|>1} |G : G_x| = |\operatorname{Fix}_G(X)| + \sum_{|\mathscr{O}|>1} |G : G_x|. \tag{94}$$

Each $|\mathscr{O}| = |G : G_x|$ is, by Lagrange's Teorem, a divisor of $|G| = p^n$, and thus is a power of p itself. If $|\mathscr{O}| > 1$, then $|\mathscr{O}|$ is divisible by p. Hence the right-hand-side of (94) is the sum of $|\operatorname{Fix}_G(X)|$ and a natural number divisible by p. □

4.3.2 Cauchy's Theorem

Theorem 4.5 (Cauchy's Theorem) *If a prime p divides the order of a finite group G, then*

$$\{g \in G \mid |g| = p\} = -1 \mod p. \tag{95}$$

In particular, there exists an element of G of order p.

Proof. Consider the action of group $\mathbb{Z}/p\mathbb{Z}$ by cyclic permutations of the factors in G^p:

$$\lambda_i \colon (g_1, \ldots, g_p) \longmapsto (g_{p-i+1}, \ldots, g_p, g_1 \ldots, g_{p-i}), \qquad (i \in \mathbb{Z}/p\mathbb{Z}).$$

Exercise 47 *Show that the subset*

$$X := \{(g_1, \ldots, g_p) \mid g_1 \cdots g_p = e\} \tag{96}$$

is invariant under the action of $\mathbb{Z}/p\mathbb{Z}$.

The map

$$(g_1, \ldots, g_{p-1}) \longmapsto (g_1, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}),$$

provides a bijection from G^{p-1} onto X, hence

$$|X| = |G^{p-1}| = |G|^{p-1}$$

is divisible by p.

A p-tuple $(g_1, \ldots, g_p)$ is a fixed point of the $\mathbb{Z}/p\mathbb{Z}$-action on X if and only if $g_1, \ldots, g_p$ is of the form $(g, \ldots, g)$ and $g^p = e$. In other words, the map

$$g \longmapsto (g, \ldots, g)$$

identifies the set

$$\{g \in G \mid g^p = e\} = \{e\} \sqcup \{g \in G \mid |g| = p\}$$

with the set of fixed points

$$\mathrm{Fix}_{\mathbb{Z}_p\mathbb{Z}}(X),$$

and the number of elements in the latter is, in view of Proposition 4.4, and a remark in the previous paragraph, divisible by p. □

4·3·3

A group G is said to be a *p-group* (for a prime p), if the order of every element $g \in G$ is a power of p.

Corollary 4.6 *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Exercise 48 *Prove Corollary 4.6.*

Exercise 49 *Prove that the center, $Z(G)$, of any finite p-group G is nontrivial, i.e., $Z(G) \neq \{e\}$. (Hint: consider the adjoint action of G.)*

Exercise 50 *Let H be a proper subgroup of a finite p-group G. Prove that there exists an intermediate subgroup $H \subsetneq H' \subseteq G$ such that $H \lhd H'$.*

Exercise 50 leads to a number of facts about the structure of a finite p-group.

4.3.4 Maximal subgroups

A proper subgroup $M \subset G$ is said to be *maximal* if any M is not contained in any proper subgroup of G.

Exercise 51 *Let H be a subgroup of prime index in a group G. Show that H is maximal.*

Exercise 52 *Let H be a subgroup of index 2 in a group G. Show that H is normal.*

4.3.5 An example

Consider the group of permutations of a 3-element set, Σ_3. All of its proper subgroups are cyclic:

$$\langle(1\,2\,3)\rangle, \qquad \langle(1\,2)\rangle, \qquad \langle(2\,3)\rangle, \qquad \langle(3\,1)\rangle,$$

and of indices 3 and 2, respectively, hence maximal. All three subgroups of index 3 are conjugate to each other, therefore they are not normal.

Group Σ_3 has order $6 = 2 \cdot 3$ and thus is the smallest non-p-group. For, in a p-group all maximal subgroups are normal.

Corollary 4.7 *Any maximal subgroup M of a finite p-group is normal.* □

This is an immediate corollary of Exercise 50.

Lemma 4.8 *Let H be a subgroup of index greater than p in a p-group G. Then there exists an intermediate subgroup*

$$H \subsetneq H' \subsetneq G. \tag{97}$$

Proof. Let H' be a subgroup of G such that $H \lhd H'$. If H is not normal in G, then H' is the desired group.

If H is normal, then, in view of Cauchy's Theorem, there exists a cyclic subgrup C of order p in G/H. Let H' be a preimage of C in G under the canonical quotient map $\pi\colon G \longrightarrow G/H$, cf. 3.4.4. Its order is $|H|\,|C|$, cf. Exercise 27, and

$$|H'| = |H|\,|C| = |H| \cdot p < |H|\,|G/H|$$

since $|G/H| = |G : H| > p$ by hypothesis. □

As an immediate corollary, we obtain that any flag of subgroups in a group of order p can be extended to a maximal flag of subgroups of orders dividing the order of G:

$$1 < p < p^2 < \cdots .$$

Corollary 4.9 *Any flag of subgroups*

$$H_{p^{i_1}} \subset \cdots \subset H_{p^{i_r}} \tag{98}$$

in a p-group G of order p^n, where $H_{p^{i_k}}$ has order p^{i_k}, is contained in some maximal flag

$$1 \subset \cdots \subset H_{p^i} \subset \cdots \subset G \tag{99}$$

where H_{p^i} has order p^i, $i = 0, 1, \ldots, n$. □

4.4 p-subgroups of finite groups

4.4.1

Exercise 53 *a Let P be a p-subgroup of a group G. Show that p divides either the index of P in its normalizer,*

$$|N_G(P) : P|,$$

or the number of subgroups in G which are conjugate to P is congruent to 1 modulo p,

$$|\{{}^gP \mid g \in G\}| = 1 \mod p. \tag{100}$$

Hint: prove that

$$|G : P| = |N_G(P) : P| \mod p. \tag{101}$$

4.4.2

Definition 4.10 *A maximal p-subgroup P of a finite group G is called a* Sylow p-subgroup.

4·4·3

Let P be a Sylow p-subgroup and let $|P| = p^l$. If $|N_G(P) : P|$ were divisible by p, then the quotient group $N_G(P)/P$ would contain an element a of order p. This follows from Cauchy's Theorem, cf. 4.5.

In that case, $N_G(P)$ would contain a subgroup, P', containing P and of order p^{l+1}. Indeed, the preimage $\pi^{-1}(\langle a \rangle)$ under the canonical epimorphism

$$\pi\colon N_G(P) \twoheadrightarrow N_G(P)/P$$

would be such a group. That would contradict the maximality of P.

Thus, $|N(P) : P|$ is not divisible by p. By combining this with Exercise 53, we deduce that the number of conjugates of any Sylow p-subgroup equals 1 modulo p, cf. (100).

4·4·4

By combining the result of Section 4.4.3 with (101), we deduce that the index, $|G : P|$, is not divisible by p. In other words, the order of a maximal p-subgroup in G coicides with the maximum power p^e of p which divides $|G|$.

If we represent $|G|$ as the product of p^e and an integer m not divisible by p, then we obtain that the number of conjugates of a Sylow p-subgroup,

$$|G : N_G(P)|$$

divides

$$m = |G : P|.$$

.

4·4·5

Let Q be any p-subgroup. It acts on G/P by left multiplication. By combining the result of Section 4.4.3 with conguence (101) and Proposition 4.4, we deduce that

$$|\operatorname{Fix}_Q(G/P)| = 1 \mod p. \tag{102}$$

Thus, there exists $g \in G$ such that

$$Q \subseteq \operatorname{stab}_G(gP) = {}^gP,$$

cf. (83).

We arrive at the following fundamental result.

Theorem 4.11 *Let G be a group of order $p^e m$ where $p \nmid m$. Then:*

(i) Any p-group Q is contained in some Sylow p-subgroup P and all Sylow p-subgroups have order p^e.

(ii) Any two Sylow p-subgroups are conjugate.

(iii) The number of Sylow p-subgroups, $s_p(G)$, satisfies the following two constraints:

$$s_p(G) \mid m, \tag{103}$$

and

$$s_p(G) = 1 \mod p. \tag{104}$$

4.4.6

Assertions (i), (ii), and (iii), are usually called the *First*, the *Second*, and the *Third Sylow Theorems*.

Exercise 54 *Show that $N_G(N_G(P)) = N_G(P)$ for any Sylow p-subgroup $P \subseteq G$.*

4.4.7 Frattini's Argument (in its original form)

Exercise 55 *Let Q be a Sylow p-subgroup of a normal subgroup $H \triangleleft G$. Show that*

$$G = HN_G(Q). \tag{105}$$

Exercise 56 *Let P be a Sylow p-subgroup of G and $H \triangleleft G$ be a normal subgroup. Show that $P \cap H$ is a Sylow subgroup of H.*

4.5 Nilpotent groups

4.6

In Section 3.5 we introduced the class of sovable groups, $\mathscr{S}$, which is the smallest class closed under extensions which contains abelian groups. Now we shall discuss an important subclass $\mathscr{N} \subset \mathscr{S}$ of *nilpotent groups*.

4.6.1

Denote the class of abelian groups by $\mathscr{N}_0$. Groups that are *central* extensions of abelian groups will form the class $\mathscr{N}_1$. Groups that are central extensions of a group of class $\mathscr{N}_1$ will form the class $\mathscr{N}_2$, and so on: groups that are central extensions of a group of class $\mathscr{N}_l$ will form the class denoted $\mathscr{N}_{l+1}$.

Definition 4.12 *A group is said to be* nilpotent *(of level l) if it belongs to class $\mathscr{N}_l$.*

Exercise 57 *Show that, for any group G, the following two conditions are equivalent:*

(a) G is nilpotent of level 1;
(b) $[G, G] \subseteq Z(G)$.

4.6.2 Upper central series

For any group G, define inductively the sequence of subgroups

$$Z_0(G) := 1, \qquad \text{and} \qquad Z_{l+1}(G) := \{g \in G \mid [g, G] \subseteq Z_l(G)\}. \tag{106}$$

4.6.3

It follows directly from the definition that $Z_{l+1}(G)/Z_l(G)$ is contained in the center of $G/Z_l(G)$ and thus $G/Z_l(G)$ is a central extension of $G/Z_{l+1}(G)$ by $Z_{l+1}(G)/Z_l(G)$.

Accordingly, if $Z_{l+1}(G) = G$, then $G/Z_l(G)$ is abelian, i.e., nilpotent of level 0, $G/Z_{l-1}(G)$ is nilpotent of level 1, and so on. In particular, $G = G/Z_0(G)$ is nilpotent of level l.

Exercise 58 *Prove that, for any group G and $l \in \mathbb{N}$, one has*

$$Z_l(G/Z(G)) = Z_{l+1}/Z(G). \tag{107}$$

4.6.4 Lower central series

For any group G, define inductively the sequence of subgroups

$$L_0(G) := G, \qquad \text{and} \qquad L_{l+1}(G) := [L_l(G), G]. \tag{108}$$

4.6.5

It follows directly from the respective definitions that, for any group G, the following three conditions are equivalent:

(a) $Z_{l+1}(G) = G$;

(b) $L_{l+1}(G) = 1$;

(c) $[\dots[,[g_0,g_1],g_2],\dots,g_l] = 1$ for any $g_0,g_1,\dots,g_l \in G$.

By combining this with 4.6.3 and with Exercise 58, we see that any of the above conditions characterizes groups nilpotent of level l.

4.6.6

Exercise 59 *Prove that for any proper subgroup $H \subset G$, one has*

$$N_G(H) \neq H. \tag{109}$$

.

4.6.7

Exercise 60 *Prove that every Sylow subgroup of a finite nilpotent group G is normal in G.*

4.6.8

Exercise 61 *Deduce from Exercise 4.6.7 that a finite group is nilpotent if and only if G is isomorphic to a product of p-groups.*

4.6.9 The Frattini subgroup

For any finite group G we define $\operatorname{Frat} G$ as the intersection of all of its *maximal* (proper) subgroups.

Exercise 62 *Let $G = \langle g \rangle$ be a cyclic group of order*

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

Prove that $\langle g^m \rangle$ is a maximal subgroup of G if and only if m is prime. Use this to prove that $\operatorname{Frat} G = \langle g^{p_1 \cdots p_r} \rangle$. In particular,

$$|\operatorname{Frat} G| = \tfrac{n}{p_1 \cdots p_r} = p_1^{e_1-1} \cdots p_r^{e_r-1}.$$

It follows that $\operatorname{Frat} C_n = 1$ if and only if n is square-free.

Exercise 63 *Prove that* $\operatorname{Frat} G \lhd G$.

Exercise 64 *Prove that, for any subgroup* $H \subseteq G$, *if*

$$(\operatorname{Frat} G)H = G,$$

then

$$H = G.$$

4.6.10

In particular, a subset $X \cup \operatorname{Frat} G$ generates group G if and only if X alone generates G.

Exercise 65 *Prove that the Frattini subgroup of any finite group is nilpotent. (Hint. Prove that every Sylow subgroup of* $\operatorname{Frat} G$ *is normal in* G.*)*

5 Group structure

5.1 Semidirect products

5.1.1

Given an action of a group G on a group N, which is understood to be via automorphisms of N:

$$\varphi\colon G \longrightarrow \operatorname{Aut} N, \tag{110}$$

one can construct the so called *semidirect product* of G and N, denoted $N \rtimes_\varphi G$, which is set $N \times G$ equipped with the multiplication

$$(m, a)(n, b) := (m\varphi_a(n), ab). \tag{111}$$

5.1.2

Note that

$${}^{(e,a)}(n, e) = (\varphi_a(n), e).$$

Thus, the action of G on N is realized in the semidirect product, $N \rtimes_\varphi G$, as conjugation of elements of $M \times 1$ by elements of $1 \times G$.

Exercise 66 *Prove that* (111) *is associative; find* $(n,a)^{-1}$.

Exercise 67 *Prove that if in a group* G *there is a normal subgroup* N *and a subgroup* H *such that*

$$G = NH \qquad \textit{and} \qquad N \cap H = 1, \tag{112}$$

then G *is isomorphic to the semidirect product* $N \rtimes_\varphi H$ *for some* φ. *Find* φ.

In this case we speak of so called *(internal) semidirect product*.

5.1.3 Semidirect products and split extensions

Semidirect product, $N \rtimes_\varphi H$, determines a natural extension of H by N, cf. 3.4.8:

$$H \xleftarrow{\;p_2\;} N \rtimes H \xleftarrow{\;i_1\;} N \tag{113}$$

This extension is equipped with a canoical splitting:

$$i_2 \colon H \longrightarrow N \rtimes_\varphi H, \qquad h \longmapsto (e,h). \tag{114}$$

Exercise 68 *Prove that any split extension of* H *by* N *is isomorphic to the semidirect product extension,* (113)*, for some* $\varphi \colon H \longrightarrow \operatorname{Aut} N$.

5.1.4 Isomorphisms of semidirect products

Let

$$f \colon N \rtimes_\varphi H \longrightarrow N' \rtimes_{\varphi'} H' \tag{115}$$

be a homomorphism of semidirect products such that

$$f(H) \subseteq H'$$

and

$$f \text{ identifies } N \text{ with } N'.$$

Denote the restriction of f to H by χ and consider it to be a homomorphism

$$\chi \colon H \longrightarrow H' \tag{116}$$

and, similarly, denote the restriction of f to N by ν and consider it to be an isomorphism

$$\nu \colon N \xrightarrow{\sim} N'. \tag{117}$$

Exercise 69 *Show that the following diagram is commutative*

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \operatorname{Aut} N \\ \Big\downarrow{\scriptstyle \chi} & & \Big\downarrow{\scriptstyle \mathrm{ad}_\nu} \\ H' & \xrightarrow{\varphi'} & \operatorname{Aut} N' \end{array} \tag{118}$$

where ad_ν *is the isomorphism induced by* ν*:*

$$\mathrm{ad}_\nu \colon \alpha \longmapsto {}^\nu\alpha = \nu \circ \alpha \circ \nu^{-1} \qquad (\alpha \in \operatorname{Aut} N). \tag{119}$$

Vice-versa, show that a pair consisting of a homomorphism, (116)*, and an isomorphism,* (117)*, defines a homomorphism* (115) *by setting*

$$f(n,h) := (\nu(n), \chi(h)) \qquad (n \in N;\, h \in H) \tag{120}$$

if diagram (118) *is commutative.*

5.1.5

Above we described a certain class of homomorphisms between semidirect products. In particular, we described all isomorphisms between $N \rtimes_\varphi H$ and $N' \rtimes_{\varphi'} H'$ such that $f(N) = N'$ and $f(H) = H'$.

Exercise 70 *Suppose that any two cyclic subgroups of prime order* p *in* $\operatorname{Aut} N$ *are conjugate. Show that, for any nontrivial homomorphisms of a cyclic group,* C_p*, of order* p *into* $\operatorname{Aut} N$*,*

$$\varphi \colon C_p \longrightarrow \operatorname{Aut} N \qquad \textit{and} \qquad \varphi \colon C_p \longrightarrow \operatorname{Aut} N,$$

the corresponding semidirect products are isomorphic:

$$N \rtimes_\varphi H \simeq N \rtimes_{\varphi'} H.$$

5.1.6

An immediate corollary of Exercise 70 is that if a finite group G equals NC_p where N is normal in G and any two cyclic subgroups of $\operatorname{Aut} N$ of order p are conjugate, then G is either isomorphic to the product $N \times C_p$ (case when φ is trivial), or is a nontrivial semidirect product $N \rtimes C_p$, and all such semidirect products are isomorphic to each other.

5.2 The group of automorphisms of a group

5.2.1

In order to be able to take advantage of Sylow's Theorems in classification of finite groups of small order one needs to understand better the structure of the automorphism group Aut of some frequently encountered groups.

5.2.2 The case of an abelian group

The set of all endomorphisms, $\operatorname{End} A$, of an abelian group $(A, +)$ forms a group under addition. The composition of endomorphisms is distributive with respect to addition, and thus $\operatorname{End} A$ is a ring with identity. Its group of invertible elements coincides with the group of automorphisms of A:

$$(\operatorname{End} A)^* = \operatorname{Aut} A. \tag{121}$$

5.2.3 The case of a cyclic group

In particular, for a cyclic group C_n of order

$$n = p_1^{m_1} \cdots p_r^{m_r},$$

one has a canonical isomorphism

$$\operatorname{End} C_n \simeq \mathbb{Z}/n\mathbb{Z}, \tag{122}$$

hence the canonical isomorphism

$$\operatorname{Aut} C_n \simeq (\mathbb{Z}/n\mathbb{Z})^* \tag{123}$$

To an element $l \in (\mathbb{Z}/n\mathbb{Z})^*$ corresponds an automorphism of C_n which sends any element $x \in C_n$ to x^l (we are using multiplicative

Since,

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z},$$

one has the isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^* \times \cdots (\mathbb{Z}/p_r^{m_r}\mathbb{Z})^*,$$

i.e., the group of automorphisms of C_n is the product

$$\operatorname{Aut} C_n \simeq \operatorname{Aut} C p_1^{m_1} \times \cdots \times \operatorname{Aut} C p_r^{m_r}.$$

Theorem 5.1 *The group of automorphisms of the cyclic group of order p^m is cyclic,*

$$C_{(p-1)p^{m-1}} \simeq C_{p-1} \times C_{p^{m-1}}, \tag{124}$$

if p is odd, and isomorphic to

$$\{\pm 1\} \times C_{2^{m-2}} \tag{125}$$

when $p = 2$ and $m \geq 2$.

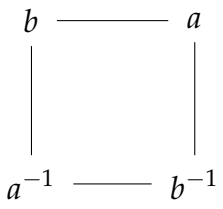
5.2.4

In the following exercises you are asked to determine $\operatorname{Aut} P$ for a few simplest 2-groups P. First, find the order of $\operatorname{Aut} P$, and then construct automorphisms of P which generate a subgroup in $\operatorname{Aut} P$ of the desired order.

Exercise 71 *Show that $\operatorname{Aut}(C_2 \times C_4)$ is the dihedral group, D_8, of order 8. (Hint: Find two elements of order 4 in $A = C_2 \times C_4$ such that*

$$X = \{a, b, a^{-1}, b^{-1}\}$$

is the set of all elements of order 4 in A. Show that the restriction to X of a nontrivial automorphism of A is a nontrivial permutation of X. This defines an embedding of $\operatorname{Aut} A$ into Σ_X. Show that any symmetry of the square



extends to an automorphism of A. Finally, find a permutation of X which does not extend to an automorphism. Deduce from this that $\operatorname{Aut} A \simeq D_8$.

Exercise 72 *Determine the structure of $\operatorname{Aut} D_8$. (Hint. Group D_8 has 5 elements of order 2: one element is central and the remaining four belong two conjugacy classes. 'Organize' those four elements into a square and show that the restriction of any automorphism of D_8 to the non-central elements of order 2*

defines an isomorphism of $\operatorname{Aut} D_8$ *with the group of symmetries of that 'square'. The latter is isomorphic to* D_8 *but the canonical map*

$$\operatorname{ad}\colon D_8 \longrightarrow \operatorname{Aut} D_8 \tag{126}$$

is not an isomorphism. What is its kernel and its image?)

Exercise 73 *Find the order,* $|\operatorname{Aut} Q|$*, of the group of automorphisms of the quaternion group* Q*. (Hint. Determine the subgroup of* $\operatorname{Aut} Q$ *which consists of automorphisms that fix* i*, and then, for any element* q *of the set of elements of order 4 in* Q*,*

$$\{\pm i, \pm j, \pm k\},$$

construct an automorphism of Q *which sends* i *to* q*.)*

Exercise 74 *Prove that any group* G *of order 56 is either a (not necessarily nontrivial) semidirect product*

$$C_7 \rtimes P_2$$

of a cyclic group of order 7 and a 2-subgroup P_2 *of order 8, or is a nontrivial semidirect product*

$$C_2^3 \rtimes C_7$$

of an elementary abelian 2-group of rank 3 and a cyclic group of order 7.

6 The permutation and the alternating groups

6.1 Cyclic decomposition of a permutation

6.1.1 Support of a permutation

Let $\sigma \in \operatorname{Bij}_X$ be a permutation of a set X. Its *support* is the set

$$\operatorname{supp} \sigma := \{x \in X \mid \sigma(x) \neq x\}. \tag{127}$$

Exercise 75 *Show that:*

$$\operatorname{supp}(\rho \circ \sigma) \subseteq \operatorname{supp} \rho \cup \operatorname{supp} \sigma \tag{128}$$

and

$$\operatorname{supp}(\sigma^{-1}) = \operatorname{supp} \sigma. \tag{129}$$

Deduce from this that the set of permutations with finite support

$$\Sigma_X := \{\sigma \in \operatorname{Bij}_X \mid \operatorname{supp} \sigma \textit{ is finite}\} \tag{130}$$

is a normal subgroup of Bij_X*.*

6.1.2

It is clear that $\operatorname{supp}\sigma$ is the complement in X of the set of fixed points of the action of the cyclic group $\langle\sigma\rangle$ on X,

$$\operatorname{supp}\sigma = X \setminus \operatorname{Fix}_{\langle\sigma\rangle}(X).$$

In particular, the support is a $\langle\sigma\rangle$-invariant subset of X.

6.1.3 Cycles

A permutation λ of a set X is called a *cycle* of *length* l if $\operatorname{supp}\lambda$ is finite and consists of a single orbit group $\langle\lambda\rangle$,

$$\operatorname{supp}\lambda = \{x_j \mid j \in \mathbb{Z}/l\mathbb{Z}\} \quad \text{and} \quad \lambda(x_j) = x_{j+1}, \quad (j \in \mathbb{Z}/l\mathbb{Z}). \tag{131}$$

(Note that since we index elements of $\mathcal{O}$ by elements of ring $\mathbb{Z}/l\mathbb{Z}$ rather than by integers, $l + 1 = 1$.)

6.1.4 Cycle notation

When dealing with cycles it is customary to employ a special notation

$$\lambda = (x_1 \ \ldots \ x_l) \tag{132}$$

(note the absence of commas).

6.1.5

Cycles of length l will be also called l-cycles. Their order equals l. Cycles of order 2 are called *transpositions*.

Exercise 76 *Suppose that set X has at least 4 distinct elements u, v, w, and x. Show that $(u\ v)(w\ x)$ and $(u\ v)(v\ w)$ can be expressed as products of 3-cycles.*

Exercise 77 *Suppose that set X has at least l distinct elements $x_1, \ldots, x_l$ where $l > 3$. Show that the 3-cycle, $(x_1\ x_2\ x_3)$ can be expressed as the product of 2 l-cycles.*

Exercise 78 *Suppose that set X has at least l distinct elements $x_1, \ldots, x_l$. Show that the l-cycle, $(x_1\ \ldots\ x_l)$ can be expressed as the product of $l - 1$ transpositions.*

6.1.6

We say that two permutations ρ and σ are *disjoint* if

$$\operatorname{supp}\rho \cap \operatorname{supp}\sigma = \emptyset.$$

Exercise 79 *Show that disjoint permutations commute*

$$\rho\sigma = \sigma\rho.$$

Exercise 80 *Let λ be a cycle of length $l = mn$. Show that λ^m is the product of m (mutually) disjoint cycles of length n,*

$$\sigma^m = \lambda_1 \circ \cdots \circ \lambda_m.$$

Proposition 6.1 *Any permutation with finite support, $\sigma \in \Sigma_X$, is the product,*

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r, \tag{133}$$

of disjoint cycles.

Proof. Let

$$\operatorname{supp}\sigma = \mathscr{O}_1 \cup \cdots \cup \mathscr{O}_r \tag{134}$$

be the decomposition of the support of σ into the disjoint union of orbits of the $\langle\sigma\rangle$-action on X. For each orbit, $\mathscr{O}_i$, let

$$\mathscr{O}_i = \{x_{i1}, \ldots, x_{il_i}\}$$

where

$$\sigma(x_{ij}) = x_{i,j+1} \qquad (j \in \mathbb{Z}/l_i\mathbb{Z}).$$

Let

$$\lambda_i := (x_{i1} \ \ldots \ x_{il_i})$$

be the cycle of length $l_i = |\mathscr{O}_i|$ which cyclically permutes the elements of $\mathscr{O}_i$. Since the orbits $\mathscr{O}_i$ in (134) are disjoint, the corresponding cycles are mutually disjoint, and (133) holds. □

6.1.7

The decomposition of σ into a product of disjoint cycles is unique up to a rearrangement of terms in (133).

Indeed, for any such decomposition, (133), the support of each λ_i is an orbit, call it $\mathscr{O}_i$, of $\langle\sigma\rangle$ on X, and the action of σ on $\mathscr{O}_i$ determines λ_i. Thus, knowledge of decomposition of X into orbits of $\langle\sigma\rangle$-action, and the action of σ on each orbit, determine the decompostion of σ into a product of disjoint cycles uniquely up to the order in which one composes the cycles.

Exercise 81 *Let λ be any cycle of length l. Show that λ^m is a cycle, necessarily of length$l$, if m relatively prime to l.*

6.1.8

The list

$$(l_1, \ldots, l_r) \tag{135}$$

is called the *cyclic type* of permutation σ. The order in (135) is unimportant. There are other ways to denote the cyclic type of a permutation, e.g., $2^3 3^2 7$, $2_3 3_2 7$, $2+2+2+3+3+7$, all can denote cyclic type

$$(2, 2, 2, 3, 3, 7).$$

Exercise 82 *Show that the order of a permutation σ of (cyclic) type* (135) *is the least common multiple of numbers $l_1, \ldots, l_r$,*

$$|\sigma| = \mathrm{lcm}(l_1, \ldots, l_r).$$

6.1.9

Exercise 83 *Show that two permutations ρ and σ are conjugate to each other if and only if they have the same cyclic type.*

Exercise 84 *Show that for any $\sigma \in \Sigma_X$, its inverse, σ^{-1}, is conjugate to σ in Σ_X.*

6.1.10 Parity of a permutation

For a permutation σ of type (135), its *parity* is defined as

$$\tilde{\sigma} := (l_1 - 1) + \cdots + (l_r - 1) \mod 2. \tag{136}$$

It is an element of $\mathbb{Z}/2Z$. Permutations of parity 0 are called *even*, and those of parity 1 – are called *odd*. Parity is sometimes written multiplicatively as $+1$, for even, and -1, for odd permutations.

6.1.11

It follows from Exercise 78 that an even permutation can be expressed as a product of even number of transpositions, and an odd permutation can be expressed as a product of even number of transpositions.

Exercise 85 *Let $\tau = (x\ y)$ be a transposition, and σ be any permutation with finite support. Show that $\sigma \circ \tau$ has parity $\tilde{\sigma} + 1$. In other words, composition with a transposition reverses the parity. (Hint. Consider separately four cases:*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r, \qquad x \in \operatorname{supp} \lambda_1 \text{ and } y \in \operatorname{supp} \lambda_2, \tag{137}$$

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r, \qquad \{x, y\} \subseteq \operatorname{supp} \lambda_1, \tag{138}$$

$$\operatorname{supp} \sigma \cap \{x, y\} = \{x\}, \tag{139}$$

and

$$\operatorname{supp} \sigma \cap \{x, y\} = \emptyset.) \tag{140}$$

6.1.12

It follows from Exercise 85 and remark 6.1.11 that the product of m transpositions has parity m modulo 2.

Exercise 86 *Prove the above statement by induction on m.*

6.1.13 The alternating group A_X

Denote by A_X the set of all permutations

$$A_X := \{\sigma \in \Sigma_X \mid \tilde{\sigma} = 0\} \tag{141}$$

Exercise 87 *Show that A_X coincides with the set of permutations that can be expressed as a product of an even number of transpositions, and that all permutations that can be expressed as a product of an odd number of transpositions form a single coset of A_X in Σ_X. In particular, A_X is a subgroup of index 2 in Σ_X.*

Exercise 88 *Show that A_X is generated by 3-cycles.*

Exercise 89 *Show that*

$$[\Sigma_X, \Sigma_X] = A_X. \tag{142}$$

6.2 Combinatorics of permutations

6.2.1

For any element a of a group G, we shall denote by $\langle\langle a \rangle\rangle_G$, or by $\langle\langle a \rangle\rangle$ — if G is clear from the context, the smallest normal subgroup of G which contains a.

Exercise 90 *Show that $\langle\langle a \rangle\rangle$ coincides with the subgroup generated by the conjugacy class of a*

$$\langle\langle a \rangle\rangle = \langle {}^G a \rangle. \tag{143}$$

6.2.2

It follows from Proposition 6.1 combined with Exercise 78 that

$$\langle\langle \tau \rangle\rangle = \Sigma_X \tag{144}$$

for any transposition τ.

Exercise 91 *Show that*

$$\langle\langle \lambda \rangle\rangle = A_X \tag{145}$$

where λ is any 3-cycle. (Hint. Use Exercise 76.)

6.2.3

Suppose that $\sigma \in \Sigma_X$ is a product of disjoint cycles (133), and λ_1 has an *odd* length. The permutation,

$$\sigma' := \lambda_1 \circ \lambda_2^{-1} \circ \cdots \circ \lambda_r^{-1}$$

has the same cyclic type and thus is conjugate to σ. Note that

$$\sigma \circ \sigma' = \lambda_1^2$$

and since the order of λ_1 is odd, is a cycle of the same length. In view of Exercise 81, the subgroup $\langle\langle \sigma \rangle\rangle$ of Σ_X contains $\langle\langle \lambda \rangle\rangle$ where λ is a cycle of an odd length.

By combining this with Exercise 77, we deduce that

$$\langle\langle \lambda \rangle\rangle \subseteq \langle\langle \sigma \rangle\rangle \tag{146}$$

for some 3-cycle λ and, in view of (145),

$$A_X \subseteq \langle\langle \sigma \rangle\rangle. \tag{147}$$

.

6.2.4

Suppose that the order of $\sigma \in \Sigma_X$ equals $2^e m$ where $m > 1$ is odd. Then, σ^{2^e} having order m, is a product of disjoint cycles of odd length. By previous argument, 6.2.3,

$$A_X \subseteq \langle\langle \sigma^m \rangle\rangle \subseteq \langle\langle \sigma \rangle\rangle.$$

6.2.5

Suppose that the order of $\sigma \in \Sigma_X$ equals 2^e where $e > 0$. Then, $\sigma^{2^{e-1}}$ has order 2.

Exercise 92 *Show that a permutation $\sigma \in \Sigma_X$ of order 2 is a product of disjoint transpositions*

$$\sigma = \tau_1 \circ \cdots \circ \tau_r. \tag{148}$$

6.2.6

If σ is a single transposition then $\langle\langle\tau\rangle\rangle = \Sigma_X$, cf. (144). If σ is a product of at least 2 disjoint transpositions,

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r,$$

where $\tau_1 = (u\ v)$ and $\tau_2 = (w\ x)$, then

$$\sigma' = (u\ w)(v\ x) \circ \tau_3 \circ \cdots \circ \tau_r,$$

has the same cyclic type as σ and is thus conjugate to σ, and $\sigma \circ \sigma'$ is the product of 2 disjoint cycles,

$$\sigma \circ \sigma' = (u\ x)(v\ w).$$

6.2.7

If X has at least 5 elements, u, v, w, x, and y, then the subgroup $\langle\langle(u\ x)(v\ w)\rangle\rangle$ contains the 3-cycle

$$(u\ x)(v\ w) \circ (x\ y)(v\ w) = (u\ x\ y)$$

and hence contains $\langle\langle(u\ x\ y)\rangle\rangle = A_X$.

6.2.8

By combining everything together, we conclude that, for any non-identity permutation $\sigma \in \Sigma_X$, the smallest normal subgroup $\langle\langle\sigma\rangle\rangle$ which contains σ contains A_X – provided X has at least 5 elements. When $|X| = 4$ this is false: The subgroup

$$\langle\langle(u\ x)(v\ w)\rangle\rangle$$

in this case has order 4 and is normal in Σ_X and is strictly contained in A_X.

6.2.9

When σ is even, then $\langle\langle\sigma\rangle\rangle \subseteq A_X$, hence

$$\langle\langle\sigma\rangle\rangle = A_X \tag{149}$$

in this case.

6.2.10

When σ is odd, then $\sigma \notin A_X$, hence $\langle\langle\sigma\rangle\rangle$ is strictly bigger than A_X. Since $\Sigma_X : A_X| = 2$, Langrange's Theorem implies that

$$\langle\langle\sigma\rangle\rangle = \Sigma_X \tag{150}$$

in this case.

Thus we proved the following theorem.

Theorem 6.2 *For any set X of cardinality different from 4, the group of permutations withh finite support, Σ_X, has a unique nontrivial normal subgroup, namely A_X.*

6.2.11

The above theorem implies that no nontrivial normal subgroup H of A_X can be normal in Σ_X. Since $N_{\Sigma_X}(H) = A_X$ and $|\Sigma_X : A_X| = 2$, any such subgroup would have only 2 conjugacy classes in Σ_X,

$$H \qquad \text{and} \qquad {}^{\rho}H$$

where ρ is any odd permutation.

Below we shall demonstrate, however, that A_X has no nontrivial normal subgroups if X has at least 5 elements.

6.2.12

When h is an element of a subgroup H of G, then $\langle\langle h\rangle\rangle_H$ usually differs from $\langle\langle h\rangle\rangle_G$. For example,

$$\langle\langle(1\ 2)\rangle\rangle_{\Sigma_n} = \Sigma_n \qquad (n \geq 2).$$

The two subgroups coincide, however, when ${}^{H}h = {}^{G}h$. This happens often for elements of $H = A_X$ viewed as a subgroup in $G = \Sigma_X$.

Exercise 93 *Show that, for $\sigma \in A_X$,*

$${}^{A_X}\sigma = {}^{\Sigma_X}\sigma \tag{151}$$

if and only if there exists $\rho \in \Sigma_X \setminus A_X$ such that

$$\rho\sigma = \sigma\rho.$$

Exercise 94 *Show that* (151) *holds, for* $\sigma \in A_X$*, if*

$$\operatorname{supp} \sigma \neq X.$$

In particular,

$$\langle\langle \sigma \rangle\rangle_{A_X} = \langle\langle \sigma \rangle\rangle_{\Sigma_X} = A_X \tag{152}$$

in this case.

Exercise 95 *Show that* (151) *holds, for* $\sigma \in A_X$*, if* σ *is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \cdots \circ \lambda_r$$

with at least one cycle having even length. In particular, (152) *holds in this case as well.*

Exercise 96 *Show that* (151) *holds, for* $\sigma \in A_X$*, if* σ *is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r$$

with λ_1 *and* λ_2 *being cycles of the same odd length* l*:*

$$\lambda_1 = (u_1 \ \ldots \ u_l)$$

and

$$\lambda_2 = (v_1 \ \ldots \ v_l)$$

In particular, (152) *holds in this case as well.*

6.2.13

The above exercises demonstrate that the conjugacy classes in A_X and in Σ_X coincide for many even permutations. In particular, the normal subgroups they generate are all equal to A_X. For some even permutations however, ${}^{A_X}\sigma$ is indeed different from ${}^{\Sigma_X}\sigma$, and we need another method to show that $\langle\langle \sigma \rangle\rangle_{A_X} = A_X$ also in this case.

6.2.14

Suppose that $h \in H \subseteq G$, then

$$[a, h] = aha^{-1}h^{-1} \in \langle\langle h \rangle\rangle_H$$

for any a H. In particular,

$$\langle\langle [a, h] \rangle\rangle_H \subseteq \langle\langle h \rangle\rangle_H. \tag{153}$$

Exercise 97 *Calculate*

$$[(1\ 2\ 3), (1\ \ldots\ l)] \qquad (l \geq 2).$$

Use your calculation combined with remark 6.2.14 to show that (152) *holds if* $\sigma \in A_X$ *is a product of disjoint cycles*

$$\sigma = \lambda_1 \circ \lambda_2 \circ \cdots \circ \lambda_r$$

with at least one cycle having length greater or equal 4.

6.2.15

The above sequence of remarks and exercises shows that

$$\langle\langle \sigma \rangle\rangle_{A_X} = \langle\langle \sigma \rangle\rangle_{\Sigma_X} = A_X$$

for any even permutation $\sigma \neq \mathrm{id}_X$ in A_X.

We have proved the following important theorem.

Theorem 6.3 *The alternating group* A_X *has no nontrivial normal subgroups if set* X *has at least 5 elements.*

6.2.16

Note that A_X has non nontrivial normal subgroups also when X has fewer than 4 elements, so Theorem 6.3 excludes only the case $|X| = 4$. In that case A_X contains unique nontrivial normal subgroup, namely its Sylow 2-subgroup

$$\langle\langle \sigma \rangle\rangle_{A_X}$$

where σ is any element of order 2 in A_X.

6.3 Simple groups

6.3.1

Definition 6.4 *A simple group is a group with no nontrivial normal subgroups.*

6.3.2

An abelian simple group A has no nontrivial subgroups since every subgroup in an abelian group is normal. Such a group is cyclic of prime order. Indeed, if $g \in A \setminus 1 = \{a \in A \mid a \neq 1\}$ does not generate A, then $1 \neq \langle g \rangle \neq A$ is a nontrivial subgroup.

6.3.3

The center of a non-abelian simple group G is trivial

$$Z(G) = 1$$

and the commutator subgroup is the whole G

$$[G, G] = G. \tag{154}$$

Definition 6.5 *Groups satisfying* (154) *are called* perfect.

6.3.4

Since the kernel of any homomorphism $f\colon G \longrightarrow G'$ is normal, a nontrivial homomorphism from a simple group into any group is always injective.

6.3.5

Since $Z(P) \neq 1$ and $[P, P \neq P$ for any nonabelian p-group P, a p-group is simple if and only if it is cyclic of order p.

Exercise 98 *Show that any group of order* 42 *has a normal subgroup of order* 7*.*

Exercise 99 *Show that any group of order* 30 *has a normal subgroup of order* 3 *or* 5*.*

Theorem 6.6 *If a simple group G acts nontrivially on a set X of cardinality l, then $|G| \leq l!$.*

Proof. If G acts nontrivially on X, then there exists at least one element $x \in X$ which is not fixed by G. In this case, the G-action of G on the orbit, $\mathscr{O} = Gx$, of x defines a nontrivial homomorphism

$$G \longrightarrow \Sigma_{\mathscr{O}}.$$

By remark 6.3.4 this embeds G into the permutation group, $\Sigma_{\mathscr{O}}$. Thus, $|G| \leq |\Sigma_{\mathscr{O}}| = l!$. □

Corollary 6.7 *A simple group G of order less than $l!$ has no subgroup of index less or equal l.*

Proof. For any subgroup H of G the latter acts transitively on the set of left cosets G/H, cf. Exercise 38. If $H \neq G$, then G acts nontrivially on $X = G/H$ and the latter has cardinality $l = |G : H|$. □

6.3.6 Example: no group of order 24 is simple.

Sylow subgroups of a group G of order 24 have orders 8 and 3. The index in G of any Sylow 2-group is 3 and $3! = 6 < 24 = |G|$. By Corollary 6.7, G cannot be simple.

Exercise 100 *Show that no group of order 36 is simple.*

Theorem 6.8 *A simple group of order 60 has 5 Sylow 2-subgroups, and is canonically isomorphic to $A_{\mathrm{Syl}_2 G}$. In particular, there is only one simple group of order 60 up to an isomorphism.*

Proof. By the Third Sylow Theorem, the number $s_5(G) = |\mathrm{Syl}_5 G|$ divides $60/5 = 12$ and is congruent to 1 modulo 5. This leaves only two possibilities:

$$s_5(G) = 6 \quad \text{or} \quad 1.$$

In the case $s_5(G) = 1$, group G would have a normal subgroup of order 5, contradicting the simplicity hypothesis. Thus, $s_5(G) = 6$, and there are exactly $6 \cdot (5 - 1) = 24$ elements of order 5.

By the aforementioned Third Sylow Theorem, the number of Sylow 3-subgroups, $s_3(G)$, divides $60/3 = 20$ and is congruent to 1 modulo 3. This leaves only two possibilities:

$$s_3(G) = 10 \quad \text{or} \quad 1.$$

Again, $s_3(G) = 1$ would contradict the simplicity hypothesis. Thus, $s_3(G) = 10$, and there are exactly $10 \cdot (3-1) = 20$ elements of order 5.

All the elements of all the Sylow 2-subgroups are contained in the set

$$\{g \in G \mid g^3 \neq 1 \text{ and } g^5 \neq 1\}$$

which has $60 - (24 + 20 + 1) = 15$ elements.

The number off Sylow 2-subgroups, $s_2(G)$, divides $60/4 = 15$. If $s_2(G) = 3$, then G would act nontrivially on a set of cardinality 3, and $3! = 6 < 60 = |G|$. In view of Theorem 6.6 that is impossible.

If $s_2(G) = 15$, then at least two Sylow 2-subgroups, P and Q, must have a nontrivial element:

$$a \in P \cap Q.$$

Consider the centralizer, $C_G(a)$. Its order is divisible by $|P| = 4$ and greater or equal $|P \cup Q| = 6$. At the same time, is a divisor of $|G| = 60$. This leaves three possibilities:

$$12 = 3 \cdot 4, \qquad 20 = 5 \cdot 4, \qquad \text{or} \qquad 60 = 15 \cdot 4.$$

In the last case a would belong to the center of G and the center is trivial since G is obviously nonabelian.

In the second case, the index of $C_G(a)$ in G would be 3 and we know that G has no subgroups of order l such that $l! < |G|$.

The only possibility left is thus $|C_G(a)| = 5$.

The action of G on the set of left cosets, $X = G/C_G(a)$, then identifies G with a subgroup of index 2 in Σ_X, and there is only one such subgroup: A_X.

We proved that G is isomorphic to A_5. But this contradicts our assumption that $s_2(G) = 15$ since $s_2(A_5) = 5!$.

This proves that $s_2(G) = 5$ after all, and the transitive action of G on $\mathrm{Syl}_5(G)$ defines a canonical embedding of G onto $A_{\mathrm{Syl}_5(G)}$. □

6.3.7

It follows from Exercises 74, 98, 99, and 100, in combination with Section 6.3.6, that no nonabelian group of order less than 60 is simple. Thus, the alternating group on a 5-element set is the smallest nonabelian simple group.

6.3.8

The next nonabelian simple group has order 168. It is isomorphic to the group

$$\operatorname{Aut} C_3^2 = \mathrm{GL}_3(\mathbb{F}_2)$$

which is the group of collineations of the Fano plane: the smallest projective plane which has 7 points and 7 lines.

6.4 Linear groups

6.4.1 General linear group

Let F be a field. The group of automorphisms of the n-dimensional vector space F^n is identified with the group, $\mathrm{GL}_n(F)$, of invertible $n \times n$-matrices with entries in F: just associate to an automorphism its matrix in the standard basis of F^n. Group $\mathrm{GL}_n(F)$ is called the *general linear group* of F (of rank n).

6.4.2 General projective group

The center, $Z(\mathrm{GL}_n(F))$, consists of diagonal matrices

$$\begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \qquad (\lambda \in F^*) \tag{155}$$

where F^* denotes the multiplicative group of F. Note that $F^* = \mathrm{GL}_1(F)$.

The quotient by the center, $\mathrm{GL}_n(F)/Z(\mathrm{GL}_n(F))$, is called the *general projective group*. It is a subgroup of the group of all collineations of a projective $n-1$-dimensional space which is *coordinatized* by field F.

6.4.3 Special linear group

The general linear group is equipped with the canonical homomorphism

$$\det\colon \mathrm{GL}_n(F) \longrightarrow F^* \tag{156}$$

which is called the *determinant*. Its definition and properties are the subject of an introductory Linear Algebra course.

The kernel of (156) is denoted $\mathrm{SL}_n(F)$ and called the *special linear group*.

6.4.4 Special projective groups

The center of $\mathrm{SL}_n(F)$ consists of diagonal matrices (155) with λ being the roots of 1 of degree n. This group is always finite. In fact, it has no more than n elements since all such roots are zeros of the polynomial

$$X^n - 1$$

and any polynomial of degree n has at most n distinct roots.

The quotient by the center, $\mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$, is called the *special projective group*.

6.4.5

Note that over a 2-element field $\mathbb{F}_2$, one has

$$\mathrm{GL}_n(F_2) = \mathrm{GL}_n(F_2) = \mathrm{SL}_n(\mathbb{F}_2) = \mathrm{PSL}_n(\mathbb{F}_2).$$

Theorem 6.9 *With the exception of* $\mathrm{PSL}_2(\mathbb{F}_2)$ *and* $\mathrm{PSL}_2(\mathbb{F}_3)$*, which have orders 6 and 12, respectively, the special linear group of rank* $n > 1$ *of any field* F*, is simple.* □

7 Classification of groups of small order

7.1 Groups of order 12

7.1.1

Sylow subgroups of a group G of order $12 = 2^2 \cdot 3$ have orders 4 and 3. Sylow 2-subgroups are either cyclic, C_4, or elementary abelian, $C_2^2 = C_2 \times C_2$.

7.1.2 Case I: G has a normal subgroup of order 3

In this case, G is a semidirect product of C_3 and its Sylow 2-subgroup P_2.

If $P_2 \lhd G$, then G is abelian and either is cyclic,

$$G \simeq C_3 \times C_4 \simeq C_{12},$$

or is isomorphic to the product of two cyclic groups,

$$G \simeq C_3 \times C_2 \times C_2 \simeq C_6 \times C_2.$$

Otherwise, the adjoint action of P_2 on $P_3 = C_3$ defines a nontrivial homomorphism

$$P_2 \longrightarrow \operatorname{Aut} C_3 = \{\pm 1\}. \tag{157}$$

7.1.3 Subcase: P_2 is elementary abelian

There is only one such homomorphism when $P_2 = C_4$. In this case,

$$G \simeq C_3 \rtimes C_4 = \langle a, b \mid a^4 = b^3 = aba^{-1}b = 1 \rangle \tag{158}$$

What you see on the righ-hand side of (158) is the often used in Group Theory notation giving a so called *presentation* of the group in terms of some set of generators (here, $\{a, b\}$), and defining relations (three in our case, $a^4 = 1$, $b^3 = 1$, and $aba^{-1} = b^{-1}$).

7.1.4 Subcase: P_2 is elementary abelian

When $P_2 = C_2^2$, there are three nontrivial homomorphisms (157): if $\{u, v, w\}$ denotes the set of elements of order 2 in C_2^2, then one element is sent to 1 and the remaining two are sent to -1. In either case,

$$G \simeq (C_3 \rtimes C_2) \times C_2 = \Sigma_3 \times C_2$$

where the factor C_2 is the subgroup of C_2^2 generated by the element of $\{u, v, w\}$ which acts trivially on C_3.

7.1.5 Case II: P_3 is not normal

In this case there are 4 cyclic subgroups of order 3, and 8 elements of order 3. This leaves room for only 3 elements $g \in G$ such that $g^3 \neq 1$. Since $P \setminus 1$, for any Sylow 2-subgroup has exactly 3 such elements, we conclude that there is only one Sylow 2-subgroup in G. In other words, $P_2 \lhd G$, and therefore

$$G = P_2 \rtimes C_3.$$

The adjoint action of C_3 on P_2 defines a nontrivial homomorphism

$$C_3 \longrightarrow \operatorname{Aut} P_2. \tag{159}$$

Since $\operatorname{Aut} C_4 = \{\pm 1\}$, there is no such homomorphism if P_2 is cyclic.

On the other hand, there are two such homomorphisms if P_2 is elementary abelian C_2^2, since $\operatorname{Aut} C_2^2 = \Sigma_X$ where X is the set of elements of order 2 in C_2^2. The corresponding semidirect products

$$C_2^2 \rtimes C_3$$

are isomorphic: this follows from Exercise 70. Thus, there is only one group, up to isomorphism, of order 12 without a normal subgroup of order 3.

Note that the action of G on the set, $\operatorname{Syl}_3 G$, of Sylow 3-subgroups defines a homomorphism

$$G \longrightarrow \Sigma_{\operatorname{Syl}_3 G}. \tag{160}$$

Let K denote its kernel and $\bar{G} \simeq G/K$ denote its image. Since $\bar{G}$ acts transitively on $\operatorname{Syl}_3 G$, number $4 = |\operatorname{Syl}_3 G|$ divides $|\bar{G}|$ and the latter divides $12 = |G|$. This leaves only two possibilities for $|\bar{G}|$: either 4 or 12. In the former case, K would be a normal subgroup of order $12/4 = 3$, and that would contrardict the fact that G has no such subgroup. Thus, $|\bar{G}| = 12$ and $K = 1$. In other words, homomorphism (160) identifies G with a subgroup of $\Sigma_{\operatorname{Syl}_3 G}$ of index 2.

The permutation group, Σ_X, of a finite set X has only one subgroup of index 2, namely the alternating group A_X. Thus we proved that

$$\begin{array}{l}\text{a group of order 12 with no normal subgroup} \\ \text{of order 3 is canonically isomorphic to } A_{\operatorname{Syl}_3 G}.\end{array} \tag{161}$$

7.1.6

To sum up, there are exactly 5 groups of order 12 up to isomorphism, two of them are abelian, the rest are nonabelian:

$$C_3 \rtimes C_4, \qquad \Sigma_3 \times C_2 \qquad \text{and} \qquad A_4. \tag{162}$$

Exercise 101 *Show that* $\mathrm{PSL}_2(\mathbb{F}_3)$ *is isomorphic to the alternating group,* A_4*. Provide two different proofs: one, group-theoretic, by finding a normal subgroup in* $\mathrm{PSL}_2(\mathbb{F}_3)$ *of order 4, or by finding at least two different subgroups of order 3, and then using Case II of the above classification of groups of order 12; another one, using methods of elementary Linear Algebra, by proving that* $\mathrm{PSL}_2(\mathbb{F}_3)$ *acts faithfully on the set of lines in the 2-dimensional vector space* $\mathbb{F}_3^2$ *which pass through the origin.*