The Elements of Group Theory

Edward Chernysh

E-mail address: edward.chernysh@mail.mcgill.ca
URL: http://cs.mcgill.ca/~echern2/

Last Updated: March 2, 2018.

Contents

Note: Chapters and sections labeled with $*$ may be omitted on a first reading.

Preface

This text is intended as a primary reference for a first course (at the honours level) in group theory. Although technically a first course, we do will assume that the reader possesses some level of mathematical maturity. To be more precise, although we study gruops from first principles, we will not dwell on the introduction of university level mathematics and we will assume that the reader is already familiar with abstract mathematics and has written proofs in the past. Furthermore, some results presented in this text (albeit very few) will call upon algebraic results from other areas of mathematical (say, field theory).

We will begin with a chapter involving the abstract theory of groups. The results established in this chapter will hold for all groups, or for every finite group. This includes Lagrange's theorem and a discussion of cyclic groups. This will allow us to give a short and elegant proof of the primitive root theorem, which states that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for every prime p. We will then explore normal subgroups and homomorphisms of groups. The chapter will conclude with the isomorphism and correspondence theorems for finite groups which will underpin much of the theory in the chapters that follow.

In the second chapter, we focus on the actions of groups upon finite sets; which has a great deal of applications in combinatorics and in number theory. We will establish the standard orbit-stabilizer theorem and the Burnside formula, the two of which are extremely useful in practice and will be the cornerstone of the Sylow and Jordan-Hölder theorems. We present Cayley's isomorphism theorem in a concise manner.

In the chapter that follows, we explore two perspectives of finite groups: the Sylow and Jordan-Hölder philosophies. First, we establish the Sylow theorems which relate to groups and subgroups whose order is a power of a prime. We also give applications of the Sylow theorem to certain categories of finite groups (say, groups of order pq). In the final

half of the chapter, we explore the Jordan-Hölder philosophy and introduce the concept of a semidirect product.

The final chapter of this text is dedicated to the absolute basics of representation theory of finite groups. This chapter assumes a familiarity with finite dimensional linear algebra and offers an alternative perspective on the structure of finite groups. Unfortunately, this last chapter requires a background in linear algebra. More precisely, the reader should be familiar with linear transformations, changes of bases, inner product spaces and the spectral theorem.

Abstract Groups and Properties

In this chapter we are interested in the abstract notion of a group, and we will mostly focus on concepts and results that are applicable to all groups (or all *finite* groups). Group theory has become a prominent and fundamental part of modern abstract algebra and is regarded by many to be profound and beautiful. Although I do not entirely share this view (I greatly prefer analysis), it is impossible to argue against the importance of group theory in a graduate education in mathematics.

1. Groups and Subgroups

Throughout this document, unless otherwise specified, we shall write G to denote a non-empty set and $\odot$ denotes an operation on G:

$$\odot : G \times G \longrightarrow G.$$

DEFINITION 1. A pair $(G, \odot)$ is called a group if

(1) G is associative under $\odot$, i.e. if $a \odot (b \odot c) = (a \odot b) \odot c$ for all $a, b, c \in G$
(2) There exists an element $e \in G$ such that $g \odot e = e \odot g = g$ for all $g \in G$. This is called the identity element of the group.
(3) For each $g \in G$ there exists $g^{-1} \in G$ such that

$$g \odot g^{-1} = g^{-1} \odot g = e.$$

We will often omit the notation '$\odot$' and simply write gh to mean $g \odot h$ for $g, h \in G$. Note that by our definition of $\odot$ it follows that $gh \in G$ whenever $g, h \in G$. Moreover, we shall write G to mean a group $(G, \odot)$ to simplify notation.

EXAMPLE 1. The set of real numbers $\mathbb{R}$ is a group when endowed with the usual notion of addition as the group operation. In fact, if $\mathcal{R}$ is a ring then the pair $(\mathcal{R}, +)$ is a group.

EXAMPLE 2. The set $\mathbb{C}^\times := \{z \in \mathbb{C} : z \neq 0\}$ is a group under multiplication.

EXAMPLE 3. Let $p \in \mathbb{N}$ be a prime; the set $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group under multiplication.

We would first like to establish some consequences of the group axioms. First, this identity element is unique. Indeed, assume that e' satisfies condition (2) of our group definition. Then,

$$e = ef = fe = f.$$

In a similar vein, the inverse to any element is unique. To see that this is true, fix $g \in G$ and assume $gh = hg = e$. Then,

$$g^{-1} = g^{-1}e = g^{-1}(gh) = \left(g^{-1}g\right)h = eh = h.$$

A group G is called **Abelian** if it is commutative, i.e. $gh = hg$ for all $g, h \in G$. We shall say that G has finite order if $\#G < \infty$.

DEFINITION 2. If G is a group, a set $H \subseteq G$ is called a subgroup of G whenever

(1) $e \in H$.
(2) Given $g, h \in H$ we have $gh \in H$.
(3) For each $g \in H$ the inverse $g^{-1} \in H$.

From these axioms it is easy to verify that H is a group in its own right. The sets $\{e\}$ and G are called the trivial subgroups of G; indeed they are always subgroups. We shall write $H < G$ as shorthand to say that H is a subgroup of G. A subgroup H is called **cyclic** provided there exists an element $g \in H$ such that

$$\langle g \rangle := \{g^m : m \in \mathbb{Z}\} = H.$$

In this case, we say that H is generated by g and that g is a generator of H. For any element $g \in H$ we then define the *order of* h, denoted $\mathrm{ord}(g)$, to be the minimal positive integer k such that $g^k = e$. If no such element exists, we put $\mathrm{ord}(g) = \infty$. It is also easy to check that $\langle x \rangle$ is a subgroup of G, for each $x \in G$. This is called the cyclic group generated by x in G.

PROPOSITION 1.1. *Let G be a group and $g \in G$. Then* $\mathrm{ord}(g) = \#\langle g \rangle$.

PROOF. Suppose that $\mathrm{ord}(g) = \infty$, then for any positive integers n and m we have $g^n \neq g^m$. Otherwise, assume without loss of generality that $m < n$ and note that g^m has inverse g^{-m} it follows that $g^{n-m} = e$ which contradicts $\mathrm{ord}(g) = \infty$. Thus, the set $\langle g \rangle$ contains infinitely many distinct elements which must then give $\#\langle g \rangle = \infty$.

Suppose now that $\mathrm{ord}(g) = k < \infty$. Then, clearly,

$$\langle g \rangle = \left\{e, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\right\}$$

where all these elements must be distinct by the minimality of $\mathrm{ord}(g)$. This concludes the proof. □

LEMMA 1.2. *Let G be a group and $\{H_\alpha\}_{\alpha\in I}$ and indexed family of subgroups of G.*[1] *Then $\bigcap_{\alpha\in I} H_\alpha$ is a subgroup of G.*

PROOF. Since $e \in H_\alpha$ for all indices $\alpha \in I$ we have $e \in \bigcap_{\alpha\in I} H_\alpha$. Similarly, for each $g \in \bigcap_{\alpha\in I} H_\alpha$ we have $g \in H_\alpha$ for all α whence $g^{-1} \in H_\alpha$ for each $\alpha \in I$ which gives us $g^{-1} \in \bigcap_{\alpha\in I} H_\alpha$. A verbatim argument shows that $\bigcap_{\alpha\in I} H_\alpha$ is closed under the group operation of G. □

DEFINITION 3. Denote by G a group and let $\{g_\alpha\}_{\alpha\in I}$ a family of elements in G. The minimal subgroup generated by this family, which we denote $\langle\{g_\alpha\}_{\alpha\in I}\rangle$, is the group

$$\bigcap_{G>H\supseteq\{g_\alpha\}_{\alpha\in I}} H_\alpha.$$

2. Cosets and Lagrange's Theorem

We once again fix a group G and let H be a subgroup of G. A (left)-coset of H in G is merely a set of the form

$$gH = \{gh : h \in H\} \subseteq G,$$

and a right coset is defined in the analogous way. Note that a coset of H in G depends on the choice of $g \in G$. Unless stated otherwise, we will only speak of left cosets of H in G, although much of the theory could still be developed using right cosets. Given a group G and a subgroup H of G, we shall denote by G/H the collection of all left cosets of H in G, i.e.

$$G/H := \{gH : g \in G\}.$$

As we shall soon see, this choice of notation is very convenient.

LEMMA 1.3. *Let G be a group and H a subgroup of G. If $x, y \in G$ we say $x \sim y$ if $x \in yH$. Then $\sim$ defines an equivalence relation on G where the equivalence class of x, denoted $[x]$, is simply xH.*

PROOF. Since H contains the identity e, it is obvious that $x = xe \in xH$. Thus, $x \sim x$. If $x \sim y$ then $x \in yH$ so that $x = yh$ for some $h \in H$. This means that $xh^{-1} = y$ whence it follows that $y \in xH$, i.e. $y \sim x$. If $x \sim y$ and $y \sim z$ we have both $x \in yH$ and $y \in zH$. Choose now h_1 and h_2 in H such that $x = yh_1$ and $y = zh_2$. Then

$$x = yh_1 = zh_2h_1 = zh' \in zH.$$

Hence, $x \sim z$ which verifies that $\sim$ is an equivalence relation. Given $x \in G$ we have that

$$[x] = \{y \in G : y \sim x\} = \{y \in G : y \in xH\} = xH.$$

[1] Each H_α is a subgroup of G. Note that I need not be countable here!

□

Therefore, one can view G/H, the collection of left cosets, as $G/\sim$ where $\sim$ is the equivalence relation defined above in the lemma. A very powerful (but elementary!) result is Lagrange's theorem which both justifies the choice of notation for G/H and gives an essential tool in the study of finite groups. If G is a finite group and H is a subgroup of G, the *index of H in G* is defined to be

$$[G : H] := |G/H|$$

where $|\cdot|$ gives the cardinality of a set.

REMARK 1.1. In the case of infinite groups, one can still make sense of the index of a subgroup in terms of cardinal numbers.

THEOREM 1.4 (Lagrange). *Let G be a finite group and H a subgroup of G. Then,*

$$[G : H] = \frac{|G|}{|H|}.$$

In particular, the order of a subgroup divides the order of the group.

PROOF. Let $x, y \in G$ be given and consider the cosets xH and yH. We first show there exists a bijection between the two. Indeed, we first define a map

$$f : xH \longrightarrow yH$$

by letting $xh \mapsto yh$. To see that this is a surjection we need only note that every element $b \in yH$ is of the form yh for some $h \in H$. Then $f(xh) = yh = b$. To see that f is injective, note that $yh_1 = yh_2$ if and only if $h_1 = h_2$.

This argument now shows that any two cosets of H in G have the same number of elements. Since cosets are equivalence classes, we choose a finite family of representatives $x_1, \ldots, x_N$ in G for these cosets. Since G is then the disjoint union of equivalence classes (in our case, cosets) it follows that

$$|G| = \left| \bigsqcup_{j=1}^{N} x_j H_j \right| = \sum_{j=1}^{N} |x_j H| = \sum_{j=1}^{N} |eH| = N \cdot |H| .$$

Since $N = [G : H]$ this concludes the proof. □

REMARK 1.2. We would like to point out a choice of notation that will be frequently glossed over throughout this book. We use the notation $\bigcup$ to mean the union of sets, and the symbol $\bigsqcup$ to mean a disjoint union of sets, i.e. the indexed family consists of pairwise disjoint sets.

We now point out some immediate consequences of Lagrange's theorem.

COROLLARY 1.5. *If G is a finite group and $g \in G$, then* $\operatorname{ord}(g) \mid |G|$.

PROOF. Indeed, $\langle g \rangle$ is a subgroup of G that has order $\operatorname{ord}(g)$. □

COROLLARY 1.6. *Let G be a finite group of order p for some prime p. Then G is cyclic.*

PROOF. Let $g \in G$ be non-trivial, i.e. $g \neq e$. Then $\langle g \rangle$ is a subgroup of G, containing more than one element, whose order divides p. Since $1 < \text{ord}(g) \mid p$, it follows that $\text{ord}(g) = p$. Thus, $\langle g \rangle = G$. □

Cyclic groups are of great interest to many and possess many interesting properties. We will continue to explore such groups in the subsequent section.

3. Cyclic Groups

We recall that a group G is called cyclic provided there exists $g \in G$ such that $G = \langle g \rangle$. Note also that G need not be finite for this to hold. Indeed, $\mathbb{Z}$ is a group under addition that is generated by the element 1. However, we shall assume for the remainder of this section that G is a finite cyclic group of order $n \in \mathbb{N}$ and that g is a generator of G, i.e. that

$$G = \langle g \rangle.$$

LEMMA 1.7. *Let $1 \leq a \leq n$ be a positive integer, then*

$$\text{ord}(g^a) = \frac{n}{\gcd(a, n)}.$$

PROOF. We note that if $g^{ar} = e$ then $n \mid ar$. Indeed, suppose that $g^{ar} = e$ but that $n \nmid ar$. By the Euclidean division algorithm, there exists $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{N}$ with

$$ar = \alpha n + \beta, \quad 0 < \beta < n.$$

In this case, $e = g^{ar} = g^{\alpha n} \cdot g^{\beta} = g^{\beta}$ which contradicts the fact that $n = \text{ord}(g)$ (recall that n must be the least positive integer k such that $g^k = e$). Therefore, $g^{ar} = e$ if and only if $n \mid ar$. In particular, $\text{ord}(g^a)$ is the smallest integer r for which $n \mid ar$. Note that

$$\frac{n}{\gcd(a, n)}.$$

is certainly a valid candidate for r. Furthermore, if $n \mid ar$ then

$$n = \gcd(a, n) \cdot \frac{n}{\gcd(a, n)} \mid ar$$

which implies that

$$\frac{n}{\gcd(a, n)} \mid r.$$

□

COROLLARY 1.8. *The element g^a generates G if and only if $\gcd(a, n) = 1$. Hence, G has precisely $\varphi(n)$ generators, where $\varphi(n)$ is Euler's totient function.*

A special result concerning cyclic group is the following, which characterizes all the subgroups of cyclic groups.

PROPOSITION 1.9. *Let G be a cyclic group of order n. Then for each $d \mid n$ there exists a unique cyclic subgroup of order d in G.*

PROOF. As a first step we shall show that every subgroup of G is cyclic. Indeed, let H be a subgroup of order d in G and let g be a generator of G. If $H = \{e\}$ we are done. Otherwise, let $a \in \mathbb{N}$ be the minimal integer such that $g^a \in H$. We claim $H = \langle g^a \rangle$. The inclusion $\supseteq$ is trivial. For the reverse inclusion, let $h \in H$ and write $h = g^b$ for $b \in \mathbb{N}$. Suppose $a \nmid b$ so that

$$b = ak + c, \quad 0 \leq c < a.$$

Since a is minimal, we must have $c = 0$ which proves that H is cyclic. If $d \mid n$, one can write $n = td$ for $t \in \mathbb{N}$. Then the element g^t has order

$$\operatorname{ord}(g^t) = \frac{n}{\gcd(t, n)} = d$$

so that $H = \langle g^t \rangle$ is a subgroup of order d. It remains only to show that this subgroup is unique. Indeed, we define

$$K := \left\{ x \in G : x^d = e \right\}$$

and note that K is a subgroup of G containing H. Every element of K has order no greater than d, and since K is cyclic (by the first part), it follows that K contains no more than d elements by Lagrange's theorem. Thus, $K = H$ which proves that H is unique since K has no dependency on H. More precisely, K will contain any subgroup of order d. □

3.1. Applications to Finite Field Theory. We first give a property related to the Euler totient function.

LEMMA 1.10. *Let $n \in \mathbb{N}$, then*

$$n = \sum_{d \mid n} \varphi(d).$$

PROOF. Let us fix a cyclic group G of order n; such a group always exists as one can take $\mathbb{Z}/n\mathbb{Z}$ under addition. If $x \in G$ then $\operatorname{ord}(x)$ divides n. More generally, if $d \mid n$ then every element of order d belongs to a single cyclic subgroup of G. Thus, there will be exactly $\varphi(d)$ such elements. Since every element has order dividing n it follows that

$$n = \sum_{d \mid n} |\{x \in G : \operatorname{ord}(x) = d\}| = \sum_{d \mid n} \varphi(d)$$

as was asserted. □

Proposition 1.9 has a converse, which we present below. This is a useful criterion for a group being cyclic.

PROPOSITION 1.11. *Let G be a finite group of order n such that for each divisor d of n there exists at most a single subgroup of order d. Then G is cyclic.*

PROOF. If $h \in G$ is an element of order $d \mid n$ there exists a subgroup of G with order d. This subgroup will be cyclic and will contain all elements of order d. Hence, G will have $\varphi(d)$ elements of order d. All of this together gives the relation

$$n = \sum_{d|n} \varphi(d)\varepsilon_d$$

where $\varepsilon_d = 0$ if no elements of order d exist and 1 if such an element exists. However, our previous lemma gives

$$n = \sum_{d|n} \varphi(d)\varepsilon_d = \sum_{d|n} \varphi(d)$$

which shows that $\varepsilon_n = 1$, i.e. that G is cyclic. □

We are now capable of proving the subsequent generalization of the primitive root theorem, which is of importance in number theory.

COROLLARY 1.12. *Let $\mathbb{F}$ be a finite field and denote by $\mathbb{F}^\times$ the group of units in $\mathbb{F}$ under multiplication. Then $\mathbb{F}^\times$ is cyclic.*

PROOF. Let n denote the order of $\mathbb{F}^\times$ and fix a divisor d of n; it suffices to check that $\mathbb{F}^\times$ has at most a single subgroup of order d. Certainly, let

$$D := \left\{ x \in \mathbb{F}^\times : x^d = 1 \right\}$$

and recall that D can contain at most d-elements. Now, if $\mathbb{F}^\times$ has a subgroup of order d, this subgroup will be contained in D (by Lagrange's theorem). Hence, D is the unique subgroup of order d if one exists. □

4. Normal and Quotient Groups

We now briefly return to the case of a general group, which is not necessarily finite. Let H be a subgroup of G, the centralizer of H is denoted $\mathrm{C}(H)$ and is defined by

$$\mathrm{C}(G) := \{g \in G : gh = hg, \forall h \in H\}. \tag{1.1}$$

It is left to the reader as an exercise to very that $\mathrm{C}(H)$ is a subgroup of G. Similarly, the center of G is defined by

$$Z(G) := \{g \in G : gh = hg, \forall h \in G\}. \tag{1.2}$$

Once again, one can easily verify that $Z(G)$ is a subgroup of G and that $Z(G)$ is **Abelian**. Finally, the normalizer of $H < G$ is defined by

$$N_G(H) := \{g \in G : gH = Hg\}. \tag{1.3}$$

It is left as a simple exercise to check that $N_G(H)$ is a subgroup of G.

DEFINITION 4. A subgroup N of a group G is called *normal in G* whenever one has $gN = Ng$ for all $g \in G$. We shall write $N \lhd G$ to say that N is normal in G

DEFINITION 5. A group G is called simple if the only normal subgroups of G are $\{e\}$ and G itself.

This is an abstract definition and of which the motivation is likely unclear. Before we explore applications, let us give a practical characterization of this result which first relies upon an easy lemma.

LEMMA 1.13. *Let G be a group and H a subgroup of G. If $g \in G$, then $gH = H$ if and only if $g \in H$.*

PROOF. If $gH = H$ then obviously $g \cdot e \in gH \in H$ so that $g \in H$. Conversely, if $g \in H$ then $gH \subseteq H$ by closure under the group operation. Choose now $h \in H$ and write $h = gg^{-1}h = g \cdot h'$ where $h' = g^{-1}h \in H$. This shows that $H \subseteq gH$ which establishes their equality. □

We may now easily characterize the normal subgroups of G.

PROPOSITION 1.14. *Let G be a group and N a subgroup of G. The following statements are equivalent:*

(1) $N \lhd G$,
(2) $gN \subseteq Ng$ *for all* $g \in G$,
(3) $gng^{-1} \in N$ *for all* $g \in G$ *and* $n \in N$.

PROOF. Suppose $N \lhd G$, then $gN = Ng$ so that $gN \subseteq Ng$, for all $g \in G$. If we instead assume that (2) holds true and let $n \in N$ we obtain that $gn \in gN \subseteq Ng$ so that $gn = n'g$. Hence, $gng^{-1} = n' \in N$ which establishes (3). Supposing that (3) holds, it is immediate that $gN \subseteq Ng$ for each $g \in G$. For the reverse inclusion, let $ng \in Ng$ be given where $n \in N$ and $g \in G$. Then

$$ng = g\underbrace{g^{-1}ng}_{\in N} = gn' \in gN.$$

□

A quick example is certainly in order. Let H be a subgroup of G and consider its normalizer: $N_G(H)$ which is a subgroup of G which contains H (why?). We claim that H is normal in $N_G(H)$. Certainly, if $n \in N_G(H)$ then

$$nH = hN$$

by construction.

4.1. Construction of Quotient Groups. We now fix an arbitrary non-trivial group G, i.e. $G \supsetneq \{e\}$. Assume that N is a normal subgroup G and consider the collection of left cosets of N in G:

$$G/N := \{gN : g \in G\}.$$

The "normality" of N in G will allow us to give a group structure to G/N. By Lagrange's theorem, we already know that $|G/N| = |G| / |N|$, hence the term *quotient group*. Let now $x, y \in G/H$, they can be represented as

$$x = aN, \quad y = bN$$

for $a, b \in G$. We define $xy = (aN) \cdot (bN) := (ab)N$. Our first task is to check that this well defined, i.e. if

$$x = a_1 N = a_2 N, \quad a_{1,2} \in G$$

and

$$y = b_1 N = b_2 N, \quad b_{1,2} \in G$$

then $(a_1 b_1)N = (a_2 b_2)N$. To see that this is so, note that we can write $a_2 = a_1 n_a$ and $b_2 = b_1 n_b$, for $n_a, n_b \in N$. It then follows that

$$(a_2 b_2)N = (a_1 n_1 b_1 n_b)N = (a_1 b_1 \underbrace{b_1^{-1} n_b b_1}_{\in N} n_b)N = (a_1 b_1 n')N = (a_1 b_1)N.$$

This shows that our group operation is well defined and independent of representative. Clearly, the identity element is then $N = eN$ and the inverse of $x = aN$ is $a^{-1}N$. Furthermore, if G is Abelian then so is G/N.

DEFINITION 6. A group G is called simple if the only normal subgroups in G are $\{e\}$ and G itself.

Simple groups will play an important role in the future, although we shall not yet worry too much about these groups.

LEMMA 1.15. *Let G be a group and B, N subgroups of G with $N \lhd G$. Then,*

(1) *$B \cap N$ is normal in B;*

(2) *$BN = \{bn : b \in B, n \in B\}$ is a subgroup of G. Also, NB is a subgroup of G such that $BN = NB$.*

(3) *If $B \lhd G$ then $BN \lhd G$ and $B \cap N \lhd G$.*

(4) *If both B and N are finite then*

$$|BN| = \frac{|B| \cdot |N|}{|B \cap N|}. \tag{1.4}$$

PROOF. We first check (1). Let $n \in B \cap N$ and $b \in B$, then bnb^{-1} lives in B by closure under the group operation and $bnb^{-1} \in N$ since N is normal in G. Thus, $B \cap N \lhd B$. Let $b_1 n_1$ and $b_2 n_2$ be elements of BN and note that

$$(b_1 n_1)(b_2 n_2) = b_1 n_1 b_2 n_2 = b_1 b_2 \underbrace{b_2^{-1} n_1 b_2}_{\in N} n_2 = b_1 b_2 n' \cdot n_2 \in BN.$$

Clearly, $e = e \cdot e \in BN$ and

$$(bn)^{-1} = n^{-1}b^{-1} = b^{-1}\underbrace{bn^1b^{-1}}_{\in N} \in BN.$$

Furthermore, since N is normal in G it must also be normal in B. Thus,

$$BN = \bigcup_{b\in B} bN = \bigcup_{b\in B} Nb = NB.$$

Thus, (2) holds true. Let $g \in G$ and $x = bn \in BN$. Then

$$gxg^{-1} = gbng^{-1} = \left(gbg^{-1}\right) \cdot \left(gng^{-1}\right)$$

where $gbg^{-1} \in B$ and $gng^{-1} \in N$. Thus, $BN \lhd G$. Let now $x \in B \cap N$ and $g \in G$; it is not hard to see that

$$gxg^{-1} \in B \quad \text{and} \quad gxg^{-1} \in N$$

since B and N are both normal in G. This establishes the third point. For the final point, we consider the map

$$f : B \times N \longrightarrow BN, \quad (b, n) \mapsto bn.$$

It suffices to check that for each $x = bn \in BN$ there exist exactly $|B \cap N|$ pairs (b, n) mapping to x under the action of f. Obviously, f is surjective and "reaches" all elements of BN. Suppose now that

$$b_1n_1 = b_2n_2$$

for $b_{1,2} \in B$ and $n_{1,2} \in N$. Then, $b_2 = b_1n_1n_2^{-1}$ and $n_2 = b_2^{-1}b_1n_1$. Let us now define $x = n_1n_2^{-1}$ which belongs to $B \cap N$. Note also that $x^{-1} = b_2^{-1}b_1$. Thus,

$$(b_2, n_2) = (b_1x, x^{-1}n_1)$$

for some $x \in B \cap N$. Clearly, for each $x \in B \cap N$ we have $(b_1x, x^{-1}n_1) \mapsto b_1n_1$, as was required. □

5. Homomorphisms of Groups

In this section we study mappings between groups that preserve the structure of the domain. Let G and H be groups, we say a map $f : G \longrightarrow H$ is a homomorphism of groups (or simply a homomorphism) provided

$$f(gh) = f(g)f(h), \quad \forall (g, h) \in G \times G.$$

This property has several useful consequences. First, note that $f(e_G) = f(e) = e_H = e$. Indeed,

$$f(e) = f(e \cdot e) = f(e)f(e)$$

whence $f(e) = e$. Also, $f(g^{-1}) = f(g)$ since

$$f(g)f(g^{-1}) = f(gg^{-1}) = e.$$

A group homomorphism is called an isomorphism if it is also bijective. These are of particular importance, as they provide a method of classifying groups. We shall say two groups G and H are isomorphic if there exists an isomorphism $f : G \longrightarrow H$. To ease notation, we shall then write $G \cong H$. We note that being isomorphic is an equivalence relation on groups, as is easy to check. It is therefore practical to consider two groups G and H to be identical whenever they are isomorphic. We will very shortly be considering how isomorphisms preserve groups, but for now consider only the weaker homomorphisms.

If $f : G \longrightarrow H$ is a homomorphism of groups, we denote by $\mathrm{Im}(f)$ the set $f(G)$, which is a subgroup of H (check this as an exercise). The kernel of f, defined to be

$$\mathrm{Ker}\, f := \{g \in G : f(g) = e\},$$

is a subgroup of G (as is easy to verify). In fact, much more can be said!

LEMMA 1.16. *Let $f : G \longrightarrow H$ be a homomorphism of groups. Then* $\mathrm{Ker}\, f \lhd G$ *and f is injective if and only if* $\mathrm{Ker}\, f = \{e\}$. *For every $h \in \mathrm{Im}(f)$, the fiber*

$$f^{-1}(h) = \{g \in G : f(g) = h\}$$

is a (left)-coset of the kernel.

PROOF. If $n \in \mathrm{Ker}\, f$ we need only check that $f(gng^{-1}) = e$ for all $g \in G$. Certainly, $f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e$. Thence, $\mathrm{Ker}\, f \lhd G$. If f is injective then e can be the only element $g \in G$ such that $f(g) = e$, i.e. $\mathrm{Ker}\, f = \{e\}$. Conversely, if $\mathrm{Ker}\, f = e$ and $f(x) = f(y)$ for $x, y \in G$ it follows that $f(x)f(y)^{-1} = f(xy^{-1}) = e$ so that $xy^{-1} \in \mathrm{Ker}\, f$. That is, $xy^{-1} = e$ so that $x = y$. Now let $h \in \mathrm{Im}(f)$ and consider the fiber $f^{-1}(h)$. Since this set is non-empty, we are free to choose $x \in G$ such that $f(x) = h$. Then $x\mathrm{Ker}\, f \subseteq f^{-1}(h)$ since

$$f(xn) = f(x)f(n) = h, \quad \forall n \in \mathrm{Ker}\, f.$$

For the reverse inclusion suppose $f(y) = h = f(x)$. Then $f(yx^{-1}) = e$ so that $yx^{-1} \in \mathrm{Ker}\, f$, i.e. $y \in x\mathrm{Ker}\, f$ since $\mathrm{Ker}\, f \lhd G$. □

PROPOSITION 1.17. *Let G and H be finite groups and $f : G \longrightarrow H$ a homomorphism. If $g \in G$ then* $\mathrm{ord}(f(g)) \leq \mathrm{ord}(g)$.

PROOF. Let $k = \mathrm{ord}(g)$, then $g^k = e$. Now, $f(g)^k = f(g^k) = f(e) = e$. □

LEMMA 1.18. *Let G be a group and $N \lhd G$. The map $\pi_N : G \longrightarrow G/N$ given by $\pi_N(g) = gN$ is a surjective homomorphism of groups. Moreover,* $\mathrm{Ker}\, \pi_N = N$.

PROOF. Obviously, π_N is a homomorphism of groups. Clearly, π_N is surjective since $g \mapsto gN$ and any element of G/N is of this form. To see that $\mathrm{Ker}\, \pi_N = N$, we need only observe that $gN = N$ if and only if $g \in N$ (by Lemma 1.13). □

Surprisingly, we have the following.

COROLLARY 1.19. *Let G be a group and N a subgroup of G. Then N is normal if and only if N is the kernel of a group homomorphism defined on G.*

5.1. Images under Homomorphisms.

PROPOSITION 1.20. *Let $f : G \longrightarrow H$ be a homomorphism.*

(1) *If $A < G$ then $f(A) < H$,*

(2) *If $B < H$ then $f^{-1}(B) < G$,*

(3) *If f is surjective and $A \lhd G$ then $f(A) \lhd H$,*

(4) *If $B \lhd H$ then $f^{-1}(B) \lhd G$.*

PROOF. It is trivial to check that $e \in f(A)$ since $f(e) = e$. If $h_1, h_2 \in f(A)$ then there exist $g_1, g_2 \in A$ such that $f(g_1) = h_1$ and $h_2 = f(g_2)$. Then $g_1 g_2 \in A$ so that $f(g_1 g_2) = f(g_1)f(g_2) = h_1 h_2 \in f(A)$. Similarly, $f(g_1^{-1}) = f(g_1)^{-1} \in f(A)$.

Again, $e \in f^{-1}(B)$. Choose $g_1, g_2 \in f^{-1}(B)$ so that $f(g_1), f(g_2) \in B$. This implies that $f(g_1)f(g_2) = f(g_1 g_2) \in B$ so that $g_1 g_2 \in f^{-1}(B)$. One also has $f(g_1)^{-1} = f(g_1^{-1}) \in B$ so that $g_1^{-1} \in f^{-1}(B)$.

Suppose that f is surjective and that $A \lhd G$. Let $n \in f(A)$ and $h \in H$ be given; then $h = f(g)$ and $n = f(a)$ for some $g \in G$ and $a \in A$ so that

$$hnh^{-1} = f(g)f(a)f(g)^{-1} = f(gkg^{-1})$$

where $gag^{-1} \in A$ since $A \lhd G$. It follows that $hnh^{-1} = f(a') \in f(A)$.

For the final point, let $g \in G$ and $a \in f^{-1}(B)$, we show that $gag^{-1} \in f^{-1}(B)$. Certainly, we need only observe that

$$f(gag^{-1}) = f(g)f(a)f(g)^{-1}$$

where $f(a) \in B \lhd H$. Thus, $f(gag^{-1}) = f(g)f(a)f(g)^{-1} \in B$ which implies that $gag^{-1} \in f^{-1}(B)$, as was required. □

We shall now present two results that, although not of immediate use, will pop-up in results in the subsequent chapters. We give their proofs now as we have already developed all the required tools.

PROPOSITION 1.21. *Let G be a group and p, q distinct primes. Let P and G be groups of G having order p and q, respectively. Then $P \cap Q = \{e\}$.*

PROOF. Since P and Q are subgroups, they both contain the identity. That is, $\{e\} \subseteq P \cap Q$. Now $P \cap Q$ is a subgroup of P which, by Lagrange's theorem, means that $|P \cap Q|$ divides $|P| = p$. Likewise, $|P \cap Q|$ is a divisor of q. This implies that $|P \cap Q| \leq \gcd(p, q) = 1$. This means that $P \cap Q$ contains at most one element, i.e. $P \cap Q = \{e\}$. □

PROPOSITION 1.22. *Let G be a group and suppose that N, K are normal subgroups of G with $N \cap K = \{e\}$. Then the elements of N commute with those in K, i.e.*

$$nk = kn, \quad \forall (n,k) \in N \times K.$$

PROOF. Let $n \in N$ and $k \in N$ be given. Notice that $nk = kn$ if and only if $nkn^{-1}k^{-1} = e$. Since $K \lhd G$, it follows that

$$\underbrace{nkn^{-1}}_{\in K} k^{-1} \in K.$$

In a similar vein,

$$n \underbrace{kn^{-1}k^{-1}}_{\in N} \in N.$$

This means that $nkn^{-1}k^{-1} \in K \cap N = \{e\}$. This proves the proposition. □

6. Group Isomorphisms

In this section we focus on the notion of a group isomorphism, which is extremely useful in the identification of groups. As previously mentioned, being isomorphic is an equivalence relation on groups. This is particularly useful in studying groups of prime order p, which is our first topic of the section. As we shall soon see, there is really only one group of order p, and this group is $\mathbb{Z}/p\mathbb{Z}$.

LEMMA 1.23. *Let G and H be finite groups such that $G \cong H$. Then G is cyclic if and only if H is cyclic.*

PROOF. Let $f : G \longrightarrow H$ be an isomorphism of groups. By symmetry, it suffices to show that H is cyclic whenever G is. Let g be a generator of G, we claim $h := f(g)$ generates H. Certainly, if $y \in H$ then there exists a unique $x \in G$ with $f(x) = y$. Write $x = g^a$ for some $a \in \mathbb{N}$ and note that

$$h = f(x) = f(g^a) = f(g)^a.$$

If $a = \text{ord}(g) = |G|$ we have $h = e$. Hence, $H = \langle f(g) \rangle$. □

LEMMA 1.24. *Suppose $G \cong H$. If G is Abelian, then so is H.*

PROOF. Let $f : G \longrightarrow H$ be an isomorphism of groups and fix $h_1, h_2 \in H$. There exist $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Then,

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2)f(g_1) = h_2 h_1.$$

□

THEOREM 1.25 (Classification of Prime Groups). *Let p be a prime and G a group of order p. Then G is cyclic, Abelian, and isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

PROOF. We already know from Corollary 1.6 that G is necessarily cyclic. Let g be a generator of G and define a map $G \longrightarrow \mathbb{Z}/p\mathbb{Z}$ by $g^a \mapsto a$, where $a \in \mathbb{N}$ is considered modulo p. This clearly defines a homomorphism of groups since the group operation of $\mathbb{Z}/p\mathbb{Z}$ is addition. Also, this association is obviously bijective since G contains precisely p elements which are completely determined by a modulo p. We conclude that $G \cong \mathbb{Z}/p\mathbb{Z}$ and the statement follows from Lemma 1.24. □

PROPOSITION 1.26. *Let G and H be finite groups and $f : G \longrightarrow H$ an isomorphism. Then f preserves the order of elements. That is,* $\mathrm{ord}(f(g)) = \mathrm{ord}(g)$ *for all $g \in G$.*

PROOF. Let $g \in G$ and note that $g^{|G|} = e$. Hence, $\mathrm{ord}(g) < \infty$. Also, since f is a homomorphism:

$$f(g)^{\mathrm{ord}}(g) = f\left(g^{\mathrm{ord}}(g)\right) = f(e) = e.$$

Hence, $\mathrm{ord}(f(g)) \leq \mathrm{ord}(g)$. To see the reverse inequality, note that for $\ell := \mathrm{ord}(f(g))$ one has

$$e = f(g)^\ell = f(g^\ell).$$

Since f is injective, it follows that $g^\ell = e$. Hence, $\mathrm{ord}(g) \leq \ell$. □

PROPOSITION 1.27. *Let G and H be groups and $f : G \longrightarrow H$ a group homomorphism. If G is Abelian, then $f(G)$ is an Abelian subgroup of H.*

PROOF. Let $h_1, h_2 \in f(G)$ and choose $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Observe then that

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2)f(g_1) = h_2 h_1.$$

□

COROLLARY 1.28. *Let G and H be groups and suppose G is Abelian. If $G \cong H$, then H is also Abelian.*

6.1. The Isomorphism Theorems. We dedicate the remainder of this section to the isomorphism theorems. These results are useful, once again, in studying the basic "building blocks" of groups. We shall make heavy use of these results when identifying groups up to isomorphism or when developing the "Sylow philosophy". The usefulness of these results will become clearer in the future.

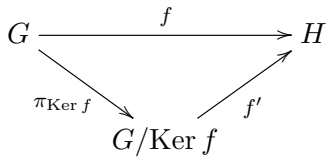
THEOREM 1.29 (First Isomorphism Theorem). *Let G and H be groups and*

$$f : G \longrightarrow H$$

a group homomorphism. There exists an injective group homomorphism

$$f' : G/\mathrm{Ker}\, f \longhookrightarrow H$$

such that the following diagram commutes



(FI)

In particular, $G/\mathrm{Ker}\, f \cong f(G)$.

PROOF. We first note that the statement makes sense as $\mathrm{Ker}\, f$ is a normal subgroup of G, thus we can give a group structure to $G/\mathrm{Ker}\, f$. We now define

$$f' : G/\mathrm{Ker}\, f \longrightarrow H, \quad g\mathrm{Ker}\, f \mapsto f(g).$$

This is well defined, indeed if $x\mathrm{Ker}\, f = y\mathrm{Ker}\, f$ then $y = xn$ for some $n \in \mathrm{Ker}\, f$ whence we obtain

$$f'(y\mathrm{Ker}\, f) = f(y) = f(xn) = f(x) = f'(x\mathrm{Ker}\, f).$$

Since f is itself a homomorphism of groups, it is clear that f' is a homomorphism in its own right. To see that f' is injective, assume that

$$f'(x\mathrm{Ker}\, f) = f(x) = f(y) = f'(y\mathrm{Ker}\, f)$$

for some $x, y \in G$. Then $f(xy^{-1}) = e$ so that $xy^{-1} \in \mathrm{Ker}\, f$, i.e. $x \in y\mathrm{Ker}\, f$ (since $\mathrm{Ker}\, f$ is normal in G). It then follows that $x\mathrm{Ker}\, f \subseteq y\mathrm{Ker}\, f$. By symmetry, equality then holds. Thus, f' is indeed an injective homomorphism whose image is $f(G)$. It follows that $G/\mathrm{Ker}\, f \cong f(G)$. □

This first isomorphism theorem will often serve as a stepping stone.

THEOREM 1.30 (Second Isomorphism Theorem). *Let G be a group and B, N subgroups of G such that $N \lhd G$. Then*

$$B/(B \cap N) \cong BN/N.$$

REMARK 1.3. We first point out that the statement here makes sense. Indeed, the subgroup $(B \cap N)$ is normal in B by Lemma 1.15. By this same lemma, BN is a subgroup of G which implies, in particular, that N is normal in BN.

PROOF OF SECOND ISOMORPHISM THEOREM. We proceed directly and define a mapping between groups

$$f : B/(B \cap N) \longrightarrow BN/N, \quad b(B \cap N) \mapsto bN.$$

This makes sense since $bN = (be)N \in BN/N$. First, we check that this function is well defined. Indeed, if $b_1(B \cap N) = b_2(B \cap N)$ for $b_1, b_2 \in B$ then $b_2 = b_1 x$ for some $x \in B \cap N$. This implies that

$$b_2 \overset{f}{\mapsto} b_2 N = b_1 x N = b_1 N.$$

It is easy to check that f is a group homomorphism. Also, f is surjective since every element of BN/N is a coset $(bn)N = bN$ which is mapped to by the element $b(B \cap N)$. It remains only to verify that f is injective. To see that this is so, assume that

$$f(b_1(B \cap N)) = b_1N = b_2N = f(b_2(B \cap N)).$$

Then, $b_2 = b_1n$ for some $n \in N$. In particular, $n \in B \cap N$ so that

$$b_2(B \cap N) = (b_1n)(B \cap N) = b_1(B \cap N).$$

We conclude that the theorem holds. □

We conclude this section with the following result, which is frequently dubbed the *third isomorphism theorem*.

THEOREM 1.31 (Third Isomorphism Theorem). *Let G be a group and $N < K < G$ be such that $N \lhd G$ and $K \lhd G$, Then*

$$G/K \cong (G/N)/(K/N).$$

PROOF. We construct a group homomorphism $f : G/N \longrightarrow G/K$ by letting $gN \mapsto gK$. We first check that this is a well defined function. Suppose that $xN = yN$ for $x, y \in G$. Then $y = xn$, for some $n \in N$, so that $yK = xnK = xK$ (since $n \in N \subseteq K$).

Clearly, f is a homomorphism whose image is G/K. Indeed, every coset in G/K can be written as gK for $g \in G$ and thus $f(gN) = gK$. It remains only to compute the kernel of f. We have

$$\begin{aligned} \operatorname{Ker} f = \left\{x \in G/N : f(x) = e_{G/K} = K\right\} &= \{gN : gK = K\} \\ &= \{gN : g \in K\} \\ &= K/N. \end{aligned}$$

By the first isomorphism theorem,

$$G/K \cong (G/N)/\operatorname{Ker} f = (G/N)/(K/N).$$

□

7. The Correspondence Theorems

A frequent addition to the previous isomorphism theorems are the so-called *correspondence theorems*, which we present below

THEOREM 1.32. *Let $f : G \longrightarrow H$ be a surjective homomorphism of groups. There exists a bijection*

$$F : \{\textit{subgps. of } G \textit{ containing } \operatorname{Ker} f\} \longrightarrow \{\textit{subgps. of } H\}.$$

PROOF. We introduce notation. For the remainder of the proof we denote by G_1 an arbitrary subgroup of G containing the normal subgroup $\operatorname{Ker} f$ of G; H_1 will denote an arbitrary subgroup of H. We then define

$$F(G_1) := f(G_1) < H.$$

By earlier results, it is indeed true that $f(G_1)$ is a subgroup of H. We also construct an auxiliary function:

$$F'(H_1) := f^{-1}(H_1) < G.$$

It suffices to show that $F \circ F' = \mathbf{1}$ and $F' \circ F = \mathbf{1}$. First, fix $H_1 < H$. Let $y \in H_1$. Then $y = f(x)$ for some $x \in f^{-1}(H_1)$. It follows that $y = f(x) \in f(f^{-1}(H_1))$, i.e. $H_1 \subseteq f(f^{-1}(H_1))$. If $y \in f(f^{-1}(H_1))$ then there exists $x \in f^{-1}(H_1)$ so that $y = f(x)$ whence $f(x) \in H_1$. This shows that $H_1 = f(f^{-1}(H))$. Hence,

$$F \circ F' = \mathbf{1}.$$

Let $G_1 < G$ be as above. Let $x \in G_1$ so that $f(x) \in f(G_1)$. It follows that $x \in f^{-1}(f(G_1))$ whence $G_1 \subseteq f^{-1}(f(G_1))$. For the reverse (and final) inclusion we fix $x \in f^{-1}(f(G_1))$ so that $f(x) \in f(G_1)$. Take $g \in G_1$ so that $f(x) = f(g)$. Since f is a homomorphism of groups it follows that $xg^{-1} \in \operatorname{Ker} f$. Hence, $x \in [\operatorname{Ker} f]g = g\operatorname{Ker} f \in G_1$ where this last inclusion follows from the fact that $g \in G_1$ and $\operatorname{Ker} f < G_1$. This shows that $F' \circ F = \mathbf{1}$ which completes the proof of the correspondence theorem. □

THEOREM 1.33. *Let G and H be groups and $f : G \longrightarrow H$ a surjective homomorphism of groups. Suppose* $\operatorname{Ker} f < G_1 < G_2 < G$. *Then $G_1 \lhd G_2$ if and only if $f(G_1) \lhd f(G_2)$. In this case,*

$$G_2/G_1 \cong f(G_2)/f(G_1).$$

PROOF. Let $f : G_2 \longrightarrow f(G_2)$ denote the restriction of f to G_2. This is clearly once again a homomorphism of groups. If $G_1 \lhd G_2$, it follows from the fact that f is surjective that $f(G_1) \lhd f(G_2)$ (see Proposition 1.20). Conversely, suppose that $f(G_1) \lhd f(G_2)$. Then, by this same proposition,

$$f^{-1}(f(G_1)) \lhd f^{-1}(f(G_2)) = G_2.$$

Clearly, $G_1 \subseteq f^{-1}(f(G_1))$. If $x \in f^{-1}(f(G_1))$ then $f(x) \in f(G_1)$. Hence, for some $g \in G_1$, there holds $f(x) = f(g)$ so that $f(xg^{-1}) = e$. This means that xg^{-1} belongs to $\operatorname{Ker} f$ whence $x = kg$ for some $k \in \operatorname{Ker} f \subseteq G_1$. This shows that $f^{-1}(f(G_1)) \subseteq G_1$.

Assume now that $G_1 \lhd G_2$, the quotient group $f(G_2)/f(G_1)$ is (by the first part) well defined. Consider the map

$$\Gamma : G_2/G_1 \longrightarrow f(G_2)/f(G_1), \quad gG_1 \mapsto f(g)f(G_1).$$

We first show that this is well defined. If $xG_1 = yG_1$ then $y = xg$ for $g \in G_1$. Therefore, $f(g) \in f(G_1)$ whence

$$\Gamma(yG_1) = f(y)f(G_1) = f(xg)f(G_1) = f(x)f(g)f(G_1) = f(x)f(G_1).$$

If $xG_1, yG_1 \in G_2/G_1$ then

$$\Gamma(xyG_1) = f(xy)f(G_1) = f(x)f(y)f(G_1) = \Gamma(xG_1)\Gamma(yG_1)$$

so that Γ is a homomorphism. Given $yf(G_1) \in f(G_2)/f(G_1)$ there must exist $x \in G_2$ such that $f(x) = y$. Hence Γ is surjective. Finally, to see that Γ is injective assume

$$\Gamma(xG_1) = f(x)f(G_1) = f(y)f(G_1) = \Gamma(yG_1)$$

for $(x, y) \in G_2 \times G_2$. Then $f(y) = f(x)h$, for some $h \in f(G_1)$. It follows that $f(yx^{-1}) \in f(G_1)$. By a previous argument, this means that $yx^{-1} \in G_1$ whence Γ is injective. □

8. Exercises

Here we give some problems pertinent to the topics presented in this chapter. We give very few exercises, although they require a certain creativity to solve.

EXERCISE 1.1. Let $n \in \mathbb{N}$ and denote by S_n the family of all bijective functions

$$\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}.$$

Prove that S_n is a group under composition of functions. This group is called the *symmetric group on n letters*.

EXERCISE 1.2. Let G be a group. Verify that $Z(G)$ is a subgroup of G.

EXERCISE 1.3. A boolean group is a group $\mathfrak{B}$ such that $g^2 = e$ for every $g \in \mathfrak{B}$. Prove that any boolean group $\mathfrak{B}$ is Abelian.

EXERCISE 1.4. Let $\mathbb{F} \subseteq \mathbb{K}$ be two finite fields and suppose $|\mathbb{F}| = q$ for some $q \geq 2$. Establish each of the following.

(1) $|\mathbb{K}| = q^n$ for some $n \geq 1$.
(2) If $x^q = x$ for all $x \in \mathbb{F}$.
(3) If $x \in \mathbb{K}$ is such that $x^q = x$ then $x \in \mathbb{F}$.

EXERCISE 1.5. Let G and H be groups of finite order and let $n := |G|$ and $m := |H|$. Prove that if $\gcd(n, m) = 1$, then every homomorphism $G \longrightarrow H$ is the trivial[2] one.

EXERCISE 1.6. Let G be a group and fix $x \in G$. Define a map

$$\tau_x : G \longrightarrow G, \quad g \mapsto xgx^{-1}.$$

Prove that τ_x is a bijective homomorphism of groups. Such a map is called an *automorphism* of G.

EXERCISE 1.7. Let G be a group. An automorphism of G is a bijective group homomorphism $G \longrightarrow G$. Let $\mathrm{Aut}(G)$ denote the (non-empty) set of all automorphisms of G. Prove that $\mathrm{Aut}(G)$ is a group under composition.

[2]The trivial homomorphism $f : G \longrightarrow H$ is that which takes every $g \in G$ to e_H.

Chapter 2

Group Actions

Throughout this chapter we shall mainly study how groups can act upon a arbitrary sets. This notion is useful both in combinatorics and in geometry, although we will not dwell on these. The theory that is developed in this chapter will be essential when we study p-groups (groups whose order is a positive power of a prime) and in the Sylow-philosophy. We now introduce group actions.

1. The Basics

Unless stated otherwise, G will denote a group and S will denote a non-empty set. We say that G acts upon S if we are given a function

$$\bigstar : G \times S \longrightarrow S, \quad (g, s) \mapsto g * s$$

that satisfies each of the following:

(1) $e * s = s$ for all $s \in S$,

(2) $g_1 * (g_2 * s) = (g_1 g_2) * s$ for all $g_1, g_2 \in G$ and $s \in S$.

For $s \in S$, we define the *orbit* and *stabilizer* of s by

$$\mathrm{Orb}(s) = \{g * s : g \in G\}, \tag{2.1}$$

$$\mathrm{Stab}(s) = \{g \in G : g * s = s\}. \tag{2.2}$$

Note that $\mathrm{Orb}(s) \subseteq S$ and $\mathrm{Stab}(s) \subseteq G$, for each $s \in S$. One should view G as the collection of symmetries of S. More precisely, we make the following observations G and S as above.

PROPOSITION 2.1. *Let G act upon a non-empty set S.*

(1) *If $s_1, s_2 \in S$ we say $s_1 \sim s_2$ if $s_1 \in \mathrm{Orb}(s_2)$. This is an equivalence relation on S. In particular, S is the disjoint union of orbits.*

(2) *For each $s \in S$ the set $\mathrm{Stab}(s)$ is subgroup of G.*

(3) *For each S there exists a bijection between the collection of left cosets of $\mathrm{Stab}(s)$ in G and $\mathrm{Orb}(s)$. That is, there is a one-to-one correspondence*

$$G/\operatorname{Stab}(s) \longleftrightarrow \operatorname{Orb}(s).$$

PROOF. Since $s = e * s$ it is clear that $s \sim s$. If $s_1 \sim s_2$ then $s_1 \in \mathrm{Orb}(s_2)$ so that there exists $g \in G$ such that $s_1 = g * s_2$. It follows that $s_2 = g^{-1} * s_1$ and $s_2 \in \mathrm{Orb}(s_1)$, i.e. $s_2 \sim s_1$. Suppose now that $s_1 \sim s_2$ and $s_2 \sim s_3$. One can then choose $g_1, g_2 \in G$ such that $s_1 = g_1 * s_2$ and $s_2 = g_2 * s_3$. Then,

$$(g_1 g_2)s_3 = g_1 * (g_2 * s_3) = g_1 * s_2 = s_1.$$

Thus, $s_1 \sim s_3$ since $s_1 \in \mathrm{Orb}(s_3)$. Also note that

$$[s] = \{x \in S : x \sim s\} = \operatorname{Orb}(s)$$

and so it follows that S is the disjoint union of equivalence classes (orbits). This verifies (1). For the second point let $s \in S$ and consider $\mathrm{Stab}(s)$. This is a non-empty subset of G (it always contains e). If $g_1, g_2 \in \mathrm{Stab}(s)$ then $g_1 * s = s$ and $g_2 * s = s$ whence

$$(g_1 g_2) * s = g_1 * (g_2 * s) = g_1 * s = s.$$

It follows that $\mathrm{Stab}(s)$ is closed under the group operation. If $g \in \mathrm{Stab}(s)$ then $g * s = s$ which implies that $g^{-1} * s = s$ as well. Thus, (2) holds. It now only remains to establish (3). Let $s \in S$ be fixed and define a mapping

$$f : G/\operatorname{Stab}(s) \longrightarrow \operatorname{Orb}(s), \quad g\operatorname{Stab}(s) \mapsto g * s.$$

Although $\mathrm{Stab}(s)$ is not necessarily a normal subgroup, we can make sense of left-cosets of $\mathrm{Stab}(s)$ in G and thus the above makes sense. We now check that the above is well defined. Suppose $g_1 \operatorname{Stab}(s) = g_2 \operatorname{Stab}(s)$; then $g_1\sigma = g_2$ for some $\sigma \in \mathrm{Stab}(s)$. It follows that

$$g_2 * s = (g_1\sigma) * s = g_1 * (\sigma * s) = g_1 * s.$$

If $x \in \mathrm{Orb}(s)$ then $x = g * s$ for some $g \in G$. This means that

$$f(g\operatorname{Stab}(s)) = g * s = x,$$

i.e. that f is a surjective map whose image is $\mathrm{Orb}(s)$. To conclude the proof, we check that f is injective. If $g*s = g'*s$ for $g, g' \in G$ it follows that $g^{-1}g'*s = s$ so that $g^{-1}g' \in \mathrm{Stab}(s)$, or rather than $g' \in g\operatorname{Stab}(s)$. This implies that $g'\operatorname{Stab}(s) \subseteq g\operatorname{Stab}(s)$. By symmetry we must also have $g'\operatorname{Stab}(s) \supseteq g\operatorname{Stab}(s)$ which concludes the proof. □

This proposition has a very useful consequence that applies when G and S are finite sets: the orbit-stabilizer formula, which is exceptionally useful in combinatorics.

COROLLARY 2.2 (Orbit-Stabilizer). *Let G be a finite group acting upon a finite set S. For each $s \in S$ there holds*

$$|G| = |\mathrm{Orb}(s)| \cdot |\mathrm{Stab}(s)|\,. \tag{2.3}$$

PROOF. By the previous proposition, there exists a bijection

$$G/\mathrm{Stab}(s) \longleftrightarrow \mathrm{Orb}(s)$$

which implies by Lagrange's theorem that

$$\frac{|G|}{|\mathrm{Stab}(s)|} = |\mathrm{Orb}(s)|\,.$$

□

2. Cayley's Theorem and Burnside's Formula

If A is a finite non-empty set we denote by Σ_A the collection of all bijections $A \longrightarrow A$. It is very easy to check that Σ_A is a group under composition. It is also clear that $\Sigma_A \cong \mathsf{S}_n$, where S_n is the permutation group on n-letters[1]. Let G be a finite group acting upon a finite set S via some action $\star$. Define a map

$$\Psi : G \longrightarrow \Sigma_S$$

by letting $\psi(g) : S \longrightarrow S$ be given by $\psi(g)(s) := g * s$. For each fixed g, the map $\Psi(g)$ is surjective since $g^{-1} * s \in S$ and $\psi(g)(g^{-1} * s) = g * (g^{-1} * s) = s$. $\Psi(g)$ is also an injection since $\psi(g)(s_1) = \psi(g)(s_2)$ if and only if $g * s_1 = g * s_2$. Multiplying through by g^{-1} yields then that $s_1 = s_2$. Thus, $\Psi(g)$ indeed belongs to Σ_S for each $g \in G$. Our next step is to argue that Ψ is in fact a homomorphism of groups. Ψ is certainly a homomorphism since

$$\Psi(g_1 g_2)(s) = (g_1 g_2) * s = g_1 * (g_2 * s) = (\Psi(g_1) \circ \Psi(g_2))(s).$$

It is also easy to see that

$$\mathrm{Ker}\,\Psi = \bigcap_{s \in S} \mathrm{Stab}(s).$$

Conversely, given such a homomorphism $\Psi : G \longrightarrow \Sigma_S$ we define an action $g * s := \Psi(g)(s)$. We have proven:

PROPOSITION 2.3. *Let G be a group and S a non-empty set. Then G acts upon S if and only if there exists a homomorphism $\Psi : G \longrightarrow \Sigma_S$ as above.*

On its own this proposition is not of much importance. However, there is a particular such Ψ that is of great interest.

THEOREM 2.4 (Cayley's Theorem). *Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.*

[1] S_n is the collection of all bijections $\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$. This is clearly a group under composition of functions. As mentioned above, $\Sigma_A \cong \mathsf{S}_n$ where $n = |A|$.

PROOF. We let G act upon itself by defining $S := G$ and defining

$$G \times S \longrightarrow S, \quad g * s := gs.$$

It is very easy to check that this is a well defined action of G (in fact this is immediate from the group axioms). By what we have done earlier in this section, this action corresponds to a group homomorphism

$$\Psi : G \hookrightarrow \Sigma_S \cong \mathsf{S}_n,$$

where $\Psi(g) : S \longrightarrow S$ is given by $\Psi(g)(s) = gs$. However, we are also claiming that Ψ is injective[2]. To verify this, suppose $\Psi(g_1) \equiv \Psi(g_2)$, i.e. $g_1 s = g_2 s$ for all $s \in S$. Since $S = G$, we take $s = e$ to obtain $g_1 = g_2$. Thus, Ψ is indeed an injection which shows that

$$G \cong \Psi(G) < \Sigma_G \cong \mathsf{S}_n.$$

This completes the proof of Cayley's theorem. □

We now turn towards an efficient combinatorial formula for group actions. Suppose once again we are given a finite group G which acts upon a finite set S. For an element $g \in G$ we define

$$I(g) := |\{s \in S : g * s = s\}|. \tag{2.4}$$

Thus, $I(g)$ is the number of elements in S fixed by the action of g.Loosely speaking, it is the "stabilizer in S". We now prove the following result:

THEOREM 2.5 (Burnside). *Let G be a finite group acting upon a finite set S and let $I(g)$ be as in (2.4). If N denotes the number of orbits in S*

$$N = \frac{1}{|G|} \sum_{g \in G} I(g).$$

PROOF. We first define a binary map $\mathsf{T} : G \times S \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by

$$\mathsf{T}(g, s) := \begin{cases} 1, & \text{if } g * s = s, \\ 0, & \text{else.} \end{cases}$$

[2]Often, an injective homomorphism of groups is called an embedding. In the context of topological spaces, an embedding is an injective continuous function.

Fix now representatives $\{s_1, s_2, \ldots, s_N\}$ for the orbits in S and write

$$\begin{aligned}\sum_{g\in G} I(g) = \sum_{g\in G}\sum_{s\in S} \mathsf{T}(g,s) &= \sum_{s\in S}\sum_{g\in G} \mathsf{T}(g,s)\\ &= \sum_{s\in S} |\mathrm{Stab}(s)|\\ &= \sum_{s\in S} \frac{|G|}{|\mathrm{Orb}(s)|}\\ &= \sum_{k=1}^{N} \sum_{s\in \mathrm{Orb}(s_k)} \frac{|G|}{|\mathrm{Orb}(s)|}\\ &= \sum_{k=1}^{N} \sum_{s\in \mathrm{Orb}(s_k)} \frac{|G|}{|\mathrm{Orb}(s_k)|}\\ &= \sum_{k=1}^{N} |G|\end{aligned}$$

which is precisely $N \cdot |G|$. The proof is now complete. □

This formula, also seemingly strange to consider, allows for a simple proof of a surprising fact. First, we require the following definition.

DEFINITION 7. If G is a group acting on a finite set S, we say G acts transitively on S if S has only one orbit.

COROLLARY 2.6. *Suppose G is a finite group acting transitively upon a finite set S, where $|S| > 1$. There exists $g \in G$ without fixed points.*

PROOF. Suppose, by way of contradiction, that every $g \in G$ has at-least one fixed point in S. Then, by Burnside's formula we have $N = \frac{1}{|G|}\sum_{g\in G} I(g)$ where

$$\sum_{g\in G} I(g) = I(e) + \sum_{g\neq e} I(g) = |S| + \sum_{g\neq e} I(g) > 1 + \sum_{g\neq e} I(g) \geq |G|\,.$$

This implies that

$$N = \frac{1}{|G|}\sum_{g\in G} I(g) > 1$$

which is a contradiction. □

2.0.1. *Subgroups of Minimal Prime Index are Normal.* Let G be a finite group and suppose H is a subgroup of G of index p, where p is the minimal prime dividing the order of G.

We claim that H is normal in G. To this end, we consider the action of G upon G/H by left multiplication:

$$\bigstar : G \times G/H \longrightarrow G/H, \quad (g, xH) \mapsto gxH.$$

It is left as an exercise to check that this a well defined action. Now, we have seen that this is equivalent to giving a homomorphism of groups

$$\Psi : G \longrightarrow \mathsf{S}_p, \quad g \mapsto \psi(g)$$

where $\Psi(g)$ takes xH to gxH. We now point out that $N = \operatorname{Ker}\Psi$ is a normal subgroup of G that is contained in H. Indeed, if $g \in \operatorname{Ker}\Psi$ then $\Psi(g)$ takes xH to xH for every $xH \in G/H$. In particular, $gH = H$, which is only possible if $g \in H$. This grants us the inclusion $N \subseteq H$. We must now only show the reverse inequality. The first isomorphism theorem gives

$$\Psi(G) \cong G/N.$$

Since $\Psi(G)$ is a subgroup of S_p, we have that $|\Psi(G)| \mid p!$. However, since $|\Psi(G)|$ also divides $|G|$, it follows that either $|\Psi(G)| = 1$ or $|\Psi(G)| = p$. Now,

$$|\Psi(G)| = \frac{|G|}{|H|} \cdot \frac{|H|}{|N|} \geq p$$

whence it follows that $|\Psi(G)| = p$. Thus, $[G : N] = p$. However, this means that

$$\frac{|G|}{|N|} = \frac{|G|}{|H|}$$

which gives $|N| = |H|$. Thus, $H = N$ as was required.

3. Conjugation of Groups

There is a very special action that, surprisingly, appears frequently in the study of finite groups. The conjugacy action of G upon itself is simply the map $\star : G \times G \longrightarrow G$ which takes $(g, x) \mapsto gxg^{-1}$, for fixed g. Then,

$$\operatorname{Orb}(x) = \{g * x : g \in G\} = \left\{gxg^{-1} : g \in G\right\}$$

is called the *conjugacy class of x in G*, which we affectionately denote by $\operatorname{Conj}(x)$. By what we know about group actions, it follows that G it itself the disjoint union of orbits (and, thus, of conjugacy classes). The stabilizer of $x \in G$ is given by

$$\operatorname{Stab}(x) = \left\{g \in G : gxg^{-1} = x\right\} = \{g \in G : gx = xg\} = \operatorname{C}(x).$$

Thus, $\operatorname{Stab}(x)$ is precisely the centralizer of x. It also follows that there exists a bijection

$$G/\operatorname{C}(x) \longleftrightarrow \operatorname{Conj}(x).$$

Suppose that $|G| < \infty$; if we choose representatives for the conjugacy classes in G, it follows that

$$|G| = \sum_{x \text{ repr.}} |\mathrm{Conj}(x)|\,.$$

Now, if $x \in Z(G)$ (where $Z(G)$ is the center of G)

$$\mathrm{Conj}(x) = \left\{gxg^{-1} : g \in G\right\} = \{x\}$$

since x commutes with all elements of G. Thus, the equation for $|G|$ becomes

$$|G| = |Z(G)| + \sum_{\substack{x \notin Z(G) \\ x \text{ repr.}}} |\mathrm{Conj}(x)| = |Z(G)| + \sum_{\substack{x \text{ repr.} \\ x \notin Z(G)}} \frac{|G|}{\mathrm{C}(x)}. \tag{2.5}$$

The above is known as the *class equation*. This equation is useful in the "counting of finite groups". For the remainder of this section, G will denote a finite group.

PROPOSITION 2.7. *Given $n \in \mathbb{N}$, there exist only finitely many groups of order n.*

PROOF. This is immediate from the fact that, up to isomorphism, there exist only finitely many functions $G \times G \longrightarrow G$ whenever G is finite. □

LEMMA 2.8. *Let $q \in \mathbb{Q}$ with $q > 0$. For each $t \in \mathbb{N}$, there exist at most finitely many $n_j \in \mathbb{N}$, $1 \leq j \leq t$, such that*

$$q = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_t}.$$

PROOF. The proof goes by way of induction on t. If we take $t = 1$ then the claim is obvious. Assume that the claim holds up to $t-1$, we proceed to establish it for t. Suppose we are given a representation

$$q = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_t}$$

as in the statement of the lemma. We may assume without loss of generality that $n_1 \geq n_2 \geq \cdots \geq n_t$. Thus,

$$q \leq \sum_{j=1}^{t} \frac{1}{n_t} = \frac{t}{n_t}.$$

Rather, $n_t \leq t/q$. Thus, we have a bound on the largest term of the representation. Applying the induction hypothesis to

$$q - \frac{1}{n_t}$$

for each possible representation (if some exist) the proof is complete. □

THEOREM 2.9. *Let $d \in \mathbb{N}$, there exist (up to isomorphism) at most finitely many finite groups with d conjugacy classes.*

PROOF. Let G be a finite group with d conjugacy classes. By equation (2.5) we have that

$$|G| = |Z(G)| + \sum_{\substack{x \text{ repr.} \\ x \notin Z(G)}} \frac{|G|}{\mathrm{C}(x)}.$$

Then,

$$1 = \frac{1}{|G| / |Z(G)|} + \sum_{\substack{x \text{ repr.} \\ x \notin Z(G)}} \frac{1}{\mathrm{C}(x)}$$

Since there are only finitely many ways to write this sum, we have determined the possible structures G can have. □

We conclude this section with the following characterization of normal subgroups.

PROPOSITION 2.10. *Let G be a group and H a subgroup of G. Then H is normal in G if and only if H is the disjoint union of conjugacy classes.*

PROOF. Suppose $H \lhd G$ and choose representatives $x_1, \ldots, x_d$ for the conjugacy classes in G. Every element $h \in H$ lies in exactly one of $\mathrm{Conj}(x_j)$. Let $x_1, \ldots, x_k$ be those for which $H \cap \mathrm{Conj}(x_j) \neq \varnothing$. Clearly, $H \subseteq \bigsqcup_{j=1}^{k} \mathrm{Conj}(x_j)$ since these conjugacy classes are disjoint. Since H is normal in G, we have for some $h_j \in H$ that $\mathrm{Conj}(x_j) = \mathrm{Conj}(h_j)$ so that

$$\mathrm{Conj}(x_j) = \mathrm{Conj}(h_j) = \left\{ g h_j g^{-1} : g \in G \right\} \subseteq H$$

whence we conclude that $H = \bigsqcup_{j=1}^{k} \mathrm{Conj}(x_j)$. Conversely, let us suppose that $H = \bigsqcup_{j=1}^{k} \mathrm{Conj}(x_j)$ for representatives x_j. Let $g \in G$ and $h \in H$. Then $h \in \mathrm{Conj}(x_j)$ for a unique index j. Then $\mathrm{Conj}(x_j) = \mathrm{Conj}(h)$ so that

$$ghg^{-1} \in \mathrm{Conj}(h) = \mathrm{Conj}(x) \subseteq H.$$

The proof is now complete. □

4. The Coset Representation

When studying the relationship between subgroups and larger groups containing said subgroups, it is common to consider the action of G upon the family of cosets G/H. This leads to a canonical homomorphism known as the *coset representation*. This "point of view" will be crucial in many of the exercises found at the end of this chapter.

The set up is simple: we consider a group G (not necessarily finite) and fix a subgroup H in G having index $n \in \mathbb{N}$. We define a map

$$G \times G/H \longrightarrow G/H, \quad (g, xH) \mapsto (gx)H.$$

This is clearly a well defined group action. By earlier results, we may therefore associate a group homomorphism

$$\Psi : G \longrightarrow \Sigma_{G/H} \cong \mathsf{S}_n.$$

The kernel of this homomorphism will be $\bigcap_{a\in G/H}\mathrm{Stab}(a)$ which is precisely the (normal) subset of G given by $\bigcap_{g\in G}\mathrm{Stab}(gH)$. We claim further that $\mathrm{Stab}(gH) = gHg^{-1}$. Indeed, if $x \in gHg^{-1}$ then $x = ghg^{-1}$ for some $h \in H$ whence it follows that

$$(x, gH) \mapsto (ghg^{-1}g)H = (gh)H = gH.$$

Hence, $gHg^{-1} \subseteq \mathrm{Stab}(gH)$ is clear. Conversely, suppose that $x \in \mathrm{Stab}(gH)$, i.e. $xgH = gH$. This implies that $xg = gh$ for some $h \in G$. It follows that $x = ghg^{-1} \in gHg^{-1}$. Thus, $\mathrm{Stab}(gH) = gHg^{-1}$ whence it follows that

$$\mathrm{Ker}\,\Psi = \bigcap_{g\in G} gHg^{-1}.$$

5. Exercises

We conclude this chapter with some exercises related to group actions. Some of these exercises are actually important results in the theory of finite groups that we shall make use of in later sections.

EXERCISE 2.1. Let G be a finite group and H a subgroup of G. Suppose p is the minimal prime dividing the order of G and assume $[G : H] = p$. Prove that H is normal in G.

EXERCISE 2.2. Suppose that G is a finite group and that A is a proper subgroup of G (that is, $A \neq G$). Prove that

$$G \supsetneq \bigcup_{g\in G} gAg^{-1}.$$

EXERCISE 2.3. Let G be a group acting upon a set S and let $s_1 \in \mathrm{Orb}(s)$, for some $s \in S$. Prove that $\mathrm{Stab}(s_1)$ is conjugate to $\mathrm{Stab}(s)$.

EXERCISE 2.4. Let G be a group and suppose H, K are subgroups of G having finite index. Prove that $H \cap K$ is also a subgroup of G and that $H \cap K$ has finite index in G.

EXERCISE 2.5. Recall that a group G is called simple if the only normal subgroups of G are G and $\{e\}$. Let G be a simple group of order n and let H be a subgroup of index $k \neq 1$. Prove that $k! \geq n$.

EXERCISE 2.6. The number of conjugacy classes in a group G is called its class number. Show that if G is a finite group with an even class number, then $|G|$ is even.

Chapter 3

The Sylow and Jordan-Hölder Philosophies

Throughout this chapter we examine the building blocks of finite groups, from two very different perspectives. This first point of view takes a number theoretic approach. Indeed, the Sylow philosophy examines groups whose orders are powers of primes (these are called p-groups). The Jordan-Hölder approach is quite different and instead investigates "chains" of normal subgroups of G whose quotients are both simple and Abelian. Although we could present the Jordan-Hölder theorem before those of Sylow, we feel the Sylow approach is simpler, clearer, and easier to motivate–especially to the reader with sufficient background in number theory.

1. p-Groups

This section is devoted to obtaining fundamental results regarding p-groups. These p-groups are fundamental to the Sylow-theorems.

DEFINITION 8. Let G be a finite group. We say that g is a p-group if $|G| = p^r$ for some p prime p and $r \in \mathbb{N}$.

It is understood that when we say "G is a p-group" the number p is prime. It is quite redundant to repeat this each time we mention a p-group.

LEMMA 3.1. *Let G be a p-group. Then the center of G is non-trivial, i.e. $Z(G) \supsetneq \{e\}$.*

PROOF. If $Z(G) = G$ then the result follows. Otherwise, choose $x \in G \setminus Z(G)$ and recall the class equation (see (2.5)) which states that

$$|G| = |Z(G)| + \sum_{\substack{x \text{ repr.} \\ x \notin Z(G)}} \frac{|G|}{\mathrm{C}(x)}.$$

Since $x \notin Z(G)$ we must have that $\mathrm{C}(x)$ is a proper subgroup of G. Hence,

$$p \mid |G| \,/\, |\mathrm{C}(x)|$$

which implies, by the class equation, that $p \mid |Z(G)|$ since

$$|Z(G)| = G - \sum_{\substack{x \text{ repr.} \\ x \notin Z(G)}} \frac{|G|}{\mathrm{C}(x)}.$$

where each term on the right hand side is divisible by $p > 1$. Thus, $|Z(G)| \geq p$ and $Z(G)$ is non-trivial. □

THEOREM 3.2. *Let G be a p-group.*

(1) *For each proper subgroup $H \lhd G$ there exists a subgroup $K < G$ with $H \lhd K \lhd G$ such that $[K : H] = p$.*

(2) *There exists a finite sequence of subgroups*

$$\{e\} =: H_0 < H_1 < \cdots < H_n := G \tag{3.1}$$

such that $|H_k| = p^k$ for each $k \in \{0, 1, \ldots, n\}$.

PROOF. We first prove (1). Since H is a proper normal subgroup of G, the quotient group G/H is well defined and has order $|G| \,/\, |H| \geq p$. Thus, G/H is a p-group in its own right. By the previous lemma, we may choose $x \in Z(G/H)$ with $x \neq e_{G/H}$. Then $\mathrm{ord}(x) = p^a$ for some $a \in \mathbb{N}$. We define now

$$y := x^{p^{a-1}}$$

so that $\mathrm{ord}(y) = p$. Hence, G/H contains an order of element p. Let $K' := \langle y \rangle$, which is a normal subgroup of G/H since y commutes with the elements of G/H (indeed, x, and thus y, belongs to $Z(G/H)$). Consider the canonical surjective homomorphism

$$\pi_H : G \longrightarrow G/H, \quad g \mapsto gH$$

and let $K := \pi_h^{-1}(K')$. Since $K' \ni e_{G/H}$ and $\mathrm{Ker}\, \pi_H = H$, it is immediate that $H \lhd K$. By the correspondence theorem, we also know that $K \lhd G$. We now need only show that $[K : H] = p$. By the first isomorphism theorem[1]

$$K/\mathrm{Ker}\, \pi_H = K/H \cong K'$$

[1] Rather, we view π_H as the map $\pi_H : K \longrightarrow G/H$ given by $k \mapsto kH$. Obviously, this is again a homomorphism of groups to which we can apply the first isomorphism theorem.

whence $[K : H] = p$, as was required. For the second part, we let $H_0 := \{e\}$ and note that H_0 is a proper subgroup of G. By the first part, we may choose a subgroup $H_1 \lhd G$, strictly containing H_0, with $[H_1 : H_0] = p$. If $H_1 = G$ then we are done. Otherwise, H_1 is a proper normal subgroup of G and therefore we may choose a subgroup $H_2 \lhd G$ with $H_2 \rhd H_1$ such that $[H_2 : H_1] = p$. If $H_2 = G$ then we shut off the proof. Proceeding in this way, we construct a sequence of normal subsets of G as in (3.1). Notice that $|H_1| = p$ whence it follows by induction that

$$|H_k| = [H_k : H_{k-1}] \cdot |H_{k-1}| = p \cdot p^{k-1} = p^k.$$

□

The second part of this theorem we will important in future sections. It will relate p-groups to what we will shortly call *solvable groups*.

We may further refine the statement of this theorem, as is shown in the following proposition.

PROPOSITION 3.3. *Let G be a p-group and H a proper subgroup of G. There exists a subgroup H^+ of G with $H^+ \supseteq H$ and $[H^+ : H] = p$. Moreover, if $H \neq \{e\}$, there exists a subgroup $H^- \subseteq H$ such that $[H : H^-] = p$.*

PROOF. We shall argue by induction on the order of G. If $|G| = p$ then the statement is obvious. Suppose now that the claim holds up to p^r and let G be of order p^{r+1}. By applying the previous theorem to the normal subgroup $\{e\}$, we may extract a normal subgroup J of G whose order is precisely p. We now distinguish two possible cases.

If $J \not\subseteq H$ then we define $H^+ := JH$; this is a subgroup of G since $J \lhd G$. It now suffices to compute

$$\left|H^+\right| = \frac{|J| \cdot |H|}{|J \cap H|} = j\,|H|\,.$$

That is, $[H^+ : H] = p$.

Suppose now that $J \subseteq H$. We consider the quotient group G/J which has order p^r. Noting that H/J is a proper subgroup of G/J, we may apply our induction hypothesis to obtain a subgroup K of G/J that contains H/J. We may choose this K such that $[K : H/J] = p$. Consider the canonical projection

$$\pi_J : G \to G/J, \quad g \mapsto gJ.$$

Let $H^+ := \pi_J^{-1}(K)$ (thus $H^+ \supseteq H$) and observe that

$$[H^+ : H] = \frac{|H^+| \,/\, |J|}{|H| \,/\, |J|} = \frac{|K|}{|H/J|} = p.$$

If $H \neq \{e\}$ then we need only make use of the second part of the previous theorem. □

LEMMA 3.4. *Let G be a group and suppose $H \lhd Z(G)$. If G/H is cyclic, then G is Abelian.*

PROOF. We pause for a moment and make sure that the statement makes sense. For G/H to have a group structure, we need $H \lhd G$. If $g \in G$ and $h \in H$ then $ghg^{-1} = h$ since h commutes with all elements of G. More generally, any subgroup of $Z(G)$ is normal in G.

Let us now assume that G/H is a cyclic group. More precisely, there exists an element xH in G/H such that $G/H = \langle xH \rangle$. Let $g_1, g_2 \in G$ be given. Then $g_1 \in x^i H$ and $g_2 \in x^j H$, for some $i, j \in \mathbb{N}$, since G is the disjoint union of (left)-cosets. It then follows that $g_1 = x^i h_1$ and $g_2 = x^j h_2$ for $h_1, h_2 \in H$. Since $H \subseteq Z(G)$:

$$g_1 g_2 = (x^i h_1)(x^j h_2) = (h_2 x^j)(h_1 x^i) = g_2 g_1.$$

This shows that G is Abelian. □

We now prove Cauchy's theorem for Abelian groups. The result for general groups is not very useful and the proof is incredibly tedious. In the case where G is Abelian, there exists an elegant proof for the theorem.

DEFINITION 9. Let G be a finite group and N a proper normal subgroup of G. We say N is a maximal normal subgroup if the only normal subgroup of G strictly containing N is G itself.

THEOREM 3.5 (Cauchy's Theorem). *Let G be a finite Abelian group and p a prime dividing the order of G. There exists an element in G of order p.*

PROOF. The proof is by way of induction on $|G|$. In the case $|G| = 2$ there is nothing to show since G has prime order and is therefore cyclic. Assume that the statement holds up to (and including) $n - 1$ where $n = |G|$. Let us now fix a maximal (proper) normal subgroup N of G.

If p divides $|N|$ we need only apply our induction hypothesis to obtain the desired element of G. Hence, we handle only the case where p does not divide $|N|$. Choose $x \in G \setminus N$ and let $B = \langle x \rangle$. Since G is Abelian, $B \lhd G$. Note now that BN is then a normal subgroup of G *strictly* containing N. Hence $BN = G$ and

$$p \mid \frac{|B| \cdot |N|}{|B \cap N|}$$

which implies that p divides $|B|$. In particular, $p \mid \text{ord}(x)$. Write $\text{ord}(x) = r = pt$ and then note that

$$\text{ord}(x^t) = \frac{pt}{\gcd(pt, t)} = p.$$

This concludes the proof. □

REMARK 3.1. We would like to point out that, in the proof, we only made use of the fact that G is Abelian to conclude that $B \lhd G$.

2. Sylow's Theorems

This section is devoted to Sylow's theorems which study the p-subgroups of finite groups. Throughout this section G will denote a group of order n, where $n = p^r m$ for a prime p and $r, m \in \mathbb{N}$ with $\gcd(p, m) = 1$. Given a subgroup H of G, we also recall that the normalizer of H is defined by

$$N_G(H) := \{g \in G : gH = Hg\}.$$

Note also that $H \lhd N_G(H)$.

THEOREM 3.6. *There exists a subgroup of order p^r in G.*

PROOF. We now proceed by induction on the order of G. If $|G| = 2$ then the result is clear as G must be cyclic (isomorphic to $\mathbb{Z}/2\mathbb{Z}$). Now let $|G| = n = p^r m$ and suppose the claim holds for all groups of order strictly less than n. There are now two cases to distinguish.

Suppose that p divides $|Z(G)|$, which we know to be Abelian. We invoke Theorem 3.5 to obtain an element $x \in Z(G)$ of order p. Consider the normal subgroup $N = \langle x \rangle \lhd G$ which has order p. The quotient group G/N will then have order $p^{r-1}m$. Applying the induction hypothesis to $p^{r-1}m$, one can extract a subgroup $K' < G/N$ of order p^{r-1}. Consider the canonical projection

$$\pi_N : G \longrightarrow G/N, \quad g \mapsto gN.$$

This is a surjective homomorphism of groups whose kernel is N. We now define $K := \pi_N^{-1}(K')$ which certainly contains N. Also, by the first isomorphism theorem

$$K/N \cong K'$$

which shows that $|K| = |K'| \cdot |N| = p^r$.

Suppose instead that p does not divide the order of $|Z(G)|$. By equation (2.5) there exists $x \notin Z(G)$ such that p does not divide

$$\frac{|G|}{\mathrm{C}(x)}$$

where $\mathrm{C}(x)$ is a proper subgroup of G since $x \notin Z(G)$. It follows that p^r divides the order of $\mathrm{C}(x)$. Applying the induction hypothesis to $\mathrm{C}(x)$, the proof is complete. □

This theorem is often referred to as the *existence part* of Sylow's theorems.

LEMMA 3.7. *Let P be a maximal p-subgroup of G and Q any p-subgroup. Then,*

$$P \cap Q = Q \cap N_G(P).$$

PROOF. If $m = 1$ then the result is clear. Otherwise, note that $P \cap Q \subseteq Q \cap N_G(P)$. For the reverse inclusion, define $A = N_G(P) \cap Q$ and note that A is a subgroup of $N_G(P)$ that

is itself a p-group. Since $P \lhd N_G(P)$ it follows that AP is a subgroup of $N_G(P)$. Hence,

$$|AP| = \frac{|A| \cdot |P|}{|A \cap P|}$$

which shows that AP is itself a p-group which contains A. Hence, $AP = P$ which implies that $A \subseteq P \cap Q$. □

THEOREM 3.8. *Every maximal p-subgroup of G has order p^r (and such a subgroup exists). Let n_p denote the number of maximal p-subgroups in G. Then,*

(1) $n_p \equiv 1 \pmod{p}$,

(2) $n_p \mid m$.

Maximal p-subgroups of G are then called p-Sylow subgroups.

PROOF. Let P be a p-Sylow subgroup of order p^r in G (such a subgroup certainly exists by our previous theorem). Let

$$S := \{P_1, P_2, \ldots, P_a\}$$

where $P_1 := P$ and P_j are conjugate to S. Since conjugation is an isomorphism, it follows that each element of S is a maximal p-subgroup of G as well. We now consider the action

$$G \times S \longrightarrow S, \quad (g, P_j) \mapsto gP_jg^{-1}.$$

Note that

$$a = |S| = |\mathrm{Orb}(P_1)| = \frac{|G|}{|\mathrm{Stab}(P_1)|} = \frac{|G|}{N_G(P_1)}$$

so that $a \mid m$ (since $N_G(P_1) \supseteq P_1$ which has order p^r). Let now Q be a maximal p-subgroup of G and consider the action determined by

$$Q \times S \longrightarrow S, \quad (q, P_j) \mapsto qP_jq^{-1}.$$

For j we have that

$$|\mathrm{Orb}(P_j)| = \frac{|Q|}{|\mathrm{Stab}(P_j)|} = \frac{|Q|}{|Q \cap N_G(P_j)|}.$$

Let now $Q = P_1$ whence for each j

$$|\mathrm{Orb}(P_j)| = \frac{|P_1|}{|\mathrm{Stab}(P_j)|} = \frac{|P_1|}{|P_1 \cap N_G(P_j)|} = \frac{|P_1|}{|P_1 \cap P_j|}.$$

Since the P_j's are distinct sets of the same order, $|\mathrm{Orb}(P_j)| = 1$ if $j = 1$ and is a positive power of p otherwise, Since S is the disjoint union of orbits, it follows that $a = 1 + tp$ for some $t \in \mathbb{Z}$, i.e. $a \equiv 1 \pmod{p}$.

We now claim every maximal p-subgroup of G is conjugate to P whence it will follow that $n_p = a$. To see this, suppose there exists a maximal p-subgroup Q that does not belong to S. Then for each j

$$|\mathrm{Orb}(P_j)| = \frac{|Q|}{|Q \cap P_j|}$$

which is always a proper power of p (since $P_j \cap Q$ is never equal to Q). This contradicts the fact that $a \equiv 1 \pmod{p}$. This concludes the proof. □

From Sylow's theorem we may deduce Cauchy's theorem for general groups.

COROLLARY 3.9 (Cauchy). *Let G be a group of order $n \geq 2$. If p is a prime dividing $|G|$, there exists an element of G having order p.*

PROOF. Let P be a p-Sylow subgroup. Since P is a p-group, the center of P is non-trivial. The proof is complete once we apply Cauchy's theorem for Abelian groups (Theorem 3.5) to $Z(P)$. □

2.1. Consequences of Sylow's Theorems: Groups of Order pq. We now explore a curious consequence of Sylow's theorems. Let $p, q > 0$ be primes with $p < q$ and assume that $p \nmid (q-1)$. We claim that if G is a group of order pq then G is Abelian. To this end, we require the following lemma.

LEMMA 3.10. *Let G be a finite group and d a divisor of $|G|$. Suppose there exists a unique subgroup H of order d in G. Then $H \lhd G$.*

PROOF. It suffices to check that $gHg^{-1} = H$ for all $g \in G$. First, note that given $g \in G$ the collection

$$gHg^{-1} = \left\{ghg^{-1} : h \in H\right\}$$

is a subgroup of G. Clearly, it contains e and

$$(gh_1g^{-1}) \cdot (gh_2g^1) = g(h_1h_2)g^{-1}.$$

Also, $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. Since H is the unique subgroup of order d, if we can show that $\left|gHg^{-1}\right| = d$ then it will follow that $gHg^{-1} = H$. Define a map

$$f : H \longrightarrow gHg^{-1}, \quad h \mapsto ghg^{-1}.$$

Then the above is clearly a bijection which completes the proof. □

We are now prepared to prove that G must be Abelian. The number of p-Sylow subgroups of G is given by n_p and must satisfy

$$n_p \equiv 1 \pmod{p}, \quad n_p \mid q.$$

Likewise, if n_q denotes the number of q-Sylow subgroups of G then

$$n_q \equiv 1 \pmod{q}, \quad n_q \mid p.$$

Write $n_q = 1 + kq$ for $k \in \mathbb{N}_0$ and note that $p < q$ implies (by virtue of $n_q \mid p$) that $n_q \leq q$. Hence, $n_q = 1$. Now, $n_p \mid q$ implies (since q is prime) that $n_p = 1$ or $n_p = q$. If $n_p = q$ then

$$q \equiv 1 \pmod{p}$$

which is a contradiction. Thus, $n_p = n_q = 1$. In particular, the Sylow subgroups of G (which exist) are unique. By the previous lemma, the p-Sylow subgroup and q-Sylow

subgroup, which we denote by P and Q respectively, are normal in G. Hence, PQ is a subgroup of G and

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{pq}{|P \cap Q|}.$$

The intersection $P \cap Q$ must be trivial since it is a subgroup of order dividing both p and q. Hence, $PQ = G$. Now, $P \cong \mathbb{Z}/p\mathbb{Z}$ and $Q \cong \mathbb{Z}/q\mathbb{Z}$ which shows that both P and Q are Abelian. If $x \in P$ and $y \in Q$ we must show that $xy = yx$. For this, it suffices to check that $xyx^{-1}y^{-1} = e$. Indeed,

$$xyx^{-1}y^{-1} = \underbrace{\left[xyx^{-1}\right]}_{\in Q} y^{-1} \in Q$$

and

$$xyx^{-1}y^{-1} = x \underbrace{\left[yx^{-1}y^{-1}\right]}_{\in P} \in P.$$

Thus, $xyx^{-1}y^{-1} \in P \cap Q = \{e\}$.

2.2. Consequences of Sylow's Theorems: Groups of Order p^2 and Unique p-Sylow Subgroups. In this subsection we study some structural properties that arise as a consequence of Sylow's theorems. We begin with groups of order p^2.

2.2.1. *Groups of Order p^2 are Abelian.* Let p be a prime and G a group of order p^2. We know from our theory on p-groups that $Z(G)$ is non-trivial. Thus, $|Z(G)|$ is either p or p^2. If $|Z(G)| = p^2$ we are done (then $G = Z(G)$). We thus assume that $|Z(G)| = p$. Now, the center of G is normal in G. This gives us a well defined quotient group $G/Z(G)$ which has order p. Thus, $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and is therefore cyclic. An application of Lemma 3.4 shows that G is Abelian.

2.2.2. *The case of $n_p = 1$ and elements of order p^l.* Here we consider a finite group G whose order is $p^r m$ for a prime p, $r \geq 1$ and m co-prime to p. Let $g \in G$ and suppose $\text{ord}(x) = p^l$ for some $l \in \mathbb{N}$. Clearly, $l \leq r$. Let us also assume that $n_p = 1$, i.e. there exists a unique p-Sylow subgroup, say P, in G. Can we guarantee that $g \in P$? The answer is *yes*.

Suppose that $g \notin P$ and recall that P must be a normal subgroup of G (it is the unique p-Sylow subgroup). The subgroup $Q := \langle g \rangle$ is then a subgroup of G different from P (in the sense that $Q \not\subseteq P$) whose order is precisely p^l. However, the product PQ is a subgroup of G with order precisely

$$\frac{|P| \cdot |Q|}{|P \cap Q|}.$$

This means that PQ is also a p-subgroup of G that strictly contains P. Hence, we have attained a contradiction.

3. Solvable Groups and The Jordan-Hölder Theorem

In this section we consider the composition of finite groups from a "new" perspective. Instead of studying subgroups of prime order, we consider subgroups of G that form "nice quotients".

DEFINITION 10. Let G be a group of finite order. A *normal series* in G is a strictly decreasing collection $\{G_i\})i = 0^n$ of subgroups of G such that

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_0 = \{e\}.$$

A *composition series* for G is a normal series $\{G_i\}_{i=1}^n$ such that for each i the quotient group G_{i-1}/G_i is a non-trivial[2] simple group.

Given a composition series for G, we shall call the quotients G_{i-1}/G_i, considered up to isomorphism and with multiplicity, the composition factors of G. A finite group G is called **solvable** if it has a composition series where each composition factor is Abelian.

LEMMA 3.11. *Let G be a finite group and $\{G_i\}_{i=0}^n$ be a normal series for G. This can be refined into a composition series for G. Moreover, if the G_{i-1}/G_i are Abelian then so are the quotients of the refinement. In this case, there exists a prime p such that*

$$G_{i-1}/G_i \cong \mathbb{Z}/p\mathbb{Z}$$

*for all G_{i-1}, G_i present in the **refinement**.*

PROOF. Since G is a set of finite cardinality, the length of a normal series is bounded above by some positive natural number. Hence, it suffices to show that any normal series that is not a composition series can be extended. To this end, suppose that we have a normal series for G

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

and let i be some index for which the quotient G_{i-1}/G_i is not simple. Thus, there exists a subgroup $\{e\} \subsetneq H' \subsetneq G_{i-1}/G_i$ that is normal in G_{i-1}/G_i. We now recall the existence of a surjective homomorphism

$$\pi_i : G_{i-1} \longrightarrow G_{i-1}/G_i, \quad g \mapsto gG_i.$$

We also know that $\operatorname{Ker} \pi_i = G_i$. If we define $H := \pi_i^{-1}(H')$ is follows that H is a subgroup of G_{i-1} containing $\operatorname{Ker} \pi_i = G_i$. By the correspondence theorem, it follows that

$$G_i = \operatorname{Ker} \pi_i \lhd H \lhd G_{i-1}.$$

Also, since π_i is surjective and $H' \subsetneq G_{i-1}/G_i$, one has $H \neq G_i$ and $H \neq G_{i-1}$. Let us now suppose that the quotients G_{i-1}/G_i were Abelian. It suffices to check that G_{i-1}/H and H/G_i are also Abelian. For the former, it is a consequence of the Correspondence Theorem that

$$G_{i-1}/H \cong \pi_i(G_{i-1})/\pi_i(H) = (G_{i-1}/G_i)/H'$$

[2] These quotients are always non-trivial since we assumed that the G_i decrease strictly.

which is certainly Abelian. Thus, G_{i-1}/H is Abelian. The first isomorphism theorem also yields

$$H/G_i \cong \pi_i(H) < G_{i-1}/G_i$$

which shows that H/G_i is Abelian. We will be done the proof if we can show that finite simple Abelian groups are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Let A be a finite simple Abelian group and choose a prime p dividing $|A|$. By Cauchy's theorem for Abelian groups, there exists an element $x \in A$ whose order is p. Consider $N = \langle x \rangle$, which is a normal subgroup of A. Thus, $N = A$ since A is simple and $N \supsetneq \{e\}$. □

We now state a technical lemma which will be central in the proof of Jordan's theorem. The proof is this lemma is painful and unenlightening, and as such we shall not give the proof.

LEMMA 3.12 (Zassenhaus). *Let $A \lhd A^*$ and $B \lhd B^*$ be subgroups of a group G. Then*

$$A(A^* \cap B) \lhd A(A^* \cap B^*), \quad B(B^* \cap A) \lhd B(B^* \cap A^*),$$

and

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Using this result, we will establish the following theorem:

THEOREM 3.13 (Jordan). *Let G be a finite group. Any two composition series for G have the same composition factors (considered with multiplicity).*

Let us first establish the following elementary result.

LEMMA 3.14. *Let C be a finite group and $A \lhd C$ such that C/A is non-trivial simple group. There does not exist a subgroup B such that $A \subsetneq B \subsetneq C$ and $A \lhd B \lhd C$.*

PROOF. The proof of this lemma is by contradiction. Assume we have such a normal subgroup B of C and consider the map

$$\pi_A : C \longrightarrow C/A, \quad c \mapsto cA.$$

We have already shown that π_A is a surjective homomorphism of groups whose kernel is A. Now, since B contains the A, which is the kernel of π_A, it follows from the Correspondence Theorem that $\pi_A(B) \lhd C/A$. Since C/A is a simple group, either $\pi_A(B) = \{A\}$ or $\pi_A(B) = C/A$. In the former, it would follows that $\pi_A(b) = A$ for all $b \in B$, which is to say that $A = B$. If instead $\pi_A(B) = C/A$ then, by the first isomorphism theorem,

$$C/A = \pi_A(B) \cong B/A.$$

Since C is a finite group, it follows that $|B| = |C|$ whence $B = C$. In either case, we obtain a contradiction. □

PROOF OF THEOREM 3.13. By Lemma 3.14, it suffices to show that any two normal series for a group G share a common refinement, since a composition series cannot be further refined.

To this end, suppose we have two families

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}, \tag{3.2}$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{e\} \tag{3.3}$$

for a pair $(n, m) \in \mathbb{N} \times \mathbb{N}$. For some fixed index i let us now define

$$G_{i,j} := G_{i+1}(G_i \cap H_j)$$

which is certainly contains G_{i+1} and is contained in G_i. Hence, since G_{i+1} is normal in G_i, it follows that $G_{i,j}$ is a subgroup of G_i. Furthermore,

$$G_{i,0} = G_{i+1}(G_i \cap H_0) = G_{i+1}(G_i \cap G) = G_i$$

and

$$G_{i,m} = G_{i+1}(G_i \cap \{e\}) = G_{i+1}.$$

It is also clear that $G_{i,j} > G_{i,j+1}$. As in Lemma 3.12, let $A = G_{i+1}$, $A^* = G_i$, $B = H_{j+1}$ and $B^* = H_j$. By this same lemma:

$$\begin{aligned} G_{i,j+1} = G_{i+1}(G_i \cap H_{j+1}) = A(A^* \cap B) \lhd A(A^* \cap B^*) &= G_{i+1}(G_i \cap H_j) \\ &= G_{i,j}. \end{aligned}$$

This allows us to "fill in" the gaps in the normal series (3.2). We hence obtain a new normal series for G given by $\{G_{i,j}\}_{i,j}$. Likewise for the series in (3.3), we define

$$H_{i,j} = H_{j+1}(H_j \cap G_i)$$

which will yield, by Lemma 3.12, an analogous refinement of (3.3). In this refinement one will have

$$H_j = H_{0,j} \rhd H_{1,j} \rhd \cdots \rhd H_{n,j} = H_{j+1}.$$

Now, lemma 3.12 then gives that

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)} = \frac{H_{j+1}(H_j \cap G_i)}{H_{j+1}(H_j \cap G_{i+1})} = \frac{H_{j,i}}{H_{j,i+1}}.$$

□

3.1. On Solvable Groups. Recall that a finite group G is called solvable if it has a composition series in which every composition factor is Abelian. There are several classes of groups which we would like to examine.

3.1.1. *Groups of order pq.* Suppose that G is a group of order pq, where p and q are distinct primes with $p < q$. Let n_q denote the number of q-Sylow subgroups of G. We know that $n_q \mid p$ so that $n_q = 1$ or $n_q = p$. By Sylow's theorems, it is also known that $n_q \equiv 1 \pmod{q}$. If $n_q = p$ then $n_p > 1$ so that

$$p = n_q = 1 + kq, \quad k \in \mathbb{N}.$$

But then, $p > kq \geq q$ which is absurd. Therefore G contains a unique q-Sylow subgroup, say, Q. But then Q is normal in G and G/N has order p. It follows that G/N is cyclic which shows that G is solvable.

3.1.2. *p-Groups are Solvable.* Suppose that p is a prime and G is a group of order p^r for some $r \in \mathbb{N}$. Then G is solvable. Indeed, this is trivial if $r = 1$. If $r > 1$ we need only apply the second part of Theorem 3.2 to obtain a normal series

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{e\}$$

where $[H_k : H_{k-1}] = p$ for every k. This means that each quotient H_k/H_{k-1} is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and, in particular, Abelian.

3.1.3. *Subgroups of Solvable Groups are Solvable.* Let G be a solvable finite group and K a subgroup of G. We claim that K is also solvable. Indeed, since G is solvable, there exists a composition series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

such that each quotient G_{i-1}/G_i is Abelian. We must now only construct such a series for K. First, note that

$$K = (K \cap G_0) \rhd (K \cap G_1) \rhd \cdots \rhd (K \cap G_n) = \{e\}.$$

This may not be a composition series, but if we can show the quotients are Abelian we will be done since our refinement procedure guarantees that the induced composition series will have Abelian quotients. By composition, we obtain a group homomorphism

$$K \cap G_{i-1} \longrightarrow G_{i-1} \longrightarrow G_{i-1}/G_i, \quad g \mapsto gG_i$$

whose kernel is $K \cap G_i$. By the first isomorphism theorem,

$$\frac{K \cap G_{i-1}}{K \cap G_i}$$

is isomorphic to a subgroup of G_{i-1}/G_i, which is Abelian. This concludes the proof.

We conclude this section by characterizing the automorphisms of cyclic groups. This covers, in particular, all groups of prime order.

PROPOSITION 3.15. *Let Q be a cyclic group of order q. Then* $\mathrm{Aut}(Q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$.

PROOF. Let $x \in Q$ be a generator of Q, i.e. $\operatorname{ord}(x) = q$. It follows that every element $g \in Q$ has a representation as x^a for some $a \in \mathbb{N}$. Furthermore, this a is uniquely determined modulo q. Let $f : G \longrightarrow G$ be a homomorphism. If $f(x)$ generates the group G then $\operatorname{ord}(f(x)) = q$. Then, f must be injective since

$$f(x^a) = f(x^b) \iff f(x)^a = f(x)^b \iff f(x)^{a-b} = e.$$

However, $f(x)^{a-b} = e$ if and only if $q \mid (a - b)$, which is to say that

$$a \equiv b \pmod{q}.$$

Thus, f is an automorphism if $f(x)$ generates Q. Conversely, let $f \in \operatorname{Aut}(Q)$. Then, by Proposition 1.26, it follows that $f(x)$ has order q which implies that $Q = \langle f(x) \rangle$. Thus, a homomorphism $f : Q \longrightarrow Q$ is an automorphism if and only if $f(x)$ generates G. This gives exactly $\varphi(q)$ possible automorphisms, where φ is the Euler totient function.

We now construct an explicit isomorphism $\Gamma : \operatorname{Aut}(Q) \longrightarrow (\mathbb{Z}/q\mathbb{Z})^\times$. Define this Γ by

$$\operatorname{Aut}(Q) \ni f \longmapsto a$$

where $f(x) = x^a$, and a is taken modulo q. Since f is an automorphism, $G = \langle x^a \rangle$ so that $\gcd(a, n) = 1$ by earlier results. This is a surjection since one can define an automorphism by letting $f(x) = x^a$ for any $a \in (\mathbb{Z}/q\mathbb{Z})^\times$. This map is injective because an automorphism is determined completely and uniquely by how it its value at x. That is, if $\Gamma(f) = \Gamma(g)$ then

$$f(x) = g(x)$$

so that $f \equiv g$. Finally, Γ is a group homomorphism. If $\Gamma(f) = a$ and $\Gamma(g) = b$ then there holds

$$(f \circ g)(x) = f(g(x)) = f(x^b) = f(x)^b = x^{ab}.$$

This means that $\Gamma(f \circ g) = ab$. This concludes the proof of this proposition. □

4. Semidirect Products

Let G and H be groups. There is a natural group structure one can impose on the Cartesian product $G \times H$. Certainly, we define

$$(g_1, h_1) \odot (g_2, h_2) := (g_1 g_2, h_1 h_2).$$

From the group structures of both G and H, it is clear this makes $G \times H$ into a group. We then call $G \times H$ (together with the above operation) the *direct product* of G and H.

Let us now take a step back and suppose we are given a group G and two subgroups H, K of G. Let us also assume that $H \lhd G$ and $K \lhd G$. From earlier results, we know that HG is a subgroup of G. If we also assume that $H \cap K = \{e\}$, we can conclude something special about the elements of G.

LEMMA 3.16. *Let G be a group and suppose $H, K \lhd G$ are such that $G = HK$ and $H \cap K = \{e\}$. Every $g \in G$ has a unique representation as $g = hk$ for some $h \in H$ and $k \in K$.*

PROOF. The existence of h and k, for a given g, is clear. Let $g \in G$, $h, h' \in H$ and $k, k' \in K$ be such that

$$g = hk = h'k'.$$

This implies that $h^{-1}h'k' = k \in K$. Thus, $h^{-1}h' \in K \cap H$ so that $h^{-1}h' = e$. This implies that $h = h'$. A symmetric argument gives $k = k'$. Thus, we have the uniqueness. □

We now give the subsequent result, which is our first stepping stone in to the notion of a semidirect product of groups.

PROPOSITION 3.17. *Let G be a group and $H, K \lhd G$. Suppose*

(1) $G = HK$,
(2) $H \cap K = \{e\}$.

Then $G \cong H \times K$.

PROOF. By Lemma 3.16, every element $g \in G$ may be uniquely expressed as hk, where $(h, k) \in H \times K$. Let us now define a map

$$\psi : G \longrightarrow H \times K$$

by taking $g \in G$ to this unique pair (h, k). Obviously, by uniqueness, this is a well defined map. Suppose $g_1 = h_1k_1$ and $g_2 = h_2k_2$ are elements of G. Note then that

$$g_1g_2 = h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_1^{-1}k_1k_2 = (h_1h_2)\, h_2^{-1}k_1h_2k_1^{-1}\, (k_1k_2)\,. \tag{3.4}$$

Note now that

$$\underbrace{h_2^{-1}k_1h_2}_{\in K}\, k_1^{-1} \in K \quad \text{and} \quad h_2^{-1}\, \underbrace{k_1h_2k_1^{-1}}_{\in H} \in H$$

whence $h_2^{-1}k_1h_2k_1^{-1} \in H \cap K = \{e\}$. Using (3.4), we then conclude that ψ is a homomorphism of groups. Also,

$$\operatorname{Ker} \psi = \{g = hk : h = e,\, k = e\} = \{e\}$$

which shows that ψ is injective. Since ψ is clearly a surjection, it follows that G is isomorphic to $H \times K$. □

The conditions in the statement of Proposition 3.17 are precisely those that we wish to generalize. By relaxing one of these conditions, we will obtain the notion of a semi-direct product.

DEFINITION 11. Let G be a group and H, K subgroups of G. Suppose

(1) $H \lhd G$,
(2) $H \cap K = \{e\}$,
(3) $G = HK$.

Then we say G is the semidirect product of H and K, written $G = H \rtimes K$.

This notion is simple enough, but there is an important distinction to be made. Given a semidirect product $H \rtimes K$ one cannot fully recover the structure of G. The "missing" piece of information is a homomorphism of groups

$$\phi : K \longrightarrow \mathrm{Aut}(H),$$

where $\mathrm{Aut}(H)$ is the group of automorphisms of H. We will show that, the semidirect products are determined by this ϕ. Before, let us introduce some notation. For each $k \in K$ the map $\phi(k)$ is an automorphism of H. It will be more convenient to write $\phi(k)$ as ϕ_k, since $\phi(k)$ takes $h \in H$ as an argument.

LEMMA 3.18. *Let $G = H \rtimes K$. For $k \in K$ define*

$$\phi_k : H \longrightarrow H, \quad h \mapsto khk^{-1}.$$

For each k the map ϕ_k is an automorphism of H and the association $k \mapsto \phi_k$ is a group homomorphism.

PROOF. First, ϕ_k is well defined since $H \lhd G$. Indeed, by the normality of H, $khk^{-1} \in H$ for every $h \in H$ and $k \in K$. Let $k_1, k_2 \in K$ and note that for $h \in H$

$$\phi_{k_1k_2}(h) = (k_1k_2)h(k_1k_2)^{-1} = k_1k_2hk_2^{-1}k_1^{-1} = \phi_{k_1}(\phi_{k_2}(h)) = (\phi_{k_1} \circ \phi_{k_2})(h).$$

□

REMARK 3.2. Let $G = H \rtimes K$ and $\phi : K \longrightarrow \mathrm{Aut}(H)$ be as in the proof of the above above. Then for any $h_1k_1, h_2k_2 \in HK$ there holds

$$h_1k_1h_2k_2 = h_1 \underbrace{k_1h_2k_1^{-1}}_{=\phi_{k_1}(h_2)} k_1k_2 = k_1\phi_{k_1}(h_2)h_1h_2. \tag{3.5}$$

Conversely, we wish to determine whether any such homomorphism ϕ induces a semidirect product. As we shall see, this is done by defining an operation according the the right hand side of (3.5).

THEOREM 3.19. *Suppose H and K are groups and that $\phi : K \longrightarrow \mathrm{Aut}(H)$ is a group homomorphism. There exists a semidirect product "based on the information in ϕ". This group will be denoted $H \rtimes_\phi K$.*

PROOF. The idea is to construct an operation on $H \times K$ involving ϕ. Given $(h, k), (h', k') \in H \times K$ we define

$$(h, k)(h', k') = (h\phi_k(h'), kk').$$

Before we proceed, we show that this defines a valid group operation on $H \times K$. Let $(h_1, k_1), (h_2, k_2)$ and (h_3, k_2) be elements of $H \times K$ and observe that

$$\begin{aligned}
\left[(h_1, k_1)(h_2, k_2)\right](h_3, k_3) &= (h_1\phi_{k_1}(h_2), k_1k_2)(h_3, k_3) \\
&= (h_1\phi_{k_1}(h_2)\phi_{k_1k_2}(h_3), k_1k_2k_3) \\
&= \left(h_1\phi_{k_1}\left(h_2\phi_{k_2}(h_3)\right), k_1k_2k_3\right) \\
&= (h_1, k_1)\left(h_2\phi_{k_2}(h_3), k_2k_3\right) \\
&= (h_1, k_1)\left[(h_2, k_2))(h_3, k_3)\right].
\end{aligned}$$

This verifies associativity. There is an obvious candidate for the inverse:

$$e := (e_H, e_K).$$

If $(h, k) \in G \times K$ then

$$(h, k)(e_H, e_K) = (h\phi_k(e_H), ke_K) = (he_H, k) = (h, k)$$

and likewise

$$(e_H, e_K)(h, k) = (e_H\phi_{e_K}(h), e_Kk) = (e_Hh, k) = (h, k).$$

Finally, we fix $(h, k) \in H \times K$ and show that is has an inverse in $H \times K$. Certainly, consider the element

$$(h, k)^{-1} = (\phi_{k^{-1}}(h^{-1}), k^{-1}) \in H \times K.$$

A direct calculation gives

$$(h, k)(h, k)^{-1} = (h\phi_{kk^{-1}}(h^{-1}), kk^{-1}) = (h\phi_{e_K}(h^{-1}), e_K) = (hh^{-1}, e_K) = e$$

and

$$\begin{aligned}
(h, k)^{-1}(h, k) = \left(\phi_{k^{-1}}(h^{-1}), k^{-1}\right)(h, k) &= (\phi_{k^{-1}}(h^{-1})\phi_{k^{-1}}(h), e_K) \\
&= (\phi_{k^{-1}}(e_H), e_K) \\
&= e.
\end{aligned}$$

What is important is to note that we have the natural associations

$$H \cong \{(h, e_K) : h \in H\} \quad \text{and} \quad K \cong \{(e_H, k) : k \in K\}.$$

Under these associations, it is indeed true that $H \times K = HK$. Also, it is clear that $H \cap K = e = (e_H, e_K)$. It remains only to check that, under this identification, $H \lhd H \times K$. This is easy, if $(h, k) \in H \times K$ and $(\bar{h}, e_K) \in H$ then

$$\begin{aligned}
(h, k)(\bar{h}, e_K)(h, k)^{-1} = (h, k)(\bar{h}, e_K)(\psi_{k^{-1}}(h^{-1}), k^{-1}) &= (h, k)\left(\bar{h}\psi_{k^{-1}}(h^{-1}), k^{-1}\right) \\
&= \left(h\psi_k\left(\bar{h}\psi_{k^{-1}}(h^{-1})\right), e_K\right)
\end{aligned}$$

where

$$h\psi_k\left(\bar{h}\psi_{k^{-1}}(h^{-1})\right) = h\psi_k(\bar{h})h^{-1}.$$

□

Having established this method of constructing semidirect products, we wish to show that all semidirect products arise in this way from a homomorphism ϕ.

THEOREM 3.20. *Let $G = H \rtimes K$. There exists a homomorphism $\phi : K \longrightarrow \mathrm{Aut}(H)$ such that $G \cong H \rtimes_\phi K$.*

PROOF. Let $k \mapsto \phi_k$ be as in Lemma 3.18. We will show that $H \rtimes_\phi K \cong H \rtimes K$. Consider the map

$$\Gamma : H \rtimes_\phi K \longrightarrow H \rtimes K, \quad (h,k) \mapsto hk.$$

From Lemma 3.16 we know that Γ is a bijective map. It therefore remains only to check that Γ is a homomorphism of groups. Let (h,k) and (h',k') be elements of $H \rtimes_\phi K$. Note that

$$(h,k)(h',k') = (h\phi_k(h'), kk') = (hkh'k^{-1}, kk') \overset{\Gamma}{\mapsto} hkh'k'.$$

Furthermore,

$$\Gamma(h,k) \cdot \Gamma(h',k') = (hk) \cdot (h'k') = hkh'k'.$$

□

PROPOSITION 3.21. *Let H and K be groups. Then $H \times K = H \rtimes_\phi K$ if and only if ϕ is the trivial homomorphism.*

PROOF. Suppose that ϕ is the trivial homomorphism, i.e. ϕ_k is simply the identity map $H \longrightarrow H$. Then, given any two pairs $(h,k), (h',k')$ in $H \times K$ one has

$$(h,k)(h',k') = (h\phi_k(h'), kk') = (hh', kk').$$

Conversely, assume $H \times K = H \rtimes_\phi K$. We will show that $\phi_k \equiv \mathbf{1}_H$ for fixed $k \in K$. Indeed, if $k \in K$ is fixed and $h, h' \in H$ are given,

$$(h\phi_k(h'), k) = (h,k)(h', e_K) = (hh', k).$$

This implies that $h\phi_k(h') = hh'$ so that $\phi_k(h') = h'$. Since h' was arbitrary, it follows that $\phi_k \equiv \mathbf{1}_H$. □

4.1. Application: Groups of Order pq. Let us once again revisit a group G of order pq, where p, q are distinct primes with $p < q$. In §2.1 of Chapter 3, we saw that G must be Abelian if $p \nmid (q-1)$. We now consider the case where $p \mid q-1$. Let Q be a q-Sylow subgroup of G. By Sylow's theorems,

$$n_q \mid p \quad \text{and} \quad n_q = 1 + mq$$

for some $m \in \mathbb{N}_0$. If $n_q \neq 1$ then $n_q = p$ so that $p = 1 + mq$ for some $m \geq 1$. This would imply that $p \geq q$, which is a contradiction. Hence, $n_q = 1$ so that G contains a single q-Sylow subgroup. Hence, Q is normal in G. If P is p-Sylow subgroup then $Q \cap P = \{e\}$ so that $QP = G$. This means that $G = Q \rtimes P$. We already know that $Q \cong \mathbb{Z}/q\mathbb{Z}$ and $P \cong \mathbb{Z}/p\mathbb{Z}$. We therefore, without loss of generality, take

$$Q = \mathbb{Z}/q\mathbb{Z}, \quad P = \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

Recall that $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$. Since $p \mid q-1$, there exists an element $h \in (\mathbb{Z}/q\mathbb{Z})^\times$ of order p. We now define a map which takes

$$\mathbb{Z}/p\mathbb{Z} \ni 1 \mapsto \phi_1$$

where $\phi_1 : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ is given by $\phi_1(x) = hx$. It is easy to check that $\phi_1 \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Since 1 generates $\mathbb{Z}/p\mathbb{Z}$, this association generates a homomorphism of groups $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. We shall now show that the semidirect product

$$\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$$

is non-Abelian. Consider the elements $(a,0)$ and $(0,b)$ in this semidirect product. We directly compute (recalling that $\mathbb{Z}/n\mathbb{Z}$ is considered as a group with respect to addition!)

$$(a,0)(0,b) = (a\phi_0(0), b) = (a,b)$$

and

$$(0,b)(a,0) = (\phi_b(a), b).$$

If $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ were Abelian, then $\phi_b(a) = a$ for all $a \in \mathbb{Z}/q\mathbb{Z}$ and all $b \in \mathbb{Z}/p\mathbb{Z}$. That is, if $\phi_b \equiv \mathbf{1}$ for all $b \in \mathbb{Z}/p\mathbb{Z}$. On the other hand, $\phi_1 = f_h$ which is non-constant by construction. This means that $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$ is non-Abelian.

We now claim that any other non-Abelian semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$. Consider the map ψ_1, which is an automorphism of $\mathbb{Z}/q\mathbb{Z}$. By Proposition 1.17, $\mathrm{ord}(\psi_1) \leq p$. Note that ψ_1 cannot be the trivial automorphism of $\mathbb{Z}/q\mathbb{Z}$. Indeed, 1 generates the group $\mathbb{Z}/p\mathbb{Z}$, and thus ψ is completely determined by ψ_1. Since ψ_1 is not the identity we must have $\mathrm{ord}(\psi_1) = p$.

By Proposition 3.15, we know that $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ is cyclic. Proposition 1.9 then guarantees the existence of a unique subgroup of order p in $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. This subgroup must be precisely $\langle \phi_1 \rangle$, which must then contain ψ_1. This means that we may choose a natural number r co-prime to p such that $\psi_1 = \phi_1^r = \phi_r$.

Define

$$\mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}, \quad (a,b) \mapsto (a, rb).$$

This map is injective since $(a, rb) = (a', rb')$ if and only if $a = a'$ and $b = b'$. Since it is an injective map between two sets of the same cardinality (the underlying set of both groups is $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$). it follows that the function is a bijection. We now show that this association is in fact a homomorphism of groups.

$$(a,b)(a',b') = (a + \psi_b(a'), b + b') \mapsto (a + \psi_b(a'), r(b + b')).$$

On the other hand,

$$(a,b) \mapsto (a, rb), \quad (a',b') \mapsto (a', rb')$$

so that

$$(a, rb)(a', rb') = (a + \phi_{rb}(a'), r(b + b')) = (a + \phi_b^r(a'), r(b + b')) \\ = (a + \psi_b(a'), r(b + b')).$$

We have established the following:

THEOREM 3.22. *Let p, q be distinct primes with $p < q$. There exists a non-Abelian group of order pq. Moreover, this group is unique up to isomorphism.*

4.1.1. *Does there exist a non-Abelian group of order* 165 *containing a subgroup isomorphic to* $\mathbb{Z}/55\mathbb{Z}$*?*

5. Exercises

This section comprises of exercises related to the topics explored in this chapter. The reader is advised to solve the questions on their own, and should only consult the solutions at the end of this book as a last resort.

EXERCISE 3.1. Recall that a group $\mathfrak{B}$ is called a *boolean group* provided $b^2 = e$ for every $b \in \mathfrak{B}$. In Exercise 1.3 we showed that every boolean group is Abelian. Prove that $\mathfrak{B}$ has order 2^n for some $n \geq 1$.

EXERCISE 3.2. Let G be a finite p-group and H a subgroup of G with $H \neq \{e\}$.

(1) Give a class equation for H.
(2) Prove, using (1), that $H \cap Z(G) \supsetneqq \{e\}$.

EXERCISE 3.3. Let G be a finite p-group and $H \neq \{e\}$ a subgroup of G. Prove that there exists a normal subgroup H^- of G such that

$$H^- \subseteq H \quad \text{and} \quad [H : H^-] = p.$$

EXERCISE 3.4. Prove that if G is a group of order pqr, where $p < q < r$ are primes, then G has a normal Sylow subgroup.

EXERCISE 3.5. Let G be a finite group and H a normal subgroup of G. Let P be a p-Sylow subgroup for some prime p dividing $|G|$. Show that $P \cap H$ is a maximal p-subgroup of H (where we, exceptionally, allow the case $\{e\}$). Furthermore, show that HP/H is a p-Sylow subgroup of G/H.

EXERCISE 3.6. Find two isomorphic finite groups, sharing the same composition factors, where exactly one of the two groups is Abelian.

EXERCISE 3.7. Let $n \geq 1$ be an integer and define for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ the map

$$f_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto ax.$$

Prove that $f_a \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

EXERCISE 3.8. Let $n \in \mathbb{N}$. Prove that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

EXERCISE 3.9. Let $G = N \rtimes_\phi B$. Show that G is Abelian if and only if N and B are Abelian and ϕ is the trivial homomorphism.

EXERCISE 3.10. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. Prove that the center of G is non-trivial. More generally, show that $Z(G)$ contains the 11-Sylow subgroup of G.

EXERCISE 3.11. Let G be a group of order 385.

(1) Show that the 7 and 11 Sylow subgroups are normal in G.

(2) Show that the 7-Sylow subgroup is contained in the center of G.

EXERCISE 3.12. Does there exist a non-Abelian group G of order 165 containing a subgroup isomorphic to $\mathbb{Z}/55\mathbb{Z}$?

EXERCISE 3.13. Let G be a group of order pqr, where p, q and r are distinct primes. Show that G is solvable.

Chapter 4

Rudiments of Representation Theory

In this chapter we study a very special way of representing groups. More precisely, we will view the elements of finite groups as automorphisms of finite dimensional vector spaces. This point of view embodies group theory with the richness of linear algebra.

1. The Setup

Let V be a finite dimensional vector space over $\mathbb{C}$, which we will either call a $\mathbb{C}$-vector space or a complex vector space. An automorphism of V is a bijective linear map $V \longrightarrow V$; the collection of all automorphisms of V will be denoted by $\mathrm{Aut}(V)$. It is easy to see that $\mathrm{Aut}(V)$ forms a group under composition.

DEFINITION 12. Let G be a finite group. A *finite dimensional linear representation* of G is a pair (ρ, V), where V is a finite dimensional $\mathbb{C}$-vector space and

$$\rho : G \longrightarrow \mathrm{Aut}(V)$$

is a homomorphism of groups. For the sake of simplicity, we shall say that (ρ, V) is a **representation** of G.

Given two representations (ρ, V) and (τ, W) of a group G, a morphism of representations is a linear map $T : V \longrightarrow W$ such that

$$T \circ \rho(g) \equiv \tau(g) \circ T, \quad \forall g \in G.$$

An isomorphism of representations is simply a bijective morphism of representations. We shall write $\rho \cong \tau$ to say that there exists a bijective morphism of representations for (ρ, V) and (τ, W). Note that $\rho \cong \tau$ implies that $V \cong W$, in the sense of vector spaces.

Given such representations, it is common to denote by $\mathrm{Hom}(V,W)$ the collection of all linear maps $V \longrightarrow W$. We use the notation $\mathrm{Hom}_G(V,W)$ to denote the collection of all *morphisms of representations*. Then, $\mathrm{Hom}_G(V,W) \subseteq \mathrm{Hom}(V,W)$.

DEFINITION 13. Let (ρ, V) be a representation of a finite group G. A *sub-representation* of G is a vector subspace $W \subseteq V$ such that

$$\rho(g)(W) \subseteq W, \quad \forall g \in G.$$

In this case, we denote by (ρ, W) this sub-representation.

The notation (ρ, W) is no mistake. Since $\rho(g)$ is a bijection $V \longrightarrow V$ for all g, it follows from $\rho(g)(W) \subseteq W$ that, in fact, $\rho(g)(W) = W$. Hence, $\rho(g)$ also gives an automorphism of W.

DEFINITION 14. A representation (ρ, V) of a group G is called irreducible if the only sub-representations (ρ, W) are such that $W = \{\mathbf{0}\}$ or $W = V$.

Let now (ρ, V) and (τ, W) be two representations of a group G. Recall that $V \oplus W$ is a $\mathbb{C}$-vector space, of dimension $\dim(V) + \dim(W)$, in its own right. Define now

$$(\rho \oplus \tau)(g) := (\rho(g), \tau(g))$$

which is an automorphism of $V \oplus W$, when applied in the natural way. The representation $(\rho \oplus \tau, V \oplus W)$ is called the direct sum of the representations (ρ, V) and (τ, W). Of course, given a finite family $(\rho_1, V_1), \ldots, (\rho_N, V_N)$ of representations of G, one can construct in an analogous way the representation $\bigoplus_1^N \rho_j$ on $\bigoplus_1^N V_j$.

PROPOSITION 4.1. *Let (ρ, V) and (τ, W) be representations of a finite group G and let $T : V \longrightarrow W$ be a morphism of representations. Then* $\mathrm{Ker}\, T$ *is a sub-representation of V and* $\mathrm{Im}(T)$ *is a sub-representation of W.*

PROOF. We begin by showing that $(\rho, \mathrm{Ker}\, T)$ is a sub-representation, i.e. that $\rho(g)(\mathrm{Ker}\, T) \subseteq \mathrm{Ker}\, T$ for all $g \in G$. Let $v \in \mathrm{Ker}\, T$, then since $\tau(g)$ is an automorphism of W for each g

$$(T \circ \rho(g))(v) = (\tau(g) \circ T)(v) = \tau(g)(\mathbf{0}_W) = \mathbf{0}_W.$$

This establishes the fact that $\rho(g) \in \mathrm{Ker}\, T$. Now, we claim that $(\tau, \mathrm{Im}(T))$ is a sub-representation. This is to say that $\tau(g)(w) \in \mathrm{Im}(T)$ for each $w \in \mathrm{Im}(T)$. To see that this is so, note that $w = T(v)$ for some $v \in V$ whence

$$\tau(g)(w) = (\tau(g) \circ T)(v) = (T \circ \rho(g))(v) = T(v'),$$

where $v' = \rho(g)(v) \in V$. Hence, $\tau(g)(w) \in \mathrm{Im}(t)$ as was required. □

DEFINITION 15. If G is a group and (ρ, V) is a representation of G, we define

$$V^G := \{v \in V : \rho(g)v = v, \forall g \in G\}.$$

V^G is called the space of g-invariant vectors.

Since $\rho(g)$ is a linear map for all g, it is clear that V^G is itself a vector space over $\mathbb{C}$ and a subspace of V. Note that if $v \in V$ then

$$\rho(g)v = v \in V$$

so that (ρ, V^G) is a *sub-representation* of (ρ, V).

2. Preliminary Results and Canonical Representations

We now study basic results concerning representations and introduce two important representations: the standard and regular representations.

LEMMA 4.2. *Let (ρ, V) be an irreducible representation of a finite group G. Then either $V^G = \{0\}$ or $V = V^G$. In this last case, V is a one dimensional vector space.*

PROOF. Clearly, $V^G = V$ or $V^G = \{0\}$. Suppose that $V^G = V$ and let $v \in V$ be a non-zero vector. Define $S = \mathrm{Span}_{\mathbb{C}}(v)$, which is a vector subspace of V. We now claim that (ρ, S) is a sub-representation. If $g \in G$ and $w \in S$,

$$\rho(g)(w) = w$$

whence $W = V^G = V$. □

2.1. Standard Representation. Let $n \in \mathbb{N}$ and consider S_n, the permutation group on n-letters. Then, each $\sigma \in \mathsf{S}_n$ is merely a bijection

$$\{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}.$$

We will now construct a representation $(\rho^{\mathsf{st}}, \mathbb{C}^n)$ which we will call the standard representation (of S_n). Fix now a permutation $\sigma \in \mathsf{S}_n$ and let $\rho^{\mathsf{st}}(\sigma)$ be the linear map $\mathbb{C}^n \longrightarrow \mathbb{C}^n$ defined by

$$e_i \mapsto e_{\sigma(i)},$$

where the family $\{e_i\}_{i=1}^n$ is the standard basis of $\mathbb{C}^n$. Of course, it follows that $\rho^{\mathsf{st}}(\sigma)$ is an injective endomorphism of $\mathbb{C}^n$, and thus is an automorphism of $\mathbb{C}^n$.

Two important subspaces are the following:

$$U_0 := \left\{ (x_1, x_2, \ldots, x_n) : \textstyle\sum_{j=1}^n x_j = 0 \right\}, \tag{4.1}$$

$$U_1 := \mathrm{Span}_{\mathbb{C}}(\{(1, 1, \ldots, 1)\}). \tag{4.2}$$

PROPOSITION 4.3. *Let $n \geq 2$. Then U_0 is an irreducible $n-1$ dimensional sub-representation of S_n.*

PROOF. It is clear that $\dim(U_0) = n-1$. If $n = 2$ then the claim is clear as U_0 has dimension 1. Assume $n > 2$ and let $U' \subseteq U_0$ be a non-trivial sub-representation.

First suppose U' contains a vector with exactly two non-zero coordinates. After rescaling by a complex number, we may assume that

$$x = (0, \ldots, 1, \ldots, -1, \ldots, 0).$$

Since U' is closed under the action of $\rho^{\mathsf{st}}(\sigma)$ for $\sigma \in \mathsf{S}_n$, every vector of the form $e_i - e_j$ (where $i \neq j$) belongs to U'. Since such vectors span U_0, it follows that $U_0 = U'$.

By this argument, it is clear that it suffices to check that U' contains a vector with exactly two non-zero terms. Without loss of generality, let $x \in U'$ and assume x contains (at least) 3 non-zero entries. We can write

$$x = (1, x_2, x_3, \ldots, x_n), \quad \sum_{j=1}^{n} x_j = 0.$$

We may also assume that $x_2 \notin \{0, 1\}$ and $x_3 \neq 0$. Consider

$$y = \frac{1}{x_2}(x_2, 1, x_3, \ldots, x_n)$$

and notice that

$$U' \ni x - y = \left(0, x_2 - \frac{1}{x_2}, x_3 - \frac{x_3}{x_2}, \ldots, \right).$$

Clearly, $x - y$ has more non-zero terms than x. However, the third coordinate is non-zero (and thus $x - y$ has at least two non-zero terms). Repeating this procedure until we reach a vector with exactly two non-zero coordinates, the proof is complete. □

2.2. The Regular Representation. The regular representation applies to finite groups, unlike the standard representation which is used when considering the permutation group on n-letters. Let G be a finite group of order n. Cayley's theorem yields an embedding[1]

$$G \hookrightarrow \mathsf{S}_n.$$

Now, the standard representation ρ^{st} of S_n attaches to each permutation σ an automorphism of $\mathbb{C}^n$ via a group homomorphism. By composition, we obtain a group homomorphism

$$G \longrightarrow \mathrm{Aut}(\mathbb{C}^n) \cong \mathsf{GL}_n(\mathbb{C}).$$

The homomorphism described above will be labeled ρ^{reg}. The homomorphism described by Cayley's theorem is obtained by left multiplication. Thus, the permutation of the basis elements will fix an e_j if and only if σ is the identity map.

[1] In the context of groups, this means an injective homomorphism of groups!

3. Character Groups

This brief section explores the notion of the character group accompanying some group G. Let us fix a group G; the *character group* of G, which we denote G^*, is the collection of all homomorphisms $\rho : G \longrightarrow \mathbb{C}^\times$. Recall that $\mathbb{C}^\times$ is a group under multiplication that consists of all non-zero complex numbers. Therefore,

$$G^* := \mathrm{Hom}(G, \mathbb{C}^\times).$$

We endow G^* with multiplication in $\mathbb{C}^\times$. That is, for $\rho, \tau \in G^*$ we define a $\rho\tau$ to be the map

$$(\rho\tau)(g) := \rho(g) \cdot \tau(g) \in \mathbb{C}^\times.$$

We must now make sure that this new map $\rho\tau$ is a homomorphism $G \longrightarrow \mathbb{C}^\times$. Indeed, if $g, h \in G$ then

$$\begin{aligned}(\rho\tau)(gh) = \rho(gh) \cdot \tau(gh) = \rho(g) \cdot \rho(h) \cdot \tau(g) \cdot \tau(h) &= \rho(g) \cdot \tau(g) \cdot \rho(h) \cdot \tau(h) \\ &= (\rho\tau)(g) \cdot (\rho\tau)(h).\end{aligned}$$

The obvious identity of the group is the map $\mathbf{1}_G(g) = 1$. The inverse to $\rho \in G^*$ is simply the homomorphism

$$\rho^{-1}(g) := (\rho(g))^{-1}.$$

The same argument as above shows that $\rho^{-1} \in G^*$ whenever ρ is.

Some interesting properties now in order. First, note that although G may not be Abelian, its character group G^* is. Certainly, let $\rho, \tau \in G^*$ and fix $g \in G$. Then

$$(\rho\tau)(g) = \rho(g) \cdot \tau(g) = \tau(g) \cdot \rho(g) = (\tau\rho)(g).$$

That is, $\rho\tau \equiv \tau\rho$.

PROPOSITION 4.4. *Let G and H be groups. Then $(G \times H)^* \cong G^* \times H^*$.*

PROOF. Let us identify G with $G \times \{e_H\}$ and H with $\{e_G\} \times H$. Then, every element $f \in G^*$ is a homomorphism $G \times H \longrightarrow \mathbb{C}^\times$. Let us define

$$\Gamma : (G \times H)^* \longrightarrow G^* \times H^*, \quad f \mapsto \left(f_{|G}, f_{|H}\right).$$

We check that this is well defined, i.e. that $\Gamma(f) \in G^* \times H^*$. By symmetry, it suffices to check that $f_{|G} \in G^*$ if $f \in (G \times H)^*$. If $g \in G$, we associate it to $(g, 1)$ so that

$$f_{|G}(g) = f(g, 1) \in \mathbb{C}^\times.$$

Also, if $g_1, g_2 \in G$ then

$$f_{|G}(g_1 g_2) = f(g_1 g_2, 1) = f(g_1, 1) \cdot f(g_2, 1) = f_{|G}(g_1) \cdot f_{|G}(g_2).$$

Now, we check that Γ is an isomorphism of groups. Since it is clearly a homomorphism, it remains only to make sure that Γ is bijective. Given $(f, f') \in G^* \times H^*$ we can reconstruct an element of $(G \times H)^*$ by defining

$$F(g, h) := f(g) \cdot f'(h).$$

Conversely, if $\Gamma(f) = \Gamma(f')$ then

$$f_{|G} \equiv f'_{|G} \quad \text{and} \quad f_{|H} \equiv f'_{|H}.$$

Since $f(g,h) = f_{|G} f_{|H}$, it follows that Γ is injective. □

4. Characters of Representations

Let (ρ, V) be a representation of some finite group G. The character of (ρ, V) is defined as

$$\chi_\rho : G \longrightarrow \mathbb{C}, \quad g \mapsto \mathrm{Tr}(\rho(g)).$$

This certainly makes sense as $\rho(g)$ is an automorphism of V and hence can be represented by a matrix in some basis of V. Moreover, the trace is independent of choice of basis which shows that the above is well defined.

THEOREM 4.5. *The character function χ_ρ depends only on ρ up to isomorphism. If $g, h \in G$ then*

$$\chi_\rho(g) = \chi_\rho(hgh^{-1}). \tag{4.3}$$

Furthermore, if (τ, W) is another representative of G,

$$\chi_{\rho\oplus\tau} \equiv \chi_\rho + \chi_\tau, \quad \chi_\rho(e) = \dim(V) \quad \textit{and} \quad \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

PROOF. Suppose that $\rho \cong \tau$ for some representation (τ, V) of G. The definition then states that there exists some invertible matrix M such that

$$M\rho(g)M^{-1} = \tau(g), \quad \forall g \in G.$$

In the above we are viewing $\rho(g)$ and $\tau(g)$ as elements of $\mathsf{GL}_n(\mathbb{C})$. Thus, since M is a change of basis matrix, it follows by invariance of the trace that

$$\chi_\tau(g) = \mathrm{Tr}(\tau(g)) = \mathrm{Tr}(M\rho(g)M^{-1}) = \mathrm{Tr}(\rho(g)) = \chi_\rho(g).$$

In fact, it is precisely this invariance argument that yields property (4.3). Certainly, if $g, h \in G$ then

$$\chi_\rho(hgh^{-1}) = \mathrm{Tr}(\rho(hgh^{-1})) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h^{-1})) = \mathrm{Tr}(\rho(h)\rho(g)\rho(h)^{-1})$$

where $\rho(h)$ may be viewed as an element of $\mathsf{GL}_n(\mathbb{C})$. This implies that

$$\chi_\rho(hgh^{-1}) = \chi_\rho(g).$$

Let us fix another representation (τ, W) of G and let $\rho\oplus\tau$ be the direct sum representation. Then, for each $g \in G$

$$(\rho \oplus \tau)(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & \tau(g) \end{pmatrix}$$

is an automorphism of $V \oplus W$ whence

$$\chi_{\rho\oplus\tau}(g) = \mathrm{Tr}((\rho \oplus \tau)(g) = \mathrm{Tr}(\rho(g) + \tau(g)) = \chi_\rho(g) + \chi_\tau(g)$$

by additivity of the trace. Now, $\chi_\rho(e) = \mathrm{Tr}(\rho(e))$ where e is the identity element of the group G. Since ρ is a homomorphism $G \longrightarrow \mathrm{Aut}(V)$, it must take the identity of G to the

identity of $\mathrm{Aut}(V)$. Thus, $\rho(e)$ is the identity map, i.e. the identity matrix $V \longrightarrow V$. Thus, $\chi_\rho(e) = \mathrm{Tr}(\mathrm{I}) = \dim(V)$.

Fix $g \in G$ and let $k \in \mathbb{N}$ be the order of g in G (i.e. let $k := \mathrm{ord}(g)$). Since ρ is an automorphism of groups,

$$\rho(g)^k = \rho(g^k) = \rho(e_G) = e_{\mathrm{Aut}(V)}.$$

It follows that the minimal polynomial of $\rho(g)$, viewed as a matrix in $\mathsf{GL}_n(\mathbb{C})$, solves the polynomial $x^k - 1 = 0$. Over $\mathbb{C}$, this polynomial factors into distinct linear factors whose zeros are *roots of unity*. Hence, $\rho(g)$ is diagonalizable. There thus exists a basis Λ of V and a collection of complex numbers $\lambda_1, \ldots, \lambda_m$ such that

$$[\rho(g)]_\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_m).$$

Now, since $\rho(g)^k = \mathrm{I}$ it follows that $|\lambda_j| = 1$ for each index j. Hence, $\lambda_j^{-1} = \overline{\lambda_j}$ so that

$$[\rho(g)^{-1}]_\Lambda = \mathrm{diag}\left(\lambda_1^{-1}, \ldots, \lambda_m^{-1}\right).$$

The result now follows by invariance of the trace. □

We are now interested in the decomposition of representations and their characters. This is a long and arduous procedure and is, unfortunately, quite technical. Let (ρ, V) be a representation of a finite group G. The first step involves showing that there exists a G-invariant inner product on G.

LEMMA 4.6. *Let G be a finite group and (ρ, V) a representation of G. There exists an inner product $\langle \cdot, * \rangle$ on V that is G-invariant, i.e.*

$$\langle u, v \rangle = \langle \rho(h)u, \rho(h)v \rangle, \quad \forall (u, v) \in V \times V,\ h \in G.$$

PROOF. Define a function $\langle \cdot, * \rangle : V \times V \longrightarrow \mathbb{C}$ by letting

$$\langle u, v \rangle := \frac{1}{|G|} \sum_{g \in G} (\rho(g)u, \rho(g)v)$$

where $(\cdot, *)$ is some fixed inner product on V. We first check that this is a G-invariant map. Certainly, if $h \in G$ then

$$\begin{aligned}
\langle \rho(h)u, \rho(h)v \rangle &= \frac{1}{|G|} \sum_{g \in G} (\rho(g)\rho(h)u, \rho(g)\rho(h)v) \\
&= \frac{1}{|G|} \sum_{g \in G} (\rho(gh)u, \rho(gh)v) \\
&= \frac{1}{|G|} \sum_{g \in G} (\rho(g)u, \rho(g)v) \\
&= \langle u, v \rangle .
\end{aligned}$$

Here we have used the fact that gh ranges over G whenever g also ranges over G. It now only remains to check that $\langle \cdot, * \rangle$ is indeed an inner product on V. Obviously, the linearity of $\langle \cdot, * \rangle$ in the first variable follows from its definition as a finite sum of inner-products on V together with the fact that $\rho(g)$ is, for each $g \in G$, an endomorphism of V. If $(u, v) \in V \times V$ then

$$\overline{\langle v, u \rangle} = \frac{1}{|G|} \sum_{g \in G} \overline{(\rho(g)v, \rho(g)u)} = \frac{1}{|G|} \sum_{g \in G} (\rho(g)u, \rho(g)v) = \langle u, v \rangle .$$

Furthermore,

$$\langle u, u \rangle = \frac{1}{G} \sum_{g \in G} (\rho(g)u, \rho(g)u) \geq 0$$

since each term in the sum is real and non-negative (every summand is an inner-product). In particular, $\langle u, u \rangle \in \mathbb{R}$ for each $u \in V$. Notice that $\langle u, u \rangle = 0$ if and only if $(\rho(g)u, \rho(g)u) = 0$ for each $g \in G$. Hence, $\langle u, u \rangle = 0$ if and only if $u = \mathbf{0}_V$. This concludes the proof of the lemma. □

We now come to the main result of this section which one could call our "first representation theorem".

THEOREM 4.7. *Let G be a finite group and (ρ, V) a representation of G. Then (ρ, V) is the (finite) direct sum of irreducible representations.*

PROOF. We prove this theorem by induction on the dimension of V. If V is one-dimensional then the result is trivial (since V is clearly irreducible). By way of induction, suppose the claim holds up to $n \in \mathbb{N}$ and let (ρ, V) be a representation of dimension $\dim(V) = n + 1$.

Let $\langle \cdot, * \rangle$ be a G-invariant inner product on V (we know such an inner product exists, by the previous lemma). Suppose without loss of generality that (ρ, V) is reducible, else we are done. Let $U \subsetneq V$ be a non-trivial sub-representation and define

$$U^{\perp} := \{v \in V : \langle v, u \rangle = \mathbf{0}, \, \forall u \in U\} .$$

It is known from linear algebra that $V = U \oplus U^{\perp}$ and that

$$\dim(V) = \dim(U) + \dim(U^{\perp}).$$

By our induction hypothesis, it suffices to show that $(\rho, U^{\perp})$ is a sub-representation of V. To see that this is so, we fix $g \in G$ and $v \in U^{\perp}$; we must show that $\rho(g)v \in U^{\perp}$. Certainly, if $u \in U$ then

$$\langle \rho(g)v, u \rangle = \left\langle v, \rho(g)^{-1}u \right\rangle = \left\langle v, \rho(g^{-1})u \right\rangle = 0$$

since $\rho(g^{-1})u \in U$ by the property that (ρ, U) is a sub-representation of V. This concludes the proof. □

5. Fundamental Results of Representation Theory

In this section we give results that are of crucial importance in the theory of representation. We will rely on four main theorems, which will be proven only in the following section. The proofs of these results are to be considered "optional", in the sense that they are difficult and messy. Throughout this section, we instead focus on consequences of these four results.

Given a representation (ρ, V) and a natural number a we shall use the notation ρ^a and V^a to denote, respectively, $\bigoplus_1^a \rho$ and $\bigoplus_1^a V$. Our first fundamental result is the following:

THEOREM I. *Let (ρ, V) be a representation of a finite group G. There exist irreducible non-isomorphic representations $(\rho_1, V_1), \ldots, (\rho_t, V_t)$ and $\{a_1, \ldots, a_t\} \subset \mathbb{N}$ such that $\rho \cong \bigoplus_{j=1}^t \rho_j^{a_j}$. Furthermore, up to isomorphism, these ρ_j are uniquely determined and so are the $\{a_j\}$.*

We also recall the following definition.

DEFINITION 16. Let G be a group. A map $f : G \longrightarrow \mathbb{C}$ is called a class function on G if

$$f(hgh^{-1}) = f(g), \quad \forall (g, h) \in G \times G.$$

The number of conjugacy classes in G is called the class number. We often denote the class number of G by h. The collection of all class functions forms a vector space of dimension h over $\mathbb{C}$, which we shall denote by $\mathrm{Class}(G)$. In fact, every character is a class function.

We now construct an inner-product on $\mathrm{Class}(G)$ that will be of importance soon. Let ϕ, ψ be two class functions on G and define

$$\langle \phi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

It is left as a simple exercise to verify that this $\mathbb{C}$-mapping is indeed an inner product on $\mathrm{Class}(G)$. This inner product induces a notion of orthogonality that allows us to state the following two results.

THEOREM II. *Let (ρ, V) and (τ, W) be representations of a finite group G. If χ_ρ and χ_τ denote their respective characters,*

$$\langle \chi_\rho, \chi_\tau \rangle = \begin{cases} 1, & \text{if } \rho \cong \tau, \\ 0, & \text{otherwise.} \end{cases}$$

THEOREM III. *The characters of irreducible representations of G, considered up to isomorphism, form an orthonormal basis for $\mathrm{Class}(G)$. More precisely, there are precisely $\mathsf{h}(G) = \mathsf{h}$ representative classes for these representations. If $\rho_1, \cdots, \rho_{\mathsf{h}}$ are representatives of these representations, and $\chi_1, \ldots, \chi_{\mathsf{h}}$ their induced characters, then any representation (ρ, V) may be expressed as*

$$\rho \cong \bigoplus_1^{\mathsf{h}} \rho_j^{a_j}$$

where $a_j = \langle \chi_\rho, \chi_j \rangle$ is a non-negative integer.

These three theorems have interesting consequences that we shall explore in what remains of this section.

COROLLARY 4.8. *Let G be a finite group and (ρ, V) a representation of V. Then (ρ, V) is irreducible if and only if $\|\chi_\rho\|^2 = 1$*[2].

PROOF. Since (ρ, V) is a representation of G, by Theorem II-III we may choose non-isomorphic irreducible representations $\rho_1, \cdots, \rho_h$ so that

$$\chi_\rho = \sum_1^h a_j \chi_j,$$

where $a_j = \langle \chi_\rho, \chi_j \rangle \in \mathbb{N}$. Once again, using the fact that the χ_j are orthogonal, it follows that

$$\|\chi_\rho\|^2 = \sum_1^h \|a_j \chi_j\|^2 = \sum_1^h a_j^2.$$

The statement now follows from the above identity. □

DEFINITION 17. Let G be a finite group. The trivial representation of G is the map

$$\rho : G \longrightarrow \mathrm{Aut}(\mathbb{C}), \quad g \mapsto f(z) = z.$$

It is trivial to check that this is indeed a representation.

LEMMA 4.9. *Let G be a finite group and $(\rho, \mathbb{C})$ the trivial representation of G. Then $(\rho, \mathbb{C})$ is irreducible.*

PROOF. Let $\chi : G \longrightarrow \mathbb{C}$ be the associated character. Then, $\chi(g) = \mathrm{Tr}(\rho(g)) = 1$ for each g so that

$$\|\chi\|^2 = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = 1.$$

The result now follows from Corollary 4.8. □

LEMMA 4.10. *Let G be finite group and (ρ, V) an irreducible trivial representation of G. If $(\rho_1, \mathbb{C})$ denotes the trivial representation, then $\rho \cong \rho_1$.*

PROOF. The fact that (ρ, V) is a trivial representation is precisely the statement that $\rho(g)$ is the identity map $V \longrightarrow V$, for each $g \in G$. This is to say that $\rho(g)v = v$ for each $g \in G$ and $V \in V$. Hence, $V^G = V$ and $\dim(V) = 1$. This means that there exists an isomorphism of vector spaces $T : V \longrightarrow \mathbb{C}$.

Fix $g \in G$ and let $u \in V$ be given. Then,

$$T(\rho(g)v) = T(v) = \rho_1(g)(Tv).$$

[2]Here χ_ρ denotes the character of ρ and $\|\cdot\|$ is the norm induced by the inner product we introduced on Class(G). To be more precise, $\|\chi_\rho\|^2 = \langle \chi_\rho, \chi_\rho \rangle$.

We conclude that $\rho \cong \rho_1$ as representations. □

COROLLARY 4.11. *Let (ρ, V) be a representation of a finite group G. Then $\dim(V^G)$ is given by $\langle \chi_1, \chi_\rho \rangle$ where χ_1 is the character induced by the trivial representation of G (over V, the character of the identity map on V). Especially,*

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$

PROOF. By Theorem III we may choose non-isomorphic irreducible representations (ρ_j, V_j) such that $\chi_\rho = \sum a_j \chi_j$ for some natural numbers a_j. Lemma 4.9 shows that, after possibly letting $a_1 = 0$, we may assume χ_1 is the character of the trivial representation. Obviously, by orthogonality of the characters,

$$a_1 = \langle \chi_1, \chi_\rho \rangle = \langle \chi_\rho, \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$

It thus only remains to check that $a_1 = \dim(V^G)$. If $V = \bigoplus V_j^{a_j}$ then clearly one must have

$$V^G = \bigoplus \left((V_j^G)^{a_j} \right).$$

Now, we may assume each V_j is irreducible. Thus, $V_j^G = V_j$ or $V_j^G = \{\mathbf{0}\}$. In the former case, $\rho_j(g)$ is the trivial map for each $g \in G$ which contradicts the assumption that ρ_1 is the trivial character. Thus, $V_j^G = \{0\}$ for each $j > 1$. Hence, the result follows:

$$\dim(V^G) = a_1$$

as was required. □

COROLLARY 4.12. *Let G be a finite group and $(\rho^{reg}, \mathbb{C}^n)$ the regular representation of G. Let $\rho_1, \ldots, \rho_h$ be representatives for the irreducible non-isomorphic representations of G. Then,*

$$\rho^{reg} = \bigoplus_{j=1}^{h} \rho_j^{\dim(\rho_j)}$$

where we define $\dim(\tau) = \dim(W)$ for a representation (τ, W).

PROOF. As usual, we may write $\chi_{\rho^{\text{reg}}} = \sum a_j \chi_{\rho_j}$ where the ρ_j are the irreducible representations and $a_i \geq 0$. However,

$$\begin{aligned} a_j = \left\langle \chi_{\rho^{\text{reg}}}, \chi_{\rho_j} \right\rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\rho^{\text{reg}}}(g) \overline{\chi_{\rho_j}(g)} &= \frac{\chi_{\rho^{\text{reg}}}(e) \overline{\chi_{\rho_j}(e)}}{|G|} \\ &= \overline{\chi_{\rho_j}(e)} \\ &= \overline{\dim(\rho_j)} \\ &= \dim(\rho_j). \end{aligned}$$

□

From this we deduce the following theorem.

THEOREM IV. *Let G be a finite group of order n and let $(\rho^{reg}, \mathbb{C}^n)$ be the regular representation of G. Adopting the notation from the other theorems,*

$$|G| = \sum_{j=1}^{h} \dim(\rho_j)^2.$$

PROOF. This is an immediate consequence of the following calculation

$$|G| = n = \dim(\mathbb{C}^n) = \dim(\rho^{\text{reg}}) = \sum_{j=1}^{h} \dim(\rho_j)^2.$$

□

6. Fundamental Results of Representation Theory: Some Proofs*

The title of this section is quite self-explanatory. We devote this part of these notes to the proving the 3 main results stated in §5 of this chapter. Our exploration begins with an important lemma due to Schur.

LEMMA 4.13 (Schur's Lemma). *Let (ρ, V) and (τ, W) be two irreducible representations of a finite group G. Then,*

$$\text{Hom}_G(V, W) \cong \begin{cases} \mathbb{C}, & \text{if } \rho \cong \tau, \\ \{0\}, & \text{otherwise.} \end{cases}$$

In the above we view $\mathbb{C}$ as a group under addition. Clearly, $\{0\}$ is itself the trivial group under addition and thus may identified with $\{e\}$.

PROOF OF LEMMA 4.13. Suppose first that there exists $T \in \text{Hom}_G(V, W)$ that is not the zero map $v \mapsto \mathbf{0}_W$. We know from Proposition 4.1 that $(\rho, \text{Ker}\, T)$ and $(\tau, \text{Im}(T))$ are sub-representations of (ρ, V) and (τ, W), respectively. Since V is irreducible, either $\text{Ker}\, T = \{\mathbf{0}_V\}$ or $\text{Ker}\, T = V$. Since T is not the zero map, the morphism T must be an embedding $V \hookrightarrow W$. Likewise, either $\text{Im}(T) = \{\mathbf{0}_W\}$ or $\text{Im}(T) = W$. Again, T is injective whence $\text{Im}(T) \supsetneq \{0\}$. That is, $\text{Im}(T) = W$ so that

$$T : V \longrightarrow W$$

is an isomorphism of vector spaces. We may therefore identify V with W using this morphism T. It thus suffices to check that

$$\text{End}_G(V) \cong \mathbb{C}.$$

Let $S \in \mathrm{End}_G(V)$ and let $\lambda \in \mathbb{C}$ be an eigenvalue of S. If V_λ is the corresponding (non-zero) eigenspace, then

$$S(\rho(g)v) = \rho(g)(Sv) = \rho(g)(\lambda v) = \lambda\rho(g)v$$

which shows that $\rho(g)v \in V_\lambda$. Thus, V_λ is a sub-representation of V so that $V_\lambda = V$. It follows that $V_\lambda = V$. Consequently, $S = \lambda \cdot \mathrm{I}$. Conversely, if $\lambda \in \mathbb{C}$ and $S = \lambda \cdot \mathrm{I}$ then

$$S(\rho(g)v) = \lambda\rho(g)v = \rho(g)(\lambda v) = \rho(g)(Sv).$$

This means that every element of $\mathrm{End}_G(V)$ is a scalar multiple of the identity. The natural association then shows that $\mathrm{End}_G(V) \cong \mathbb{C}$. □

6.1. Uniqueness of Decomposition: The Proof of Theorem I.

PROOF OF THEOREM I. By Theorem 4.7, if (ρ, V) is a representation of G we may choose irreducible subspaces V_i such that

$$V \cong \bigoplus_1^N V_i^{a_i}, \quad a_i \in \mathbb{N}_0$$

Since the above is up to isomorphism, we may assume that $V_i \ncong V_j$ for $i \neq j$. Otherwise, join V_i and V_j and obtain $V_i^{a_i+a_j}$ in the above representation. In this case, we show that the a_i's are uniquely determined. To this end, suppose that

$$V \cong \bigoplus_1^N V_i^{b_i}, \quad b_i \in \mathbb{N}_0.$$

By allowing zero exponents in both representations, we may obviously assume that these expressions contain the same number of elements and the same vector subspaces V_i. It then suffices to check that $a_i = b_i$ for all $i \in \{1, \ldots, N\}$. By Schur's lemma

$$\begin{aligned}\dim(\mathrm{Hom}_G(V_i, V)) = \bigoplus_1^N \dim(\mathrm{Hom}_G(V_i, V_i^{a_i})) &= \bigoplus_1^N \dim(\mathrm{Hom}_G(V_i, V_i)^{a_i}) \\ &= \dim(\mathrm{Hom}_G(V_i, V_i))^{a_i}.\end{aligned}$$

A final application of Schur's lemma yields,

$$\dim(\mathrm{Hom}_G(V_i, V)) = \dim(\mathbb{C}^{a_i}) = a_i.$$

Repeating this procedure with our second representation will then give

$$\dim(\mathrm{Hom}_G(V_i, V)) = b_i$$

so that $a_i = b_i$. □

7. Exercises

We are rather limited in the problems we can ask here, as we have only scratched the surface of representation theory. This is no big deal; the problems here will simply ensure the reader has understood and digested the definitions of the chapter.

EXERCISE 4.1. Let (ρ, V) be an irreducible representation of a group G. Using the argument in the proof of Schur's lemma, prove that if $T \in \mathrm{End}_G(V)$ then there exists $\lambda \in \mathbb{C}$ such that $T = \lambda \cdot I$, where I is the identity map. Conclude that $\mathrm{End}_G(V) \cong \mathbb{C}$ (as vector spaces) .

EXERCISE 4.2. Let G be a finite group and $z \in Z(G)$. If (ρ, V) is an irreducible representation of G, show that $\rho(z) : V \longrightarrow V$ is a scalar multiple of the identity matrix.

EXERCISE 4.3. Classify all bijective $\mathbb{C}$-linear transformations $\mathbb{C} \to \mathbb{C}$. Conclude that the group $\mathrm{Aut}(\mathbb{C}) \cong \mathbb{C}^\times$, where $\mathbb{C}$ is considered as a complex vector space.

EXERCISE 4.4 (Character Column Orthogonality). Let G be a finite group having class number h. Let $\{\chi_j\}_{j=1}^{\mathsf{h}}$ be the orthogonal characters of G. Prove that

$$\sum_{j=1}^{\mathsf{h}} \chi_j(g)\overline{\chi_j(h)} = \begin{cases} |\mathrm{C}(g)|\,, & \text{if } g \text{ and } h \text{ are conjugate,} \\ 0, & \text{otherwise.} \end{cases} \tag{4.4}$$

EXERCISE 4.5. Let G be a finite Abelian group of order n. Prove that there are exactly n characters of irreducible representations (up to isomorphism) and that any such representation is one dimensional. Deduce that the character is a homomorphism $G \longrightarrow \mathbb{C}^\times$.

EXERCISE 4.6. Construct a character table for $\mathbb{Z}/3\mathbb{Z}$.

EXERCISE 4.7. Show that the sum of entries in the non-trivial columns of a character table evaluates to zero. More precisely, let $\{\chi_j\}$ be an enumeration of the orthonormal characters of irreducible non-isomorphic representations for a group G and fix $g \in G\backslash\{e\}$. Prove that

$$\sum_{\chi_j} \chi_j(g) = 0.$$

EXERCISE 4.8. Find the decomposition of the representation $\rho : \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{C}^2)$ via the homomorphism

$$\rho(a) := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^a$$

where a is considered modulo 4.

Solutions to Exercises

Throughout this final part of the text, we provide detailed solutions to the exercises presented at the end of the chapters. We stress the importance of trying out the exercises yourself. The exercises themselves are more theoretic than computational, and the number of given exercises reflects this fact. It is therefore crucial that one understands the solution entirely when studying the subject.

1. Solutions to Problems in Chapter 1

SOLUTION TO EXERCISE 1.1. This is not too difficult to solve. First, note that every bijection σ is invertible in the sense that there exists σ^{-1} such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma \equiv \mathbf{1}$. Hence, if we let $\mathbf{1}$, the identity map, be the identity element of S_n, it is clear that S_n is a group under composition of functions. Note that $|\mathsf{S}_n| = n!$. □

SOLUTION TO EXERCISE 1.2. We now verify that $Z(G)$ is a subgroup of G. Clearly, $e \in Z(G)$. Now, if $g \in Z(G)$ it follows that $gx = xg$ for every $x \in G$. In particular,

$$x^{-1}g^{-1} = g^{-1}x^{-1}.$$

Letting x range over G, it follows that $g^{-1} \in Z(G)$ if and only if $g \in Z(G)$. Finally, if $g_1, g_2 \in Z(G)$ and $x \in G$:

$$(g_1g_2)x = g_1(g_2x) = g_1(xg_2) = (g_1x)g_2 = x(g_1g_2).$$

This shows that $Z(G) < G$. □

SOLUTION TO EXERCISE 1.3. We show that every boolean group $\mathfrak{B}$ is Abelian. First, if $g \in \mathfrak{B}$ then $g^2 = e$ which implies that $g^{-1} = g$, by uniqueness of the inverse. Therefore, if

$x, y \in \mathfrak{B}$ we find

$$(xy) = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

This completes the proof. □

SOLUTION TO EXERCISE 1.4.

(1) For the first part, we note that $\mathbb{K}$ forms a vector space over $\mathbb{F}$, indeed this is immediate from the field axioms. Since $\mathbb{K}$ is finite, it is finite dimensional when considered over $\mathbb{F}$. Let $\{b_1, \ldots, b_n\}$ be a basis for $\mathbb{K}$ and note that any vector $u \in \mathbb{K}$ has a unique representation

$$u := \sum_{j=1}^{n} \alpha_j b_j, \quad \alpha_j \in \mathbb{F}.$$

Conversely, any such u determines a vector in $\mathbb{K}$. Since there are exactly q^n possibilities for the n-tuples $(\alpha_1, \ldots, \alpha_n)$, it follows that $|\mathbb{K}| = q^n$. This establishes (1).

(2) For the second part, we need only consider $a \in \mathbb{F}^\times$. Since $\mathbb{F}^\times$, as a group, has order $q-1$, it follows that $a^{q-1} = 1$ for every $a \in \mathbb{F}^\times$. This establishes (2).

(3) For the final part, we need only handle the case $a \in \mathbb{K}^\times$ since $\mathbb{F} \cap \mathbb{K} \supset \{0\}$. Noticing that $\mathbb{K}^\times$ has order $q^n - 1$, it becomes clear that $(q-1)$ divides the order of $\mathbb{K}^\times$. Recall that both $\mathbb{F}^\times$ and $\mathbb{K}^\times$ are cyclic groups. Now, if $a^{q-1} = 1$ then $\mathrm{ord}(a) \mid (q-1) \mid (q^n - 1)$. By Lagrange's theorem, $\langle x \rangle$ is the unique subgroup of $\mathbb{K}^\times$ having order $\mathrm{ord}(a)$. But, there also exists a cyclic subgroup of $\mathbb{F}^\times \subseteq \mathbb{K}^\times$ having order precisely $\mathrm{ord}(a)$. By uniqueness in $\mathbb{K}^\times$, we conclude that $\langle a \rangle \subseteq \mathbb{F}^\times$.

□

SOLUTION TO EXERCISE 1.5. By way of contradiction, suppose $f : G \longrightarrow H$ is a non-trivial homomorphism of groups. Then, $\mathrm{Ker}\, f \neq G$ so that the quotient group $G/\mathrm{Ker}\, f$ is non-trivial. However, the first isomorphism statements yields

$$G/\mathrm{Ker}\, f \cong f(G) < H.$$

By Lagrange's theorem, this means that $[G : \mathrm{Ker}\, f]$ is a non-trivial divisor of both $|H|$ and $|G|$, which is a contradiction. □

SOLUTION TO EXERCISE 1.6. Fix $x \in G$ and let $\tau_x : G \longrightarrow G$ be given by $\tau_x(g) = xgx^{-1}$ for $g \in G$. By closure under the group operation, this is a well defined map. For each fixed x, the function τ_x is injective since x (and x^{-1}) are invertible. τ_x is also surjective since

$$\tau_x(x^{-1}gx) = xx^{-1}gxx^{-1} = ege = g, \quad \forall g \in G.$$

Note that here it would have been enough to check that τ_x is either injective or surjective. It remains only to ensure that τ_x is a homomorphism. To this end, let $g, h \in G$ be given

and notice that

$$\tau_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = \tau_x(g)\tau_x(h).$$

□

SOLUTION TO EXERCISE 1.7. If G is a group, then the identity map $\mathbf{1}_G : G \longrightarrow G$ given by $g \mapsto g$ is a bijective homomorphism of groups (and thus an automorphism of G). This means that $\mathrm{Aut}(G) \neq \varnothing$. We first show that $\mathrm{Aut}(G)$ is closed under composition. Let $\sigma, \tau \in \mathrm{Aut}(G)$ and consider $\sigma \circ \tau$, which is again a bijective function $G \longrightarrow G$. If $g, h \in G$ then

$$(\sigma \circ \tau)(gh) = \sigma(\tau(gh)) = \sigma(\tau(g)\tau(h)) = \sigma(\tau(g))\sigma(\tau(h)) = (\sigma \circ \tau)(g)(\sigma \circ \tau)(h).$$

Therefore, $\sigma \circ \tau$ is a homomorphism and belongs to $\mathrm{Aut}(G)$. This means that $\mathrm{Aut}(G)$ is closed under composition. The identity map $\mathbf{1}_G$ described above is clearly a perfect candidate for the identity element of $\mathrm{Aut}(G)$ since

$$\sigma \circ \mathbf{1}_G \equiv \mathbf{1}_G \circ \sigma \equiv \sigma, \quad \forall \sigma \in \mathrm{Aut}(G).$$

Finally, let $\sigma \in \mathrm{Aut}(G)$. Since σ is a bijection $G \longrightarrow G$, it admits an inverse function $\sigma^{-1} : G \longrightarrow G$. It is clear that

$$\sigma \circ \sigma^{-1} \equiv \sigma^{-1} \circ \sigma \equiv \mathbf{1}_G$$

and as such it only remains to check that σ^{-1} is a homomorphism in its own right. Fix $g, h \in G$ and choose $x, y \in G$ such that $g = \sigma(x)$ and $h = \sigma(y)$. Then,

$$\sigma^{-1}(gh) = \sigma^{-1}(\sigma(x)\sigma(y)) = \sigma^{-1}(\sigma(xy)) = xy = \sigma^{-1}(g)\sigma^{-1}(h).$$

The proof is now complete. □

2. Solutions to Problems in Chapter 2

SOLUTION TO EXERCISE 2.1. We argue that H is normal in G. Consider the collection of left cosets of H in G, denoted G/H. This may or may not be a group, but it makes sense as a collection of sets! We define an action of G upon S by taking

$$(g, xH) \mapsto g * (xH) = (gx)H.$$

It is easy to check that this is a well defined action on G/H. This induces a clear homomorphism of groups

$$\psi : G \longrightarrow \mathsf{S}_p$$

since $|G/H| = [G : H] = p$. Let $N := \mathrm{Ker}\,\psi$ which is normal in G. We also note that $N \subseteq H$. To see this, suppose that $n \in N$. Then $\psi(n)$ is the identity permutation which means that

$$n * (xH) = xH, \quad \forall x \in G.$$

Especially, $nH = H$ which is possible if and only if $n \in H$. Now, the first isomorphism theorem states that G/N is isomorphic to a subgroup of S_p. This means that $[G : N]$

divides $|G|$ and $p!$. Since p is the least prime dividing the order of G, it follows that $[G : N] = 1$ or $[G : N] = p$. Since $N \subseteq H$ and H is a proper subgroup of G, it follows that $N \neq G$ whence $[G : N] = p$. But then,

$$[G : N] = \frac{|G|}{|N|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|N|} = p[H : N].$$

This implies that $[H : N] = 1$ whence $H = N$. As the kernel of a group homomorphism, N is normal in G which completes the proof. □

SOLUTION TO EXERCISE 2.2. We define an action of G upon the family of left cosets G/A. This is done by letting

$$(g, xA) \mapsto gxA$$

as in the previous exercise. Note that this action is transitive because $\mathrm{Orb}(A) = G/A$. Also, since A is a proper subgroup of G, there exists an element $x \in G$ with no fixed points. We now claim that $x \notin \bigcup_{g \in G} gAg^{-1}$.

Assume for a contradiction that $x \in gAg^{-1}$. Then $x = gag^{-1}$ for some $a \in A$ and $g \in G$. But then,

$$(x, gH) \mapsto xgH = (gag^{-1}g)H = gH$$

which contradicts the choice of x. □

SOLUTION TO EXERCISE 2.3. Since $s_1 \in \mathrm{Orb}(s)$ there exists $g \in G$ such that $s_1 = g * s$. We will show that

$$\mathrm{Stab}(s_1) = g\,\mathrm{Stab}(s)g^{-1}.$$

If $x \in g\,\mathrm{Stab}(s)g^{-1}$ then $x = gng^{-1}$ where $n \in \mathrm{Stab}(s)$. Then,

$$x * s_1 = (gng^{-1}) * s_1 = (gn) * (g^{-1} * s_1) = (gn) * s = g * s = s_1.$$

Therefore, $\mathrm{Stab}(s_1) \supseteq g\,\mathrm{Stab}(s)g^{-1}$. To see the reverse inclusion, let $x \in \mathrm{Stab}(s_1)$. Then, $g^{-1}xg \in \mathrm{Stab}(s)$ since

$$(g^{-1}xg) * s = (g^{-1}x) * s_1 = g^{-1} * s_1 = s.$$

But this means that $x \in g\,\mathrm{Stab}(s)g^{-1}$ whence the statement follows. □

SOLUTION TO EXERCISE 2.4. We define an action of G upon the set $G/H \times G/K$, which is finite since both H and K have finite index in G. This action is prescribed as follows:

$$g * (xH, yK) := (gxH, gxY).$$

It is easy to check that this is a well defined action. We consider now the stabilizer $\mathrm{Stab}((H, K))$ in G. We have already shown that there exists a bijection

$$G/\,\mathrm{Stab}((H, K)) \longleftrightarrow \mathrm{Orb}((H, K)).$$

Noticing that $\mathrm{Orb}((H,K)) \subseteq G/H \times G/K$, it follows that $G/\mathrm{Stab}((H,K))$ is a finite set. On the other hand,

$$\mathrm{Stab}((H,K)) = \{g \in G : (gH, gK) = (H,K)\} = H \cap K.$$

This shows that $H \cap K$ has finite index in G. □

SOLUTION TO EXERCISE 2.5. The collection G/H contains more than one element by hypothesis. Let us define an action of G upon G/H by letting

$$g * (xH) := (gx)H.$$

This induces a homomorphism $\psi : G \longrightarrow \mathsf{S}_k$ whose kernel is normal in G. Suppose first that $\mathrm{Ker}\,\psi = G$. Then $g(xH) = xH$ for every $x \in G$ and $g \in G$ whence $gH = H$ for every $g \in G$ which implies that $H = G$. Therefore, by the simplicity of G, ψ must be injective. This implies that $k! \geq n$. □

SOLUTION TO EXERCISE 2.6. We shall prove the contrapositive. Let G be a group of odd order. We know that we may express G as the disjoint union of conjugacy classes, where the order of any conjugacy class divides the order of G.

Let $x_1, \ldots, x_k$ be representatives for these classes so that

$$G = \bigsqcup_{j=1}^{k} \mathrm{Conj}(x_j).$$

Now, since $|\mathrm{Conj}(x_j)|$ divides $|G|$ for each j, any conjugacy class will have odd cardinality. Since any even sum of odd numbers is even, the number of conjugacy classes must be odd (otherwise $|G|$ is even). □

3. Solutions to Problems in Chapter 3

SOLUTION TO EXERCISE 3.1. This is an easy consequence of Cauchy's theorem (see Theorem 3.5). Let N denote the order of $\mathfrak{B}$; by the fundamental theorem of arithmetic it suffices to check that the only prime divisor of N is 2. Let p be a prime dividing $|\mathfrak{B}|$, by Cauchy's theorem we may extract an element b having order precisely p. Since $b^2 = e$, we must have $p \leq 2$. □

SOLUTION TO EXERCISE 3.2. We left G act upon H by conjugation:

$$(g,h) \mapsto ghg^{-1}.$$

Then, H is the disjoint union of conjugacy classes (where any representative must live in H). If $x \in Z(G) \cap H$ then $\mathrm{Conj}(x) = \{x\}$ since x commutes with the elements of G. This

implies that

$$|H| = |Z(G) \cap H| + \sum_{\substack{h \in H \text{ repr.} \\ x \notin Z(G) \cap H}} \frac{|G|}{\mathrm{C}(h)}.$$

Now, for every $h \notin Z(G)$ the subgroup $C(h)$ is a proper subgroup of G. This means that $|Z(G) \cap H| \equiv 0 \pmod{p}$ which implies that $|Z(G) \cap H| \geq p$. □

SOLUTION TO EXERCISE 3.3. We will argue by induction on the order of $|G|$. If $|G| = p$ then the result is clear since the only option is $H = G$ and $H^- = \{e\}$. Assume now the claim holds for groups up to order p^{r-1} and let $|G| = p^r$. By the previous problem, we may choose an element $x \in H \cap Z(G)$ with $\mathrm{ord}(x) = p$ and define $K := \langle x \rangle$ which is a normal subgroup of G. If $K = H$, then we need only choose $H^- = \{e\}$.

If $K \neq H$, we appeal to the quotient group G/K which has order p^{r-1}. Recall the canonical map

$$\pi_K : G \longrightarrow G/K, \quad g \mapsto gK.$$

Define $H' := \pi_k(H)$ which must be normal in G/K by the correspondence theorem. Applying the induction hypothesis, we recover a subgroup A', normal in G/K, with $[H' : A'] = p$. Let $H^- := \pi_k^{-1}(A)$ which contains K and is therefore normal in G. Then, by the third isomorphism theorem,

$$H/H^- \cong H'/A'$$

which completes the proof. □

SOLUTION TO EXERCISE 3.4. It suffices to show that one of n_q, n_p, n_r are 1. To this end, suppose $n_{q,r,p} > 1$. By Sylow's theorems, we find that $n_r \mid pq$ and

$$n_r = 1 + kr, \quad k \geq 1.$$

Since $p < q < r$, it follows that $n_r \geq pq$. Now, another application of Sylow's theorems yield $n_q \mid pr$ and

$$n_q = 1 + kq, \quad k \geq 1.$$

This means $n_q \in \{p, r, pq\}$. If $n_q = p$ then we have a contradiction. This implies that $n_q \geq r$ and, likewise, $n_p \geq q$. Groups of order p, q and r intersect only at the trivial element e. Furthermore, distinct groups of order p (or q or r) intersect only at e. This implies that

$$\begin{aligned} pqr = |G| \geq pq(r-1) + r(q-1) + q(p-1) &= pqr + rq - r - q \\ &> pqr. \end{aligned}$$

This is a contradiction. □

SOLUTION TO EXERCISE 3.5. We shall first argue that $H \cap P$ is a maximal p-subgroup of G. Obviously, $H \cap P$ is a p-subgroup of H. Now, let $H \supseteq K \supseteq H \cap P$ be a maximal p-subgroup and let K' be a maximal p-subgroup of G with $K' \supseteq K$. Then,

$$P = gK'g^{-1}$$

for some $g \in G$. This implies that

$$\begin{aligned} H \cap P = H \cap \left[gK'g^{-1}\right] \supseteq H \cap [gKg^{-1}] &= (gHg^{-1}) \cap (gKg^{-1}) \\ &= g(H \cap K)g^{-1} \\ &= gKg^{-1}. \end{aligned}$$

This implies that $|P \cap H| \geq |K|$ whence $P \cap H = K$. It now remains only to check that HP/H is a p-Sylow subgroup of G/H. Suppose that $|G| = p^r m$ with $\gcd(p, m) = 1$ and $|H| = p^a n$ where $\gcd(p, n) = 1$. Then,

$$[G : H] = \frac{p^r m}{p^a n} = p^{r-a} d, \quad d = m/n \in \mathbb{N}.$$

On the other hand,

$$|HP/H| = \frac{|H| \cdot |P| \,/\, |H \cap P|}{|H|} = \frac{|P|}{|H \cap P|} = \frac{p^r}{p^a} = p^{r-a}.$$

The proof is now complete. □

SOLUTION TO EXERCISE 3.6. Consider S_6 and $\mathbb{Z}/6\mathbb{Z}$. Only the latter is Abelian and the composition factors of each group are cyclic groups of prime order (and therefore are isomorphic). □

SOLUTION TO EXERCISE 3.7. We first check that f_a is a group homomorphism (remember that $\mathbb{Z}/n\mathbb{Z}$ is a group under addition). Certainly, if $x, y \in \mathbb{Z}/n\mathbb{Z}$ then

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

This verifies that $f \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. Now, since $\mathbb{Z}/n\mathbb{Z}$ is finite and f is an endomorphism, f is bijective if and only if f is injective. It therefore suffices to check that $ax = ay$ if and only if $x = y$. This is immediate from the fact that $(\mathbb{Z}/n\mathbb{Z})^\times$ are precisely the elements (modulo n) that are invertible. □

SOLUTION TO EXERCISE 3.8. We claim here that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Let now f be an automorphism of $\mathbb{Z}/n\mathbb{Z}$. Observe that, if $x \in \mathbb{Z}/n\mathbb{Z}$, one has

$$f(x) = f(\underbrace{1 + 1 + \cdots + 1}_{x \text{ times}}) = \underbrace{f(1) + f(1) + \cdots + f(1)}_{x \text{ times}} = xf(1).$$

Let now $a := f(1)$; we claim $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Recalling that 1 generates $\mathbb{Z}/n\mathbb{Z}$ and using 1^a to denote $1 + 1 + \cdots + 1$, we obtain

$$\mathrm{ord}(a) = \mathrm{ord}(1^a) = \frac{n}{\gcd(a, n)}.$$

Since isomorphisms (and therefore automorphisms) preserve the order of elements, we conclude that $\gcd(a, n) = 1$. It follows that every automorphism of $\mathbb{Z}/n\mathbb{Z}$ is of the form $f(x) = ax$ for $a \in \mathbb{Z}/n\mathbb{Z}$. Conversely, the previous problem shows that any such function yields an automorphism of $\mathbb{Z}/n\mathbb{Z}$.

Adopting the notation of the previous exercise, we consider the map

$$\Gamma : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad a \mapsto f_a.$$

By the argument above, this is a surjection. To see that Γ is injective, suppose $f_a \equiv f_b$ for $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$. This clearly implies that $f_a(1) = a = b = f_b(1)$. Now, Γ is a group homomorphism since

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

This concludes the proof of this result. □

SOLUTION TO EXERCISE 3.9. Suppose that N and B are Abelian and that $G = N \rtimes_\phi B$, where $\phi : B \longrightarrow \mathrm{Aut}(N)$ is the trivial homomorphism. We show that G is Abelian. Indeed, if $(n_1, b_1), (n_2, b_2) \in B \rtimes_\phi N$. Then,

$$\begin{aligned}(n_1, b_1)(n_2, b_2) = (n_1\phi_{b_1}(n_2), b_1b_2) = (n_1n_2, b_1b_2) &= (n_2n_1, b_2b_1) \\ &= (n_2\phi_{b_2}(n_1), b_2b_1) \\ &= (n_2, b_2)(n_1, b_1).\end{aligned}$$

Conversely, suppose that $N \rtimes_\phi B$ is Abelian. We first argue that N and B are Abelian. Certainly, if $(n_1, b_1), (n_2, b_2) \in B \rtimes_\phi N$ then we calculate

$$(n_1, b_1)(n_2, b_2) = (n_1\phi_{b_1}(n_2), b_1b_2) = (n_2\phi_{b_2}(n_1), b_2b_1) = (n_2, b_2)(n_1, b_1).$$

This means that $b_1b_2 = b_2b_1$ whence it follows that B is Abelian. Also, for every $b_1, b_2 \in B$ and $n_1, n_2 \in N$ there holds

$$n_1\phi_{b_1}(n_2) = n_2\phi_{b_2}(n_1). \tag{A.1}$$

Taking $b_1 = b_2 = e_B$ we recover the trivial homomorphism ϕ_e. But this means that

$$n_1n_2 = n_2n_1.$$

Hence, N is an Abelian group. It now only remains to check that ϕ is the trivial homomorphism. This amounts to proving that ϕ_b is the identity map $N \longrightarrow N$ for every $b \in B$. However, this follows by taking $n_2 = e_N$ in (A.1). The proof is now complete and we have characterized all Abelian semidirect products. □

SOLUTION TO EXERCISE 3.10. Let n_{11} denote the number of 11-Sylow subgroups of G. Then $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 3 \cdot 7 = 21$. Since neither 3, 7 or 21 reduce to 1 modulo 11, we must have $n_{11} = 1$. Hence, there is a unique 11-Sylow subgroup of G, say, R. It follows that $R \lhd G$ and $R \cong \mathbb{Z}/11\mathbb{Z}$. In particular, R is Abelian.

We construct a group homomorphism:

$$\Gamma : G/R \longrightarrow G \longrightarrow \mathrm{Aut}(R), \quad gR \mapsto g \mapsto \tau_g$$

where $\tau_g : R \longrightarrow R$ is given by $\tau_g(x) = gxg^{-1}$. There is quite a lot to check here. First, we wish to show that τ_g is indeed an automorphism of R for every $g \in G$. Indeed, since R is normal in G, $gxg^{-1} \in R$ for every $g \in G$ and $x \in R$. Since τ_g is injective, it follows that τ_g

is an automorphism of R. We now show that if $g_1R = g_2R$ then $\tau_{g_1} = \tau_{g_2}$. Here we will use that R is Abelian. We may write $g_2 = g_1r$, for some $r \in R$. Therefore, if $x \in R$

$$\tau_{g_2}(x) = g_2xg_2^{-1} = (g_1r)x(g_1r)^{-1} = g_1rxr^{-1}g_1^{-1} = g_1xg_1^{-1}.$$

It is easy to verify that Γ, from G/R into $\mathrm{Aut}(R)$, is a group homomorphism. Since $\mathrm{Aut}(R) \cong (\mathbb{Z}/11\mathbb{Z})^\times$, we know that $\mathrm{Aut}(R)$ has 10 elements. However, G/R has precisely 21 elements. Since $\gcd(21, 10) = 1$ this homomorphism Γ must be trivial (see the exercises in the first section).

This means that $\Gamma(gR)$ is the identity map $R \longrightarrow R$. In other words, τ_g is the identity map $R \longrightarrow R$ for every $g \in G$. In this case, for every $g \in G$ and $x \in R$ one has that

$$\tau_g(x) = gxg^{-1} = x$$

whence it follows that $gx = xg$ for every $x \in R$ and $g \in G$. It follows that $R \subseteq Z(G)$.

□

SOLUTION TO EXERCISE 3.11. We proceed as in the previous problem. Notice that $385 = 5 \cdot 7 \cdot 11$. Let n_7 denote the number of 7-Sylow subgroups of G. Sylow's theorems guarantee that $n_7 \mid 55$ and $n_7 \equiv 1 \pmod 7$. This last condition forces $n_7 \neq 5$ and $n_7 \neq 11$. Also,

$$55 \equiv 6 + 49 \equiv 6 \not\equiv 1 \pmod 7$$

whence we must have $n_7 = 1$. This means that the 7-Sylow subgroup is unique, and therefore normal in G. This argument can be repeated for n_{11}. Certainly, notice that $n_{11} \mid 35$ and $n_{11} \equiv 1 \pmod{11}$. Since

$$35 \equiv 2 + 33 \equiv 2 \pmod{11}$$

there must hold $n_{11} = 1$ as before. This establishes (1). For the second part, we argue as in the previous problem. Let Q denote the 7-Sylow subgroup of G. We know from the first part that $Q \lhd G$, and we may therefore speak of the quotient group G/Q which will have order 55. We construct a chain homomorphism

$$G/Q \longrightarrow G \longrightarrow \mathrm{Aut}(Q), \quad gQ \mapsto \tau_g \tag{A.2}$$

where $\tau_g(x) := gxg^{-1}$ is the map $Q \longrightarrow Q$. Since Q is normal, this τ_g is an injective homomorphism $Q \longrightarrow Q$ whence it follows that $\tau_g \in \mathrm{Aut}(Q)$ for every $g \in G$. We must only now check that $\tau_g = \tau_h$ whenever $gQ = hQ$. In this case, $g = hq$ for $q \in Q$. This means that for every $x \in Q$:

$$\tau_g(x) = gxg^{-1} = (hq)x(hq)^{-1} = h(qxq^{-1})h^{-1}.$$

Notice now that $Q \cong \mathbb{Z}/7\mathbb{Z}$ and is, in particular, Abelian. Since $x, q \in Q$ it follows that

$$\tau_g(x) = hxh^{-1} = \tau_h(x).$$

Therefore our homomorphism $G/Q \longrightarrow \mathrm{Aut}(Q)$ is well defined. Now,

$$\mathrm{Aut}(Q) \cong \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$$

which has order 6. On the other hand, G/Q has order 55. Since $\gcd(6, 55) = 1$, we conclude that the homomorphism described in (A.2) is the trivial one which takes every coset gQ to the identity map $Q \longrightarrow Q$. This implies that the map τ_g is the identity automorphism of Q, for each $g \in G$. That is, given any $g \in G$, there holds $gxg^{-1} = x$ for all $x \in Q$. This is precisely the statement that $Q \subseteq Z(G)$ and we are done. □

SOLUTION TO EXERCISE 3.12. Let $Q \cong \mathbb{Z}/55\mathbb{Z}$ be a subgroup of G. We first make the observation that $165 = 3{\cdot}5{\cdot}11$ and therefore $[G : Q] = 3$, which is the minimal prime dividing the order of G. Hence, $Q \lhd G$. Let now R be a 3-Sylow subgroup of G. Then $Q \cap R = \{e\}$ and therefore $G = Q \rtimes R$. This semidirect product is induced by a homomorphism

$$\phi : R \longrightarrow \mathrm{Aut}(Q).$$

However, $|R| = 3$ and $|\mathrm{Aut}(Q)| = |\mathrm{Aut}(\mathbb{Z}/55\mathbb{Z})| = |(\mathbb{Z}/55\mathbb{Z})^\times| = \varphi(55) = 40$. This implies that ϕ is the trivial homomorphism. Then, as the semidirect product of Abelian groups ($Q \cong \mathbb{Z}/5\mathbb{Z}$ and $R \cong \mathbb{Z}/3\mathbb{Z}$), it follows from a previous exercise that G is Abelian. □

SOLUTION TO EXERCISE 3.13. From Exercise 3.4 we know that G will contain a normal subgroup of prime order, say, r. Let N be such a subgroup in G and consider the quotient group G/N which will have order $[G : N] = pq$. Without loss of generality assume that $p < q$ and invoke Cauchy's theorem to find an element $x \in G/N$ having order precisely q. Define $\bar{K} := \langle x \rangle$ and notice that $\bar{K} \lhd G/N$ since the index of $\bar{K}$ in G/N is p, the minimal prime diving the order of the group.

We now recall the existence of a canonical surjective group homomorphism π_N which takes $G \longrightarrow G/N$ via $g \mapsto gN$. If we set $K := \pi_N^{-1}(\bar{K})$, then K will contain $N = \mathrm{Ker}\,\pi_N$ and $K \lhd G$ (by the correspondence theorems). Also, by the first isomorphism theorem

$$K/N \cong \bar{K}\text{‘}$$

whence it follows that $|K| = qr$. This allows us to construct a normal series

$$\{e\} = G_0 \lhd N \lhd K \lhd G$$

where each quotient has prime order, and is therefore Abelian. It follows from this that G is solvable. □

4. Solutions to Problems in Chapter 4

SOLUTION TO EXERCISE 4.1. We repeat the "standard" argument used in the lemma. Note first that $\mathrm{End}_G(V)$ is never empty, since if $\mathsf{Z} : V \to V$ is the zero-map:

$$\mathsf{Z}(\rho(g)v) = \mathbf{0}_V = \rho(g)(Zv).$$

Let us now fix an endomorphism of representations $T \in \mathrm{End}_G(V)$ and let $\lambda \in \mathbb{C}$ be an eigenvalue of T. If V_λ is the corresponding (non-zero) eigenspace, we claim that (ρ, V_λ) is

a sub-representation of G. Certainly, if $g \in G$ and $u \in V_\lambda$ observe that

$$T(\rho(g)u) = \rho(g)(Tu) = \rho(g)(\lambda u) = \lambda\rho(g)u.$$

Thus, $\rho(g)(V_\lambda) \subseteq V_\lambda$. Since V_λ is non-zero and (ρ, V) is irreducible, we conclude that $V_\lambda = V$ whence $T = \lambda \cdot I$. Conversely, if $T = \lambda I$ for some $\lambda \in \mathbb{C}$ it is obvious by linearity of ρ that $T \circ \rho(g) = \rho(g) \circ T$ on V.

We now define a mapping

$$\Gamma : \mathbb{C} \longrightarrow \mathrm{End}_G(V), \quad \zeta \mapsto \zeta \cdot I.$$

First, this is surjective by what we have already checked. It is also clear that Γ is injective. Now, it must be a homomorphism of vector spaces since

$$\Gamma(\zeta + \xi) = (\zeta + \xi) \cdot I = \zeta \cdot I + \xi \cdot I = \Gamma(\zeta) + \Gamma(\xi).$$

We conclude that $\mathrm{End}_G(V) \cong \mathbb{C}$. □

SOLUTION TO EXERCISE 4.2. Note that $z \in Z(G)$ is precisely the statement that z commutes with every element g of G. By virtue of the previous exercise, it suffices to check that $\rho(z) \in \mathrm{End}_G(V)$.

To this end, let $g \in G$ be given and fix $v \in V$. We calculate

$$(\rho(z) \circ \rho(g))(v) = \rho(zg)(v) = \rho(gz)(v) = (\rho(g) \circ \rho(z))(v).$$

This concludes the proof. □

SOLUTION TO EXERCISE 4.3. Let $\Gamma : \mathbb{C} \longrightarrow \mathbb{C}$ be an isomorphism of vector spaces. Notice that $\Gamma(z) = 0$ if and only if $z = 0$. Therefore, $\Gamma(1) = \alpha \in \mathbb{C}^\times$. Now, by linearity, if $z \in \mathbb{C}$ then $\Gamma(z) = \Gamma(z \cdot 1) = z\Gamma(1) = \alpha z$. Therefore, the only automorphisms (as a vector space!) of $\mathbb{C}$ is the linear map $\zeta \mapsto \alpha\zeta$ for $\alpha \in \mathbb{C}^\times$.

It is easy to check that $\mathrm{Aut}(\mathbb{C})$ forms a group under the composition of maps. We now consider the association $\mathbb{C}^\times \longrightarrow \mathrm{Aut}(\mathbb{C})$ where we take α to the map $\Gamma_\alpha(z) := \alpha z$. Obviously, this is a well defined bijection. Since it is clearly also a group homomorphism, we conclude that $\mathrm{Aut}(\mathbb{C}) \cong \mathbb{C}^\times$. □

SOLUTION TO EXERCISE 4.4. Let $\{g_1, \ldots, g_{\mathsf{h}}\}$ be representatives for the h conjugacy classes of G. Define for $i, j \in \mathbb{N}$

$$m_{ij} := \frac{1}{\sqrt{\mathrm{C}(g_j)}}\chi_i(g_j).$$

Invoking character orthogonality, we find that

$$\begin{aligned}\delta_{ik} = \langle \chi_i, \chi_k \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_k(g)} &= \frac{1}{|G|} \sum_{j=1}^{\mathsf{h}} |\mathrm{Conj}(g_j)|\, \chi_i(g_j)\overline{\chi_k(g_j)} \\ &= \sum_{j=1}^{\mathsf{h}} \left(\frac{1}{\sqrt{\mathrm{C}(g_j)}} \right)^2 \chi_i(g_j)\overline{\chi_k(g_j)} \\ &= \sum_{j=1}^{\mathsf{h}} m_{ij}\overline{m_{kj}}.\end{aligned}$$

This means that the matrix $M = (m_{ij})$ is unitary. Therefore, the transpose of M is also unitary whence it follows that

$$\delta_{ik} = \delta_{ki} = \sum_{j=1}^{\mathsf{h}} m_{ji}\overline{m_{jk}} = \sum_{j=1}^{\mathsf{h}} \frac{1}{\sqrt{|\mathrm{C}(g_i)|} \cdot \sqrt{|\mathrm{C}(g_k)|}} \chi_j(g_i)\overline{\chi_j(g_k)}.$$

The statement in (4.4) readily follows. □

Solution to Exercise 4.5. Since G is Abelian, for each $x \in G$ we have $\{x\} = \mathrm{Conj}(x)$. That is, there are n conjugacy classes in G whence $\mathsf{h} = n$. Also, we know that

$$|G| = \sum_{j=1}^{\mathsf{h}} \dim(\rho_j)^2$$

where the ρ_j are representatives for the irreducible representations. Hence,

$$n = \sum_{j=1}^{n} \dim(\rho_j)^2.$$

This implies that $\dim(\rho_j) = 1$ for every j. To complete this proof, it now suffices to check that the character of a one dimensional representation $(\rho, \mathbb{C})$ is a homomorphism $G \longrightarrow \mathbb{C}^\times$. To see this, let $g \in G$ and observe that

$$\chi_\rho(g) = \mathrm{Tr}(\rho(g)) \in \mathbb{C}^\times$$

since an automorphism of $\mathbb{C}$ is a function $f(z) = \alpha z$ for $\alpha \neq 0$. This is precisely the matrix $[\alpha]$ which has α as its trace. Furthermore, if $x, y \in G$ then

$$\chi_\rho(xy) = \mathrm{Tr}(\rho(xy)) = \mathrm{Tr}(\rho(x)\rho(y))$$

which shows that χ is a homomorphism (since the trace is multiplicative over vector spaces of dimension 1). □

SOLUTION TO EXERCISE 4.6. We start with $\mathbb{Z}/3\mathbb{Z}$. Since G is Abelian, its class number is 3 and we shall therefore have 3 characters to chart. We obtain the following skeleton for the table of $\mathbb{Z}/3\mathbb{Z}$:

$\mathbb{Z}/3\mathbb{Z}$	0	1	2
χ_1	1	1	1
χ_2	1	?	?
χ_3	1	?	?

We have used that every representations is one dimensional to fill out the first column. Now, we know that $1 = \chi_2(0) = \chi_2(1+1+1) = \chi_2(1)^3$. Therefore, it makes sense to consider the option

$$\chi_2(1) = e^{\frac{2\pi i}{3}}.$$

The purpose of the 2 will shortly become obvious. Now, since $\chi_2(2) = \chi_1(1)^2$ we obtain

$\mathbb{Z}/3\mathbb{Z}$	0	1	2
χ_1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	?	?

Likewise, we find that

$\mathbb{Z}/3\mathbb{Z}$	0	1	2
χ_1	1	1	1
χ_2	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_3	1	$e^{-2\pi i/3}$	$e^{-4\pi i/3}$

□

SOLUTION TO EXERCISE 4.7. The sum of entries in any given column will be of the form

$$\sum_{\chi_j} \chi_j(g)$$

where $g \in G$ is fixed and the sum ranges over all orthonormal characters (considered up to isomorphism of irreducible representations). By Exercise 4.4, we know that

$$\sum_{\chi_j} \chi_j(g)\overline{\chi_j(e)} = 0.$$

Since $\chi_j(e) = 1$ we are done. □

SOLUTION TO EXERCISE 4.8. We first determine the character table of $\mathbb{Z}/4\mathbb{Z}$ using the same methods of the previous problem. Again, since $\mathbb{Z}/4\mathbb{Z}$, all irreducible non-isomorphic

representations are one-dimensional. Thus, we wish to fill in the following skeleton for our table of characters

$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	?	?	?
χ_3	1	?	?	?
χ_4	1	?	?	?

The fact that χ_2 will be a homomorphism $G \longrightarrow \mathbb{C}^\times$ tells us that $\chi_2(1)^4 = 1$. Therefore,

$$\chi_2(1) = e^{\alpha\pi i/4}$$

for some $\alpha \in \mathbb{Z}$. We cannot have $\alpha = 0$ (in this case we obtain the trivial representation) and $\alpha = 1$ will not satisfy $\chi_2(1)^4 = 1$. Our first candidate is therefore $\chi_2(1) = e^{\pi i/2} = i$ which will indeed generate a homomorphism (1 generates $\mathbb{Z}/4\mathbb{Z}$). Filling in this row gives

$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	?	?	?
χ_4	1	?	?	?

For χ_3 we employ a similar argument and find that a suitable value of $\chi_3(1)$ is $e^{\pi i} = -1$. We may therefore add another row to our table:

$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	?	?	?

Using column orthogonality, we complete our table

$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i

Let χ_ρ be the character of ρ. Obviously $\chi_\rho(1) = \dim(\mathbb{C}^2) = 2$. Also,

$$\chi_\rho(1) = \mathrm{Tr}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = 0$$

and

$$\chi_\rho(2) = \mathrm{Tr}\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2\right] = \mathrm{Tr}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -2.$$

Finally,

$$\chi_\rho(3) = \mathrm{Tr}\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^3\right] = \mathrm{Tr}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 0.$$

Adding this to our character table,

$\mathbb{Z}/4\mathbb{Z}$	0	1	2	3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i
χ_ρ	2	0	-2	0

It is clear that $\chi_\rho \equiv \chi_2 + \chi_4$. Hence, $\rho \cong \rho_2 \oplus \rho_4$. □