Group Theory

Ronnie Sebastian

Contents

Chapter 1

Groups

In this chapter we see some basic definitions.

1.1 Bijective maps

1.1.1. **Injective maps**. Let X and Y be two sets. A map $f : X \to Y$ is called injective if it takes distinct elements of X to distinct elements of Y. That is, if $a, b \in X$ and $a \neq b$ then $f(a) \neq f(b)$. Here are some examples which illustrate the point.

1. Let $X = \{0, 1\}$ and let $Y = \{4, 6, 9\}$. Let $f : X \to Y$ be defined by $f(0) = 4$ and $f(1) = 6$. Then clearly f is injective.

2. Let $X = \{0, 1\}$ and let $Y = \{4, 6, 9\}$. Clearly there are no injective maps from $Y \to X$ since the size of Y is 3 and the size of X is 2. Thus, for any map $f : Y \to X$ there will be two elements of Y which map to the same element of X.

3. Let X be a set of size n and let Y be a set of size m. The total number of maps from X to Y is m^n. If $n > m$ then there are no injective maps from X to Y. If $n \leq m$ then there are $m!/(m-n)!$ injective maps from X to Y. The proofs of these simple assertions are left to the reader.

1.1.2. **Surjective maps**. A map $f : X \to Y$ is called surjective if every element of Y is contained in the image of X.

1. The map $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not surjective, since negative numbers will not be in the image of f.

2. The map $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is surjective. This map is also injective.

3. Let $\mathbb{Z}/m\mathbb{Z}$ denote the set $\{0, 1, \ldots, m-1\}$. Then there is a natural map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given as follows. For every integer n there is an integer k such that $km \leq n < (k+1)m$. Then the map is given by sending $n \mapsto n - km$, or in simple terms, it is the remainder that we get when we divide n by m.

1.1.3. **Bijective maps from $X \to Y$.** A map $f : X \to Y$ which is both injective and surjective is called a bijective map. If $f : X \to Y$ is a bijective map, then we can define its "inverse". Define a map $g : Y \to X$ as follows. Since f is a bijection, for every $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. Define $g(y) := x$. From the definition of g it is clear that $g \circ f = Id_X$ and that $f \circ g = Id_Y$. These equalities can be checked simply by applying them on elements of X and Y. For example, if $y \in Y$, let x be the unique element in X such that $f(x) = y$. Then by definition $g(y) = x$. So we get

$$(f \circ g)(y) = f(g(y)) = f(x) = y = Id_Y(y)\,.$$

This proves that $f \circ g = Id_Y$. Similarly, one may show that $g \circ f = Id_X$.

Using the above we may show that g is unique. That is, if $h : Y \to X$ is any other map such that $h \circ f = Id_X$ then $h = g$. To see this we apply g on the right on both sides. Then we get

$$h \circ f \circ g = Id_X \circ g = g\,.$$

But we also have that

$$h \circ f \circ g = h \circ Id_Y = h\,.$$

Combining these we get that $h = g$. Similarly, one may check that if $h : Y \to X$ is such that $f \circ h = Id_Y$ then too we get $h = g$. This is left as an exercise to the reader.

It is also easy to check that g is bijective. Surjectivity follows from the identity $g \circ f = Id_X$. Applying both sides to $x \in X$ we get $g(f(x)) = x$. This shows that every $x \in X$ is in the image of g. To show injectivity, suppose $a, b \in Y$ are such that $g(a) = g(b)$, then applying f to both sides we get $f(g(a)) = f(g(b))$. Since $f \circ g = Id_Y$ it follows that $a = b$.

Let us record the conclusion of the above discussion in the following proposition.

Proposition 1.1.4. *Let $f : X \to Y$ be a bijective map. Then there is a unique bijective map $g : Y \to X$ which satisfies $g \circ f = Id_X$ and $f \circ g = Id_Y$.*

1.2 Automorphisms of a set

1.2.1. **Bijective maps from $X \to X$.** Now we apply the preceding discussion to the case when $Y = X$. From the preceding subsection we conclude that given a bijective map $f : X \to X$, there is a unique bijective map $g : X \to X$ such that $f \circ g = Id_X$ and $g \circ f = Id_X$. Moreover, one easily checks that if f and g are bijective maps from $X \to X$ then the composition $f \circ g$ is also bijective.

Definition 1.2.2. *Let X be a set. Denote the set of bijective maps from $X \to X$ by $\mathrm{Aut}(X)$. Bijective maps are also referred to as automorphisms.*

Then from Proposition 1.1.4 we conclude the following.

Proposition 1.2.3. *The set $\mathrm{Aut}(X)$ and the operation*

$$\circ : \mathrm{Aut}(X) \times \mathrm{Aut}(X) \to \mathrm{Aut}(X) \qquad (f, g) \mapsto f \circ g$$

satisfies the following properties.

(1) If $f, g, h \in \mathrm{Aut}(X)$ then $(f \circ g) \circ h = f \circ (g \circ h)$

(2) There is an element $Id_X \in \mathrm{Aut}(X)$ such that $f \circ Id_X = f = Id_X \circ f$ for all $f \in \mathrm{Aut}(X)$

(3) For every $f \in \mathrm{Aut}(X)$ there is a unique $g \in \mathrm{Aut}(X)$ such that $f \circ g = g \circ f = Id_X$.

Proof. The assertion (1) is a basic property of maps between sets, often referred to associativity. The remaining assertions are clear from Proposition 1.1.4. □

A group, which we now define, is an abstraction of the above properties.

1.3 Groups

Definition 1.3.1. *A group is a triple (G, m, e) consisting of the following.*

(1) G is a set and $e \in G$ is an element.

(2) $m : G \times G \to G$ is a map such that $m(a, m(b, c)) = m(m(a, b), c)$.

(3) For all $g \in G$ we have $m(g, e) = m(e, g) = g$.

(4) For all $g \in G$ there is an h such that $m(g, h) = e$.

The element $e \in G$ is referred to as the identity of the group. The map m is referred to as the multiplication law, or the group law. Let us now see some examples of groups.

Example 1.3.2. We have already seen this example of a group. Let X be a set. Define

$$m : \mathrm{Aut}(X) \times \mathrm{Aut}(X) \to \mathrm{Aut}(X)$$

by $m(f, g) := f \circ g$. Then the triple $(\mathrm{Aut}(X), m, Id_X)$ is a group. This is the content of Proposition 1.2.3. If we take X to be the set $\{1, 2, \ldots, n\}$, then the group $\mathrm{Aut}(X)$ is often written as S_n and is called the symmetric group on n letters.

Example 1.3.3. Let $\mathbb{Z}$ denote the set of integers. For two integers m, n define $a(m, n) := m + n$. Then the triple $(\mathbb{Z}, a, 0)$ is a group.

Example 1.3.4. Let $\mathbb{Q}$ denote the set of rational numbers. For two rational numbers α, β define $a(\alpha, \beta) := \alpha + \beta$. Then the triple $(\mathbb{Q}, a, 0)$ is a group.

Example 1.3.5. Let $\mathbb{R}$ denote the set of real numbers. For two real numbers α, β define $a(\alpha, \beta) := \alpha + \beta$. Then the triple $(\mathbb{R}, a, 0)$ is a group.

Example 1.3.6. The above can be generalized to $\mathbb{R}^n$. For any two vectors $\underline{\alpha}, \underline{\beta}$ we have the addition map $a(\underline{\alpha}, \underline{\beta}) = \underline{\alpha} + \underline{\beta}$. The triple $(\mathbb{R}^n, a, 0)$ is a group.

Example 1.3.7. Consider the set $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$. For two elements in this set define $m(a, b) = ab$. Clearly, m is a map from $\mathbb{Q}^\times \times \mathbb{Q}^\times \to \mathbb{Q}^\times$. The triple

$(\mathbb{Q}^\times, m, 1)$ is a group.

Example 1.3.8. Consider the set $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$. For two elements in this set define $m(a, b) = ab$. Clearly, m is a map from $\mathbb{R}^\times \times \mathbb{R}^\times \to \mathbb{R}^\times$. The triple $(\mathbb{R}^\times, m, 1)$ is a group.

Example 1.3.9. Consider the set $S := \{\pm 1\}$. For two elements in this set define $m(a, b) = ab$. Clearly, m is a map from $S \times S \to S$. The triple $(S, m, 1)$ is a group.

Example 1.3.10. Define $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$. Then the triple $(\mathbb{C}^\times, m, 1)$ forms a group, where m as above, is the usual multiplication of complex numbers.

Example 1.3.11. Let $S^1 \subset \mathbb{C}^\times$ be the set of complex numbers with absolute value 1.

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$$

Then the triple $(S^1, m, 1)$ is a group.

Example 1.3.12. Let us denote by V a vector space over $\mathbb{R}$. Recall that a map $f : V \to V$ is called linear if for every $\lambda \in \mathbb{R}$ and $v, w \in V$ we have $f(\lambda v + w) = \lambda f(v) + f(w)$. We claim that the set of bijective linear maps from $V \to V$ forms a group under composition of maps. Let $\mathrm{Aut}_{\mathrm{lin}}(V)$ denote the space of these maps.

It is clear that $Id_V \in \mathrm{Aut}_{\mathrm{lin}}(V)$ and that for every $f \in \mathrm{Aut}_{\mathrm{lin}}(V)$ we have $f \circ Id_V = Id_V \circ f$.

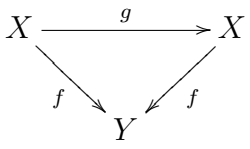
Let $f \in \mathrm{Aut}_{\mathrm{lin}}(V)$ be a bijective linear map. Since $f : V \to V$ is bijective, let g denote its inverse. We claim that g is a linear map. To check this we need to show for $\lambda \in \mathbb{R}$ and $v, w \in V$ we have $g(\lambda v + w) = \lambda g(v) + g(w)$. Since f is a bijection, this equality holds iff if it holds after applying f. That is,

$$\begin{aligned} g(\lambda v + w) = \lambda g(v) + g(w) \qquad &\iff \qquad f(g(\lambda v + w)) = f(\lambda g(v) + g(w)) \\ &\iff \qquad \lambda v + w = \lambda f(g(v)) + f(g(w)) \\ &\iff \qquad \lambda v + w = \lambda v + w \end{aligned}$$

In the above we have used that $f \circ g = Id_V$ and that f is linear. The above computation shows that g is linear. Since g is a bijection and it is linear, it follows that $g \in \mathrm{Aut}_{\mathrm{lin}}(V)$. We know that $f \circ g = Id_V = g \circ f$.

Thus, the triple $(\mathrm{Aut}_{\mathrm{lin}}(V), m, Id_V)$, where $m(f,g) = f \circ g$, is a group.

Example 1.3.13. We can construct examples of groups by considering more complicated examples of automorphisms. Let $f : X \to Y$ be a map of sets. Let $g : X \to X$ be a map such that $f \circ g = f$. This is equivalent to saying that the following diagram commutes



Let

$$\mathrm{Aut}_Y(X) := \{g \mid f \circ g = f,\ \ g \text{ is a bijection}\}\,.$$

It is an easy exercise to check that $\mathrm{Aut}_Y(X)$ is a group under composition of maps. We leave this check to the reader.

Suppose (G, m, e) is a group, then there is only one element $e \in G$ which satisfies the property that $m(g, e) = m(e, g) = g$ for all $g \in G$. Let us prove this. However, before that, we simplify our notation as follows. From now on we will suppress the m. If a, b are elements of G, then we will simply write $a \cdot b$ to mean the element $m(a, b)$. In this notation, the associativity condition will be written as $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Proposition 1.3.14. *There is only one element $a \in G$ which satisfies the property of the identity, that is, $g \cdot a = a \cdot g = g$ for all $g \in G$ implies $a = e$.*

Proof. Suppose there is a $g \in G$ such that $g \cdot a = g$. Let h denote an element such that $h \cdot g = e$. Applying h to both sides of the equation $g \cdot a = g$ we get

$$h \cdot (g \cdot a) = h \cdot g = e\,.$$

By associativity one get

$$(h \cdot g) \cdot a = (e \cdot a) = a\,.$$

This proves that $a = e$. □

Proposition 1.3.15. *Given $g \in G$, there is exactly one element $h \in G$ such that $g \cdot h = e$.*

Proof. That there is an h such that $g \cdot h = e$ is axiom (4) in the definition of a group. Suppose there is an x such that $g \cdot x = e$. We need to show that $x = h$. Let $x' \in G$ be such that $x \cdot x' = e$. By axiom (4) in the definition of a group, there is such an x'. Then we get

$$(g \cdot x) \cdot x' = (e \cdot x') = x' = g \cdot (x \cdot x') = g \cdot e = g\,.$$

This shows that $x' = g$ and so we get $x \cdot g = e$. From this we get

$$x \cdot (g \cdot h) = x \cdot e = x = (x \cdot g) \cdot h = e \cdot h = h\,.$$

This proves that $x = h$. □

Proposition 1.3.16. *Given $g \in G$, there is exactly one element $h \in G$ such that $h \cdot g = e$.*

Proof. First we need to show that there is such an h. There is an $h \in G$ such that $g \cdot h = e$, by axiom (4) in the definition of a group. There is an $h' \in G$ such that $h \cdot h' = e$. Then

$$(g \cdot h) \cdot h' = e \cdot h' = h' = g \cdot (h \cdot h') = g \cdot e = g\,.$$

This shows that $h' = g$ and so we get $h \cdot g = e$. This proves the existence of an h such that $h \cdot g = e$. Suppose $x \in G$ is such that $x \cdot g = e$. Then we get

$$(x \cdot g) \cdot h = e \cdot h = h = x \cdot (g \cdot h) = x \cdot e = x\,.$$

This shows that $x = h$, which proves the uniqueness. □

Corollary 1.3.17. *Let $g \in G$. Then there is a unique $h \in G$ such that $h \cdot g = g \cdot h = e$.*

Proof. By axiom (4) in the definition of a group there is an $h \in G$ such that $g \cdot h = e$. By Proposition 1.3.15 it follows that such an h is unique. By Proposition 1.3.16 there is an $h' \in G$ such that $h' \cdot g = e$. We need to show that $h' = h$. We have already done this twice, but let us do it once again. We have

$$h' \cdot (g \cdot h) = h' \cdot e = h' = (h' \cdot g) \cdot h = e \cdot h = h\,.$$

This completes the proof of the Corollary. □

Definition 1.3.18. *Let $g \in G$ be an element. If there is no positive integer i such that $g^i = e$ then we say that g has infinite order. If there is a positive integer i such that*

$$g^i = \underbrace{g \cdot g \cdot \ldots \cdot g}_{i} = e,$$

then the smallest such i is called the order of g and denote $O_G(g)$.

1.4 Symmetric groups

Let X denote the set $\{1, 2, \ldots, n\}$. Recall that in Example 1.3.2 we denoted by S_n the group $\mathrm{Aut}(X)$. We will be referring to this group on numerous occasions, and so it will be useful to look at it now in detail and fix some notation. The easiest way to explain this is by means of some examples.

1.4.1. $n = 1$. In this case $S_1 = \{e\}$.

1.4.2. $n = 2$. In this case $X = \{1, 2\}$. There are two bijective maps from X to itself. Such a map is either the identity or it is given by $f(1) = 2$ and $f(2) = 1$. Thus, S_2 is a group of size two. If $f \in S_2$ is the non-trivial element, then we write f as $f_{(12)}$. This means that f takes 1 to 2 and it takes 2 to 1. Note that we could have written f as $f_{(21)}$ also. It is clear, simply by checking on elements of X, that $f_{(12)} \circ f_{(12)} = Id$. The only element which has order 1 is the identity element. Since $f_{(12)} \neq Id$ its order is not 1. This shows that the order of the element $f_{(12)} \in S_2$ is 2.

1.4.3. $n = 3$. In this case $X = \{1, 2, 3\}$. There are 6 bijective maps from X to itself. We list these using the above method.

- $Id = f_{(1)(2)(3)}$ - The identity map.
- $f_{(12)(3)}$ - This map takes $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$. Check it has order 2.
- $f_{(13)(2)}$ - This map takes $1 \mapsto 3$, $3 \mapsto 1$, $2 \mapsto 2$. Check it has order 2.
- $f_{(23)(1)}$ - This map takes $2 \mapsto 3$, $3 \mapsto 2$, $1 \mapsto 1$. Check it has order 2.
- $f_{(123)}$ - This map takes $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. Check it has order 3.
- $f_{(132)}$ - This map takes $1 \mapsto 3$, $3 \mapsto 2$, $2 \mapsto 1$. Check it has order 3.

We leave it to the reader to check that $f_{(12)} \circ f_{(13)} = f_{(132)}$.

1.4.4. $n = 4$. For $n = 4$ there are 24 elements in the group S_4. The interested reader may attempt to list all the elements. However, we list a few.

- $Id = f_{(1)(2)(3)(4)}$ - The identity map.
- $f_{(12)(43)}$ - This map takes $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$, $4 \mapsto 3$. Check it has order 2.

- $f_{(14)(32)}$ - This map takes $1 \mapsto 4$, $4 \mapsto 1$, $3 \mapsto 2$, $2 \mapsto 3$. Check it has order 2.
- $f_{(23)(1)(4)}$ - This map takes $2 \mapsto 3$, $3 \mapsto 2$, $1 \mapsto 1$, $4 \mapsto 4$. Check it has order 2.
- $f_{(312)(4)}$ - This map takes $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, $4 \mapsto 4$. Check it has order 3.
- $f_{(1432)}$ - This map takes $1 \mapsto 4$, $4 \mapsto 3$, $3 \mapsto 2$, $2 \mapsto 1$. Check it has order 4.

It is an easy exercise to see that the size of S_n is $n!$.

1.4.5. **Simplifying the notation**. Now we make some simplifications in the above notations.

(1) We will drop the f from now on. So, for example, when we write $(12)(3) \in S_3$, we mean the map $f_{(12)(3)} \in S_3$.

(2) We will drop those elements in the notation on which the map acts by identity. So, for example, the element $(12) \in S_3$ will mean the element $(12)(3) \in S_3$. In other words, if an element of X does not occur in the representation of the map, then the map is supposed to fix this element. For example, when we write $(12)(34) \in S_6$, we mean the map $f_{(12)(34)(5)(6)} \in S_6$.

We may rephrase some of the earlier observations using the above notation. Earlier we saw that $f_{(12)} \circ f_{(12)} = Id$, for $f_{(12)} \in S_2$. This will be written as $(12)(12) = e$. Similarly, one of the checks that was left to the reader was that for $f_{(12)}, f_{(13)} \in S_3$ satisfy $f_{(12)} \circ f_{(13)} = f_{(132)}$. This will be written as $(12)(13) = (132)$. To make sure that the reader has understood the above notations, we give a list of exercises along with their solutions. If the reader can solve these problems correctly, then he/she has probably understood correctly what is going on.

(1) Let $(123), (132) \in S_3$. Show that $(123)(132) = e$. (e denotes the identity element)

(2) Let $(123), (134) \in S_4$. Show that $(123)(134) = (1)(234) = (234)$.

(3) Let $(12), (13) \in S_4$. Show that $(12)(13) = (132)$.

(4) Let $(12), (13) \in S_{17}$. Show that $(12)(13) = (132)$.

(5) Let $(1234) \in S_4$. Show that $(1234)(1234)(1234)(1234) = e$.

(6) Let $(12), (3, 10) \in S_{107}$. Show that $(1, 2)(3, 10) = (3, 10)(1, 2)$.

(7) Let $(12), (23), (14) \in S_6$. Show that $(12)(23)(14) = (1423)$.

(8) Let $(12), (23), (14256) \in S_6$. Show that $(12)(23)(14256) = (143)(256)$.

(9) Let $(12), (23), (14256) \in S_6$. Show that $(12)(14256)(23) = (14)(2356)$.

We hope that the above exercises familiarize the reader with the notation described above.

Definition 1.4.6. *(1) Let $a_1, a_2, \ldots, a_r$ be distinct elements of $\{1, 2, \ldots, n\}$. Then the element $(a_1, a_2, \ldots, a_r) \in S_n$ is called a cycle.*

(2) Two cycles $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_s)$ in S_n are said to be disjoint if the sets $\{a_1, a_2, \ldots, a_r\}$ and $\{b_1, b_2, \ldots, b_s\}$ are disjoint.

For example, in S_{17} the two cycles $(2, 13, 16, 9)$ and $(4, 1, 15, 3, 7, 16)$ are disjoint. But neither of these cycles is disjoint with the cycle (42). We have the following theorem.

Theorem 1.4.7. *We have in the group S_n*

(1) If $\alpha = (a_1, a_2, \ldots, a_r)$ and $\beta = (b_1, b_2, \ldots, b_s)$ are two disjoint cycles then $\alpha\beta = \beta\alpha$.

(2) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then

$$(a_1, a_2, \ldots, a_r) = (a_1, a_2)(a_2, a_3)(a_3, a_4) \ldots (a_{r-1}, a_r).$$

(3) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then its inverse is $(a_r, a_{r-1}, \ldots, a_3, a_2, a_1)$.

(4) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then it has order r.

(5) Every element of S_n can be written as a product of disjoint cycles.

(6) If an element is written as a product of disjoint cycles $c_1c_2\dots c_l$ and $c'_1c'_2\dots c'_s$ in two ways, then $l = s$ and the cycles c_i are equal to the cycles c'_j up to permutation. In other words, every element is written as a product of disjoint cycles in a "unique" way.

Proof. The first four assertions are easy and are left to the reader. The last two assertions will be proved in chapter 4, see Theorem 4.5.1. □

1.5 Exercises

1.5.1. Let $\beta \in S_n$ be a cycle and write $\beta = (a_1, a_2, \dots, a_r)$. For any $\gamma \in S_n$ show that $\gamma\beta\gamma^{-1} = (\gamma(a_1), \gamma(a_2), \dots, \gamma(a_r))$.

1.5.2. Let $Y \subset G$ be a subset. We say that Y generates G if every element of G can be written as a product $x_1x_2\dots x_r$ where each $x_i \in Y$. Note that we do not require that the x_i's be distinct. Show that

1. The transpositions $(1,2), (1,3), \dots, (1,n)$ generate S_n.
2. The transpositions $(1,2), (2,3)\dots, (n-1,n)$ generate S_n.
3. The transposition $(1,2)$ and the cycle $(1,2,\dots,n)$ generate S_n.

Chapter 2

Subgroups

2.1 Subgroups

From now on,

- instead of writing, "Let (G, m, e) be a group", we will simply say that G is a group,
- the group multiplication will be obvious from the context and it will often be suppressed. For elements $a, b \in G$ we will simply write ab instead of $a \cdot b$ or $m(a, b)$,
- when we take products of 3 or more elements, associativity allows us not to worry about the order in which the multiplication is done. Thus, for example, we will simply write abc for $(ab)c = a(bc)$.

Lemma 2.1.1. *Let $H \subset G$ be a subset which satisfies the following two conditions:*

(1) If $a, b \in H$ then $a \cdot b \in H$.

(2) If $a \in H$ then $a^{-1} \in H$.

Then H is a group.

Proof. The first condition defines the group multiplication in H. In fact, the multiplication is the same as that in G. The second condition shows that every element in H has an inverse in H. This shows proves that H is a group. □

Definition 2.1.2. *Let $H \subset G$ be a subset which satisfies the following two conditions:*

(1) If $a, b \in H$ then $a \cdot b \in H$.

(2) If $a \in H$ then $a^{-1} \in H$.

Then H is a called a subgroup of G. The word "subgroup" is justified by the previous lemma.

Let us see some examples of groups and their subgroups.

Example 2.1.3. Every group has two obvious subgroups. The first is the subgroup $H = \{e\}$ which contains only the identity element. The second is the subgroup $H = G$, that is, the entire group.

Example 2.1.4. Let X be a set and consider the group $\mathrm{Aut}(X)$ of bijective maps from X to itself. Let $Y \subset X$ be any subset. Let $H \subset \mathrm{Aut}(X)$ be the set

$$\mathrm{Aut}(X, Y) = \{\phi \in \mathrm{Aut}(X) \,|\, \phi(Y) = Y\}\,.$$

Then it is easy to check that $\mathrm{Aut}(X, Y)$ is a subgroup of $\mathrm{Aut}(X)$. For example, if we take $X = \{1, 2, 3, 4\}$, consider the group S_4 and we take $Y = \{2, 3\}$, then

$$\mathrm{Aut}(X, Y) = \{e, (23), (14), (23)(14)\}\,.$$

Example 2.1.5. Let X be a set and consider the group $\mathrm{Aut}(X)$ of bijective maps from X to itself. Let $Y \subset X$ be any subset. Let $H \subset \mathrm{Aut}(X)$ be the set

$$\{\phi \in \mathrm{Aut}(X) \,|\, \phi(y) = y \qquad \text{for all } y \in Y\}\,.$$

Then it is easy to check that H is a subgroup of $\mathrm{Aut}(X)$. It is also easy to check that H is a subgroup of $\mathrm{Aut}(X, Y)$. For example, if we take $X = \{1, 2, 3, 4\}$, consider the group S_4 and we take $Y = \{2, 3\}$, then

$$H = \{e, (14)\}\,.$$

Example 2.1.6. The above examples are of the following nature. Let $\mathcal{P}$ be a property of maps such that if $f, g \in \mathcal{P}$ then $f \circ g \in \mathcal{P}$. Then define $H_{\mathcal{P}}$ to be the collection of those f such that f satisfies $\mathcal{P}$. We can modify this idea a little to generate several subgroups of a group G. Let G be a group and let $S \subset G$ be a subset. Define

- $N_G(S) := \{g \in G \mid gxg^{-1} \in S \qquad \text{for all } x \in S\}$
- $C_G(S) := \{g \in G \mid gx = xg \qquad \text{for all } x \in S\}$

One easily checks that both $N_G(S)$ and $C_G(S)$ are subgroups of G. The first is called the ***normalizer*** of S and the second is called the ***centralizer*** of S.

Example 2.1.7. Let $\mathbb{Z}$ denote the group of integers. For any integer $n \in \mathbb{Z}$ we define $H_n := n\mathbb{Z}$. It is clear that H_n is a subgroup of $\mathbb{Z}$.

Example 2.1.8. Let $n > 0$ be an integer and consider the set

$$\mu_n := \{e^{2\pi ik/n} \in \mathbb{C} \,|\, 0 \leq k < n\}\,.$$

It is clear that μ_n is a subgroup of S^1, see Example 1.3.11.

Example 2.1.9. Let H be a subgroup of G and let K be a subgroup of H. Then it is clear that K is a subgroup of H. For example, $mn\mathbb{Z} \subset n\mathbb{Z} \subset \mathbb{Z}$ are subgroups.

Example 2.1.10. Given a group G and an element $g \in G$, we can form a subgroup using this element. We simply take the subgroup "generated" by g, that is,

$$H_{\langle g\rangle} := \{g^i := \underbrace{g \cdot g \cdot \ldots \cdot g}_{i} \mid i > 0\} \cup \{e\} \cup \{g^i := \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{-i} \mid i < 0\}\,.$$

In other words, we take all possible integral powers of the element g. We caution the reader that it is not necessary that all these powers have to be distinct. For example, if we take the group $G = \mu_n$ and let $g = e^{2\pi i/n}$, then $g^i = g^{i+n}$ for all i.

Proposition 2.1.11. *Let G be a group and let $g \in G$. The cardinality of the subgroup $H_{\langle g\rangle}$ is equal to the order of g.*

Proof. First consider the case when g has infinite order. We claim that $H_{\langle g\rangle}$ has infinite order. If not, there are two integers $i < j$ such that $g^i = g^j$. Multiplying both sides with $(g^{-1})^j$ we get that

$$g^{j-i} = e\,.$$

However, this contradicts the assumption that g has infinite order. Thus, $H_{\langle g \rangle}$ has infinite order.

Now consider the case when g has finite order, say m. We claim that $H_{\langle g \rangle}$ has exactly m distinct elements, which are

$$H_{\langle g \rangle} = \{g^j \mid 0 \leq j < m\}.$$

First note that every element of $H_{\langle g \rangle}$ is of the above form. This is because given any integer n, we may divide it by m and write $n = km + j$ where $0 \leq j < m$. Then

$$g^n = g^{km+r} = (g^m)^k g^r = (e)^k g^r = g^r .$$

Next we claim that the elements g^j with $0 \leq j < m$ are all distinct. If not, suppose there are integers $0 \leq j_1 < j_2 < m$ such that $g^{j_1} = g^{j_2}$. As before we get that $g^{j_2 - j_1} = e$. □

2.2 Cyclic and Abelian groups

In some cases it may happen that $H_{\langle g \rangle} = G$ (see Example 2.1.10). For example, the group $(\mathbb{Z}, +, 0)$ is generated by 1. It is also generated by the element -1. We note this as a definition.

Definition 2.2.1. *Let G be a group. If there is an element $g \in G$ such that $H_{\langle g \rangle} = G$ then we say that G is cyclic and generated by g.*

Definition 2.2.2. *Let G be a group. If $ab = ba$ for all $a, b \in G$, then we say that G is abelian.*

Lemma 2.2.3. *The following assertions are obvious:*

(1) A cyclic group is abelian.

(2) Let G be an abelian group. Then for every subset S we have $C_G(S) = G$.

(3) G is abelian iff for every $x \in G$ we have $C_G(x) = G$.

(4) G is abelian iff for every $x \in G$ we have $N_G(x) = G$.

(5) For a group G and $g \in G$ the subgroup $H_{\langle g \rangle}$ is cyclic.

Proof. Obvious and left as an exercise to the reader. □

2.3 Equivalence relations and Cosets

Let $H \subset G$ be a subgroup. Let $a, b \in G$ be two elements. We say that $a \sim_H b$ (a is equivalent to b) if $ab^{-1} \in H$. Let us observe the following properties.

1. $a \sim_H a$ for all $a \in G$. This is clear since $e \in H$.
2. If $a \sim_H b$ then $b \sim_H a$. If $a \sim_H b$ then we have $ab^{-1} \in H$. Since H is a group, it follows that $(ab^{-1})^{-1} \in H$. But it is clear that $(ab^{-1})^{-1} = ba^{-1}$, this can be seen by just multiplying ab^{-1} with ba^{-1}. From this it follows that $b \sim_H a$.
3. If $a \sim_H b$ and $b \sim_H c$ for $a, b, c \in G$ then $a \sim_H c$. To see this note that ab^{-1} and bc^{-1} are in H. Since H is a subgroup it follows that their product, that is, $ac^{-1} \in H$. By definition this implies that $a \sim_H c$.

Using $\sim_H$ we can break the group G into a union of disjoint subsets. This is an instance of a very general construction which we now describe.

Let X be a non-empty set and suppose we are given a subset $R \subset X \times X$ such it has the following three properties.

1. $(x, x) \in R$ for all $x \in X$.
2. If $(x, x') \in R$ then $(x', x) \in R$.
3. If $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

The subset R is called an equivalence relation. Often it is denoted by a symbol $\sim$ and instead of writing $(x, y) \in R$ one writes $x \sim y$. Using R we may divide X into a disjoint union as follows. For any $x \in X$ define the equivalence class of x as follows

$$\mathrm{EC}(x) := \{y \in X \mid (x, y) \in R\}.$$

The main observation here is the following lemma.

Lemma 2.3.1. *For $x, x' \in X$, the sets $\mathrm{EC}(x)$ and $\mathrm{EC}(x')$ are either equal or they are disjoint.*

Proof. Suppose there is $y \in \mathrm{EC}(x) \cap \mathrm{EC}(x')$. Then this shows that $(x, y) \in R$ and $(x', y) \in R$. It follows that $(y, x') \in R$. Since $(x, y) \in R$ and $(y, x') \in R$ we get $(x, x') \in R$. If $y \in \mathrm{EC}(x')$ then $(x, x') \in R$ and $(x', y) \in R$ implies that $(x, y) \in R$, that is, $y \in \mathrm{EC}(x)$. Similarly we have $(x', x) \in R$ and so we get $y \in \mathrm{EC}(x)$ implies $y \in \mathrm{EC}(x')$. This proves that $\mathrm{EC}(x) = \mathrm{EC}(x')$. □

It is clear that every equivalence class $\mathrm{EC}(x)$ is non-empty since at least $x \in \mathrm{EC}(x)$. From each set of the type $\mathrm{EC}(x)$ choose one member, and call the collection of all these elements $\Lambda \subset X$. Then it is clear that

$$X = \bigsqcup_{x \in \Lambda} \mathrm{EC}(x)\,.$$

Now we return to the situation of a group G and a subgroup H. Define $R \subset G \times G$ to consist of elements of the type (g, hg) for all $g \in G$ and $h \in H$. Then it is obvious that $(x, y) \in R$ iff $xy^{-1} \in H$. Thus, we recover the equivalence relation $\sim_H$.

Lemma 2.3.2. *Let $H \subset G$ be groups and let $\sim_H$ be as above. For any $g \in G$, the equivalence class $\mathrm{EC}(g)$ is precisely the set $Hg := \{hg \mid h \in H\}$.*

Proof. By the definition of $\mathrm{EC}(g)$ we have $x \in \mathrm{EC}(g)$ iff $x \sim_H g$ iff $xg^{-1} \in H$. Thus, if $x \in \mathrm{EC}(g)$ then there is an $h \in H$ such that $xg^{-1} = h$ and so we get $x = hg$. This shows that $\mathrm{EC}(g) \subset Hg$. Conversely, it is clear that $hg \sim_H g$ since $hgg^{-1} = h \in H$. This shows that $Hg \subset \mathrm{EC}(g)$. Thus, $\mathrm{EC}(g) = Hg$. □

The equivalence classes above, of the form Hg, are called ***right cosets***.

Remark 2.3.3. Instead of defining the equivalence $x \sim_H y$ iff $xy^{-1} \in H$ we could have defined it as $x \sim_H y$ iff $x^{-1}y \in H$. The reader may check that this defines an equivalence relation and that the equivalence classes look like gH. These are called ***left cosets***.

Let us see some examples of coset decompositions. Notice that if we have two cosets Ha and Hb then to check that they are disjoint, it is enough to check that $ab^{-1} \notin H$.

Example 2.3.4. Let $G = S_3$ and let $H = \{e, (12)\}$ (the subgroup generated by (12)). Then we claim that H, $H(123)$ and $H(132)$ are disjoint cosets. This is clear since $(123) \notin H$ and $(132)(123)^{-1} = (123)$.

$$S_3 = H \sqcup H(123) \sqcup H(132) = \{e, (12)\}\,.$$

Since both sides have size 6, clearly the above is an equality.

Example 2.3.5. Let $G = S_3$ and let $H = \{e, (123), (132)\}$ (the subgroup generated by (123)). Then

$$S_3 = H \sqcup H(12)\,.$$

Since both sides have size 6, clearly the above is an equality.

Example 2.3.6. Let $G = \mathbb{Z}$ and let $H = n\mathbb{Z}$. Then

$$\mathbb{Z} = \bigsqcup_{i=0}^{n-1} n\mathbb{Z} + i\,.$$

This is the same as saying that for any integer k we can write it uniquely as $k = dn + i$ where $0 \leq i < n$. Unlike the above two examples, where we used a cardinality argument, here we have to show explicitly that every member of the LHS is contained in the RHS.

Consider the map $R_g : G \to G$ defined as $R_g(x) := xg$. This is "translation" on the right by g. Notice that this is a bijective map since it has an inverse $R_{g^{-1}}$. It is easily checked that $R_g \circ R_{g^{-1}} = R_{g^{-1}} \circ R_g = Id$. In particular, for any subset $S \subset G$ the image $R_g(S)$ has the same cardinality as S. We are now ready to prove Langrange's Theorem.

Theorem 2.3.7 (Lagrange)**.** *Let $H \subset G$ be finite groups. Then $\#H$ divides $\#G$. The number of cosets of H in G is precisely $\frac{\#G}{\#H}$.*

Proof. Using the equivalence relation $\sim_H$ we may decompose G into equivalence classes. From each equivalence class choose an element and form a subset $\Lambda \subset G$. Each equivalence class is of the form Hg. Thus,

$$G = \bigsqcup_{g \in \Lambda} Hg\,.$$

Since $Hg = R_g(H)$ it follows that all the equivalence classes have the same cardinality, which is the cardinality of H. Thus, $\#H$ divides $\#G$. The second assertion is clear from the disjoint union above. □

Corollary 2.3.8. *Let G be a finite group. Then the order of g divides $\#G$.*

Proof. Take $H = H_{\langle g \rangle}$. Now use Proposition 2.1.11 and the above Theorem. □

Corollary 2.3.9. *Let G be a group whose cardinality is a prime p. Then its only subgroups are $\{e\}$ and G. Thus, if $g \neq e$ is any element then $G = H_{\langle g \rangle}$.*

Proof. Let H be a subgroup of G. Since $\#H$ divides p, it follows that $\#H = 1$ or $\#H = p$. It follows that $H = \{e\}$ or $H = G$. The second assertion is now clear. □

Example 2.3.10. As a converse to the above we may ask the following. Suppose d divides $\#G$ then does there exist an element of order d. The answer to this is no. For example, let $G = \{\pm 1\} \times \{\pm 1\}$. Here the group multiplication is coordinate wise, that is, $(a, b) \cdot (a', b') := (aa', bb')$. Then 4 divides $\#G$, but G has no elements of order 4. If, however, d is prime, then it is a theorem of Cauchy that there exists an element of order d. We will see a proof of this result later. Another interesting result in this direction which we will see later is Sylow's Theorem. Let d be the highest power of a prime which divides $\#G$. Then G has a subgroup of order d. In the example we just saw, G was a group of order 4 and it had no element of order 4. However, it does have a subgroup of order 4, which is the whole group itself!

In fact, given any two groups G_1 and G_2 one easily checks that we can make $H := G_1 \times G_2$ into a group in this way. Moreover, $G_1 \times \{e\}$ and $\{e\} \times G_2$ are subgroups of H.

Example 2.3.11. We may use Lagrange's Theorem to easily list all subgroups of S_3. Since the size of S_3 is 6, every proper subgroup has size 1,2 or 3. If the size of the subgroup is 1, then clearly it is the trivial subgroup $\{e\}$. By Corollary 2.3.9 it follows that every non-trivial and proper subgroup is cyclic. Thus, every subgroup of S_3 is cyclic. These are

(1) {e, (12)}

(2) {e, (13)}

(3) {e, (23)}

(4) {e, (123), (132)}

2.4 Exercises

2.4.1. Show that every subgroup of $\mathbb{Z}$ is cyclic, that is, there is an element which generates it. (HINT: Choose the smallest positive element, if it exists.) How many generators can there be?

2.4.2. Let G be a group and let $a \in G$ be an element of order n. Let $n = \prod_{i=1}^{l} p_i^{r_i}$ be the prime factorization of n. Show that G contains an element of order $p_i^{r_i}$.

2.4.3. Let G be a group and let a and b be elements of order n and m. If $\gcd(n, m) = 1$ then show that $H_a \cap H_b = \{e\}$, where H_x denotes the cyclic subgroup generated by x. (HINT: Use Lagrange's theorem)

2.4.4. Let G be an abelian group and let a and b be elements of order n and m. If $\gcd(n, m) = 1$ then show that order of ab is mn.

2.4.5. Let G be an abelian group and let a and b be elements of order n and m. Combine the previous exercises to show that there is an element whose order is $\operatorname{lcm}(n, m)$.

2.4.6. Let $H \subset G$ be a subgroup and let $h \in H$, show that $hH = H = Hh$.

Chapter 3

Homomorphisms

3.1 Homomorphisms and Kernels

Definition 3.1.1. *Let G and H be groups. A homomorphism of groups $f : G \to H$ is a map of sets such that for all $a, b \in G$ we have $f(ab) = f(a)f(b)$.*

This definition means that the map f "respects" the group operation in the two groups. The product ab is the group multiplication in G, while the product $f(a)f(b)$ is the group multiplication in H.

Example 3.1.2. A simple example of a group homomorphism is the inclusion of a subgroup into a group. If $i : H \subset G$ is the inclusion of a subgroup, then obviously i is a group homomorphism by virtue of being a subgroup.

Example 3.1.3. Consider the group homomorphism $f : \mathbb{Z} \to S^1$ defined as $j \mapsto e^{2\pi ij/m}$. It is clear that $f(a + b) = f(a)f(b)$ and so this is a group homomorphism. Notice that the subgroup $m\mathbb{Z}$ is sent to 1, which is the identity element of S^1. The image of this group homomorphism is the group μ_m, see Example 2.1.8.

Definition 3.1.4 (Kernel)**.** *Let $f : G \to H$ be a group homomorphism. Then the set $f^{-1}(e) := \{g \in G \mid f(g) = e\}$ is called the kernel of f.*

Lemma 3.1.5. *Let $f : G \to H$ be a group homomorphism. Then*

(1) $f(e) = e$.

(2) The kernel is a subgroup of G, let us denote it by K.

(3) For each $g \in G$, there is an equality of cosets $gK = Kg$ (see Remark 2.3.3).

Proof. To prove (1) note that $f(ee) = f(e)$ since $ee = e$ in G. Since f is a group homomorphism we have $f(ee) = f(e)f(e)$. Thus, we get that $f(e) = f(e)f(e)$. Multiplying with $f(e)^{-1}$ on both sides we get that $f(e) = e$.

Let $a, b \in K$. Then $f(ab) = f(a)f(b) = e \cdot e = e$. Also $f(e) = f(a^{-1}a) = f(a^{-1})f(a)$. Since $f(e) = e$ and $f(a) = e$ since $a \in K$ we get $f(a^{-1}) = e$. This shows that $a^{-1} \in K$. Thus, K is closed under multiplication and taking inverse. This proves that K is a subgroup.

Let $k \in K$ and consider the element gkg^{-1}. We claim that this is in K. Applying f we get

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = e\,.$$

Thus, $gkg^{-1} = k_1$ for some $k_1 \in K$. This shows that $gk = k_1 g \in Kg$, that is, $gK \subset Kg$. Replacing g by g^{-1} we see that $g^{-1}K \subset Kg^{-1}$. Multiplying both sides with g on the right we see that $g^{-1}Kg \subset K$. Now multiplying both sides with g on the left we see that $Kg \subset gK$. This proves that $Kg = gK$. □

The above Lemma shows that subgroups which arise as kernels of group homomorphisms enjoy the special property that, for all $g \in G$, we have $gK = Kg$. This is clearly not the case in general. For example, let us take $G = S_3$, let $H = \{e, (12)\}$ and take $g = (123)$. Then

$$gH = \{(123), (13)\} \qquad\qquad Hg = \{(123), (23)\}\,.$$

We may ask if every subgroup H which has this special property, for all $g \in G$ there is an equality of cosets $gH = Hg$, arises as the kernel of a group homomorphism. We will prove this in two ways. First we give a direct proof, only to emphasize the ideas and definitions we have seen so far.

Let X be any set. Recall that the power set of X, denoted $\mathcal{P}(X)$, is the set whose elements correspond to subsets of X. Recall the map $L_x : G \to G$ which is left translation by x, given by $L_x(g) = xg$. It is bijective because it has an inverse $L_{x^{-1}}$. Obviously the map L_x gives rise to a map $\widetilde{L}_x : \mathcal{P}(G) \to \mathcal{P}(G)$ given as follows. For any subset $S \subset G$ define $\widetilde{L}_x(S) := L_x(S)$. For a subgroup H let $\mathcal{C}(H)$ denote the subset of $\mathcal{P}(G)$ containing all subsets of the type Hg.

In the group S_3 and taking the subgroup $H = \{e, (12)\}$ we have

$$(123)H(23) = \{(123), (13)\}(23) = \{(12), (132)\}\,.$$

Now assume $\{(12), (132)\}$ is a coset of H of the type Ha for some $a \in S_3$. For every element $g' \in Hg$ we have $Hg' = Hg$, since the cosets are either equal or disjoint. Thus, we get that $\{(12), (132)\} = H(12)$, but this is clearly not the case, as is easily checked by an explicit computation. This shows that in the group S_3 the map $\widetilde{L}_{(123)}$ does not map $\mathcal{C}(H)$ to itself. This happens because H does not satisfy the property that for all $x \in S_3$, $xH = Hx$.

Proposition 3.1.6. *Let $H \subset G$ be a subgroup such that for all $g \in G$ we have $gH = Hg$. Then there is a group homomorphism $f : G \to G'$ such that the kernel of f is precisely H.*

Proof. Let us check that $L_x(Hg) = xHg = Hxg$. Start with an element $xhg \in xHg$. since $xH = Hx$ we get that $xh = h_1 x$ for some $h_1 \in H$. This shows that $xhg = h_1 xg \in Hxg$. This proves that $xHg \subset Hxg$. Similarly, the other inclusion is easily proved and so we get $L_x(Hg) = Hxg$. Let $\mathcal{C} \subset \mathcal{P}(G)$ denote the collection of cosets Hg of G. In other words this means that the map $\widetilde{L}_x$ maps $\mathcal{C}$ to itself, since $\widetilde{L}_x(Hg) = L_x(Hg) = xHg = Hxg$. This is described well by saying that the following diagram commutes.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\widetilde{L}_x} & \mathcal{C} \\ \downarrow & & \downarrow \\ \mathcal{P}(G) & \xrightarrow{\widetilde{L}_x} & \mathcal{P}(G) \end{array}$$

This proves that we get a map of sets

$$\Phi : G \to \mathrm{Aut}(\mathcal{C})$$

defined as

$$x \mapsto \widetilde{L}_x$$

Let us check that Φ is a group homomorphism. We have $\Phi(xy) = \widetilde{L}_{xy}$. To show that $\widetilde{L}_{xy} = \widetilde{L}_x \circ \widetilde{L}_y$ it suffices to check this on elements of $\mathcal{C}$.

$$\begin{aligned} \widetilde{L}_{xy}(Hg) &= L_{xy}(Hg) \\ &= xyHg \\ &= xHyg \\ &= \widetilde{L}_x(Hyg) \\ &= \widetilde{L}_x(\widetilde{L}_y(Hg)) \end{aligned}$$

This proves that $\widetilde{L}_{xy} = \widetilde{L}_x \circ \widetilde{L}_y$, that is, $\Phi(xy) = \Phi(x) \circ \Phi(y)$. Thus, Φ is a group homomorphism.

Clearly, H is contained in the kernel of Φ since $\Phi(h) = \widetilde{L}_h$ and $\widetilde{L}_h(Hg) = hHg = Hg$ since $hH = H$. Conversely, suppose x is in the kernel of Φ then we get that $\widetilde{L}_x$ acts by the identity on each coset. Applying this on the coset H we see that $\widetilde{L}_x(H) = Hx = H$, that is, $x \in H$. □

3.2 Normal subgroups and Quotients

Definition 3.2.1. *Let G be a group and let K be a subgroup such that $gK = Kg$ for all $g \in G$. Then we say that K is a normal subgroup of G.*

We remark that the condition $gK = Kg$ is equivalent to the condition that $gKg^{-1} = K$ for all $g \in G$.

For a normal subgroup K we will define a multiplication map on the set of left cosets of K and check that this makes the set of left cosets into a group. Recall that left cosets of K are subsets of G of the form gK, and that G breaks up into a disjoint union of these cosets. Let $\mathcal{C}(K)$ denote the set of left cosets of K. Our aim is to define

$$m : \mathcal{C}(K) \times \mathcal{C}(K) \to \mathcal{C}(K)\,.$$

Let C_1 and C_2 be two left cosets. Choose $x_i \in C_i$ and define

$$m(C_1, C_2) = x_1 x_2 K\,.$$

We claim that this definition does not depend on the choice of the x_i. In other words, suppose $y_i \in C_i$, then $y_1 y_2 K = x_1 x_2 K$. Let us check this. Since $x_1 \in C_1$ it follows that $C_1 = x_1 K$. Since $y_1 \in C_1$ it follows that there is $k_1 \in K$ such that $y_1 = x_1 k_1$. Similarly, there is $k_2 \in K$ such that $y_2 = x_2 k_2$. Then

$$\begin{aligned} y_1 y_2 K &= x_1 k_1 x_2 k_2 K \\ &= x_1 k_1 x_2 K \\ &= x_1 x_2 (x_2^{-1} k_1 x_2) K \\ &= x_1 x_2 K \end{aligned}$$

In the 4th equality above we have used the fact that K being a normal subgroup $x_2^{-1} k_1 x_2 \in K$ and so $(x_2^{-1} k_1 x_2)K = K$. This proves the claim.

Let us check that this defines a group structure on $\mathcal{C}(K)$.

(1) To check associativity we need to show that for three cosets $C_1 = g_1K$, $C_2 = g_2K$, $C_3 = g_3K$ we have

$$m(C_1, m(C_2, C_3)) = m(m(C_1, C_2), C_3)\,.$$

Applying the definition of m, this is clear using the associativity property of the group.

(2) We claim that the coset K acts as the identity. We need to check that $m(gK, K) = gK$. since $g \in gK$ and $e \in K$, it follows that $m(gK, K) = gK$. Similarly, $m(K, gK) = gK$. Thus, K acts like the identity.

(3) We claim that given a coset gK, the inverse is the coset $g^{-1}K$. To see this we need to check that $m(gK, g^{-1}K) = K = m(g^{-1}K, gK)$. Again this is clear from the definition.

Thus, given a normal subgroup K, the above defines a group structure on the set $\mathcal{C}(K)$. This group is denoted as G/K. Similarly, we could have defined a group structure on the set of right cosets of a normal subgroup. For right cosets the resulting group is denoted as $K\backslash G$.

Theorem 3.2.2. *Let K be a normal subgroup of a group G. Then there is a group structure on the set of left cosets of K. The resulting group is denoted G/K. There is a natural group homomorphism $G \to G/K$ given by $g \mapsto gK$. The kernel of this group homomorphism is precisely K.*

Proof. It only remains to check that the map $G \to G/K$ given by $g \mapsto gK$ is a group homomorphism. Let us denote this map by Ψ. Then we need to check that

$$\Psi(gh) = \Psi(g)\Psi(h)\,.$$

The element $\Psi(gh)$ is the coset ghK. Now let us look at the RHS. The coset $\Psi(g)$ is gK and the coset $\Psi(h)$ is hK. We may choose the coset representatives $g \in gK$ and $h \in hK$ and then it is clear from the definition of multiplication in G/K that $(gK)(hK) = ghK$. Thus, the above equality holds.

The kernel of Ψ is precisely those $g \in G$ such that $\Psi(g)$ is the identity element of the group G/K. But we know that the identity element is the coset K. Thus, $\mathrm{Ker}(\Psi) = \{g \in G \,|gK = K\}$, that is, $\mathrm{Ker}(\Psi) = K$. □

Remark 3.2.3. Before we proceed we make the following important remark. The most important property of the above construction is that the "natural" map $G \to G/K$, given by $g \mapsto gK$ is a group homomorphism. If we only wanted to make G/K into a group, then we could have done something extremely stupid, as follows. Let S be any set and H be a group such that $\#S = \#H$. Choose a bijective map $\Phi : S \to H$ and transfer the group structure from H to S using Φ. By this we mean define $s_1 \cdot s_2 := \Phi^{-1}(\Phi(s_1) \cdot \Phi(s_2))$. Then this makes S into a group, because H is a group. In fact, S and H are the "same" groups. They are "isomorphic" in the following sense.

Definition 3.2.4. *Let $f : G \to H$ be a group homomorphism. We say that f is an isomorphism if it is bijective.*

We have the following obvious proposition.

Proposition 3.2.5. *Let $f : G \to H$ be a group homomorphism. Then $f(G)$ is a subgroup of H. If the kernel of f is $\{e\}$ then $f : G \to f(G)$ is an isomorphism. In this case, G is identified with the subgroup $f(G) \subset H$.*

Proof. Obvious and left as an exercise for the reader. □

3.3 Fermat's Little Theorem

If G is an abelian group, see section 2.2, then clearly every subgroup is normal and so for every subgroup K we have the group G/K. When we take $G = \mathbb{Z}$ and let $K = n\mathbb{Z}$ then we get the group $\mathbb{Z}/n\mathbb{Z}$. This is the group of "remainders" modulo n. This group is clearly cyclic since it is generated by 1. In fact, it is trivial to prove that if G is a cyclic group then every quotient of G is cyclic. We leave this as an exercise to the reader.

Using the "additive" group $\mathbb{Z}/n\mathbb{Z}$ we may construct another group which is "multiplicative". Consider the set

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{\bar{m} \mid \gcd(m, n) = 1\}.$$

The above notation needs some explanation. Since there is a surjection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\bar{m}$ we mean the image of m. Notice that $\bar{m}_1 = \bar{m}_2$ iff n divides $m_1 - m_2$, that is, iff $m_2 = m_1 + kn$. Thus, $\gcd(m_1, n) = 1$ iff $\gcd(m_2, n) = 1$.

Therefore, the definition of $(\mathbb{Z}/n\mathbb{Z})^\times$ makes sense. Given an element in $\mathbb{Z}/n\mathbb{Z}$ we may choose any lift in $\mathbb{Z}$ and check if the lift is coprime to n. It is clear that if m_1 and m_2 are coprime to n, then $m_1 m_2$ is also coprime to n. Thus, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ possesses a multiplication, which is simply given by

$$(\bar{m}_1, \bar{m}_2) \mapsto \overline{m_1 m_2}\,.$$

It is trivial to check that this is associative and that $\bar{1}$ is the identity element. The only non-trivial thing to check is that every element has an inverse. This is same as showing that given any $\bar{m}$ there is a $\bar{l}$ such that $\overline{ml} = \bar{1}$. This in turn is equivalent to saying that if m and n are coprime, then there is an integer l such that n divides $ml - 1$. This follows from the following well known proposition.

Proposition 3.3.1. *Let $a, b \in \mathbb{Z} \setminus 0$ and let $d := \gcd(a, b)$. Then there are integers k, l such that $ak + bl = d$.*

Proof. Let e be the smallest positive integer in the set

$$S := \{ak + bl \mid k, l \in \mathbb{Z}\}\,.$$

We claim that $e = d$. First note that d divides every element of the set S since d divides a and b. Thus, d divides e. Next we claim that e divides every element of the set S. Let $m \in S$ and assume that e does not divide m. Write

$$m = te + r \qquad t \in \mathbb{Z}\,,\ 0 < r < e\,.$$

Since $m, e \in S$ it follows that $m - te \in S$. This shows that $r \in S$, contradicting the minimality of e. This proves that e divides m. In particular, we may take $m = a, b$ which shows that e divides a and b. Since d is the gcd, it follows that e divides d. Thus, $e = d$. □

Now we return to our example. Let $a = n$ and $b = m$ and apply the above proposition. Then we get that there are integers k and l such that $nk + ml = 1$. This proves that $\overline{ml} = \bar{1}$. This proves that $(\mathbb{Z}/nZ)^\times$ is a group. The order of this group is often denoted by $\varphi(n)$ and known as the Euler totient function. Applying Lagrange's Theorem to this group we get

Proposition 3.3.2. *Let $n > 1$ be an integer. Then for every $a \in \mathbb{Z}$ which is coprime to n, we have that n divides $a^{\varphi(n)} - 1$.*

Proof. Consider the image $\bar{a}$ of a in $\mathbb{Z}/n\mathbb{Z}$. By Corollary 2.3.8, it follows that $\bar{a}^{\varphi(n)} = \bar{1}$. This is same as saying that n divides $a^{\varphi(n)} - 1$. □

Corollary 3.3.3 (Fermat's Little Theorem)**.** *Let p be a prime and suppose p does not divide a. Then p divides $a^{p-1} - 1$.*

Proof. We only need to show that $(\mathbb{Z}/p\mathbb{Z})^\times$ has cardinality $p-1$. But this is clear since $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ and all classes except 0 are coprime to p. □

3.4 Universal property of quotients

Let G be a group and let K be a normal subgroup. Let $\pi : G \to G/K$ denote the natural map. Consider the following two sets.

$$S_1 := \{\text{Homomorphisms } \bar{\phi} : G/K \to H\},$$

$$S_2 := \{\text{Homomorphisms } \phi : G \to H \text{ such that } K \subset \text{Ker}(\phi)\}.$$

There is an obvious map from $\Phi : S_1 \to S_2$, namely,

$$\Phi(\bar{\phi}) := \bar{\phi} \circ \pi\,. \tag{3.4.1}$$

Theorem 3.4.2. *Let G and H be groups. Then the map Φ is a bijection.*

Proof. Let us first check that Φ is injective. This is clear using the following general fact about maps of sets. Suppose $f, g : Y \to Z$ are two maps. Let $h : X \to Y$ be a surjective map. If $f \circ h = g \circ h$ then $f = g$. We leave the proof of this simple fact to the reader. From this simple fact the injectivity of Φ follows immediately since π is clearly a surjection.

Now let us prove that Φ is a surjection. Let $\phi : G \to H$ be a group homomorphism such that $K \subset \text{Ker}(\phi)$. We need to show that there is a group homomorphism $\bar{\phi} : G/K \to H$ such that $\phi = \bar{\phi} \circ \pi$. The definition of $\bar{\phi}$ is forced onto us. Suppose a $\bar{\phi}$ existed, then applying $\phi = \bar{\phi} \circ \pi$ to $g \in G$ we get $\phi(g) = \bar{\phi}(gK)$. This shows that for a coset C, we may define $\bar{\phi}(C) := \phi(g)$, for some element $g \in C$. Let us check that this is independent of the choice of coset representative. Suppose $g' \in C$ is another element, then $g' = gk$ for some $k \in K$. Then

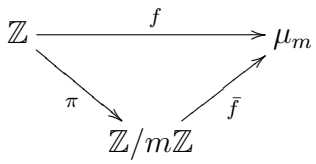
$$\phi(g') = \phi(gk) = \phi(g)\phi(k) = \phi(g)\,.$$

This defines a map $\bar{\phi} : G/K \to H$. It remains to check that $\bar{\phi}$ is a group homomorphism and that $\phi = \bar{\phi} \circ \pi$. The second is obvious. For the first, let g_1K and g_2K be two cosets. Then their product in G/K is the coset g_1g_2K. By definition we have

$$\bar{\phi}(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \bar{\phi}(g_1K)\bar{\phi}(g_2K)\,.$$

This shows that $\bar{\phi}$ is a group homomorphism. The proof of the Theorem is now complete. □

Example 3.4.3. Let us revisit example 3.1.3. There we considered the group homomorphism $f : \mathbb{Z} \to \mu_m$ (see example 2.1.8) given by $f(n) = e^{2\pi in/m}$. The kernel of this group homomorphism is precisely $m\mathbb{Z}$. Thus, using the above theorem we get that this factors as



Notice that the kernel of $\bar{f}$ is the trivial group. This is because if $\bar{f}(\bar{n}) = 1$ then $e^{2\pi in/m} = 1$ and so n is a multiple of m. Thus, $n \in m\mathbb{Z}$ and so $\bar{n}$ is the trivial element. Applying Proposition 3.2.5 we see that $\bar{f}$ is an isomorphism onto its image. However, since the map $\bar{f}$ is an inclusion, and both $\mathbb{Z}/m\mathbb{Z}$ and μ_m have the same cardinality, it follows that this map is a surjection. Thus, we get that $\bar{f}$ is actually an isomorphism of groups.

3.5 Exercises

3.5.1. Let G be a group and suppose there are two group homomorphisms $\Phi_i : \mathbb{Z} \to G$ for $i = 1, 2$. If $\Phi_1(1) = \Phi_2(1)$, show that these two are equal. In other words, a group homomorphism from $\mathbb{Z}$ to a group is completely determined by the image of 1.

3.5.2. Given an element $a \in G$ show that there is a **unique** group homomorphism $\Phi : \mathbb{Z} \to G$ such that $\Phi(1) = a$.

3.5.3. Let $a \in G$ be an element of order n. Show that the (cyclic) subgroup generated by a is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

3.5.4. Use the previous exercise to show that the order of a^i is $\frac{n}{gcd(n,i)}$. Note that this is the same as computing the order of i in $\mathbb{Z}/n\mathbb{Z}$.

3.5.5. Suppose H is a cyclic group and $f : H \to G$ is a surjective group homomorphism. Show that G is a cyclic group.

3.5.6. Let G be a cyclic group, show that there is a surjective group homomorphism $\Phi : \mathbb{Z} \to G$.

3.5.7. Let G and H be arbitrary groups and let $f : G \to H$ be a group homomorphism. Let $H_1 \subset H$ be a subgroup. Show that $f^{-1}(H_1) := \{g \in G \mid f(g) \in H_1\}$ is a subgroup of G.

3.5.8. Combine the previous exercises to show that every subgroup of a cyclic group is cyclic.

3.5.9. Show that for every $d|n$, there is a unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. In view of the isomorphism between $\mathbb{Z}/n\mathbb{Z}$ and any cyclic group of order n, this shows that given any cyclic group of order n and $d|n$, there is a unique subgroup of order n.

3.5.10. Show that a subgroup $N \subset G$ is normal if and only if $NgNh = Ngh$ for all $g, h \in G$.

3.5.11. Show that there is a bijection of sets

$$\{\text{Group homomorphisms } \phi : \mathbb{Z}/n\mathbb{Z} \to G\} \leftrightarrow \{\text{elements } a \in G \text{ such that } a^n = e\}$$

3.5.12. Let $N \subset G$ be a normal subgroup. Suppose H is a subgroup such that $N \subset H$, then show that N is normal in H, and so there is a group H/N. Show that there is a "natural" group homomorphism $H/N \to G/N$ which is an inclusion. Thus, H/N is a subgroup of G/N in a natural way.

3.5.13. In view of the previous exercise, show that there is a bijection of sets

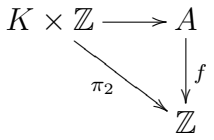
$$\{\text{Subgroups } H \text{ such that } N \subset H \subset G\} \leftrightarrow \{\text{Subgroups of } G/N\}$$

Now suppose that H is also normal in G, then show that H/N is normal in G/N and there is a natural isomorphism $G/H \cong (G/N)/(H/N)$.

3.5.14. From among the finite groups we have seen so far, give an example of a group G, a subgroup H and elements $x, y \in G$ for which $\#(HxHy) > \#H$.

3.5.15. Let H be a subgroup of G. Define the normalizer of H to be $N(H) := \{g \in G \mid gHg^{-1} = H\}$. Show that $N(H)$ is a subgroup which contains H. Show that $N(H)$ is the largest subgroup of G containing H in which H is normal, that is, if K is any subgroup of G containing H and if H is normal in K, then $K \subset N(H)$.

3.5.16. Suppose A is an abelian group and there is a surjective homomorphism $f : A \to \mathbb{Z}$. Let K denote the kernel of f. Show that there is a map $K \times \mathbb{Z} \to A$ which is an isomorphism of groups and such that the diagram



Here π_2 is the projection onto the second coordinate.

Chapter 4

Group actions

4.1 Action of $\mathrm{Aut}(X)$ on X

Let X be a non-empty set. The first example of a group that we saw was $\mathrm{Aut}(X)$. This group comes with the following obvious map

$$\Theta : \mathrm{Aut}(X) \times X \to X \qquad \Theta(\phi, x) := \phi(x)\,.$$

This map has the following properties, which are easily checked

(1) $\Theta(Id, x) = x$ for all $x \in X$

(2) $\Theta(\phi, \Theta(\psi, x)) = \Theta(\phi \circ \psi, x)$

A group action on a set X is an abstraction of the above properties. Often one deduces several results about the structure of a group by making a group act on some set, as we shall see in this chapter. But first let us see the definition of a group action.

Definition 4.1.1. *Let G be a group and let X be a set. We say that G acts on X if there is a map $\Phi : G \times X \to X$ satisfying the following two properties*

(1) $\Phi(Id, x) = x$ for all $x \in X$

(2) $\Phi(\phi, \Phi(\psi, x)) = \Phi(\phi \circ \psi, x)$

Let us see a few easy examples of group actions. Take $X = G$ and define $\Phi : G \times X \to X$ by

(a) $\Phi(g,x) = gx$

(b) $\Phi(g,x) = xg^{-1}$

(c) $\Phi(g,x) = gxg^{-1}$

One easily checks that these satisfy the assumptions of a group action. Often instead of writing $\Phi(g,x)$ we will simple write $g \cdot x$ or gx. Then the defining conditions of a group action may be written as $ex = x$ and $g(hx) = (gh)x$.

4.2 Orbits

Let G act on a set X. Then we can put an equivalence relation (see section 2.3) on the set X. Define $x_1 \sim x_2$ if there is a $g \in G$ such that $gx_1 = x_2$. Let us check that this satisfies the hypothesis of a group action. Clearly, since $ex = x$, it follows that $x \sim x$. Secondly, if $x \sim y$ then there is $g \in G$ such that $gx = y$. Applying g^{-1} to both sides we get $x = g^{-1}y$ which shows that $y \sim x$. Finally, if $x \sim y$ and $y \sim z$ then there exist $g, h \in G$ such that $gx = y$ and $hy = z$. Applying h on $gx = y$ we get $h(gx) = (hg)x = hy = z$. This proves that $x \sim z$.

The orbit of an element $x \in X$, under this action of G, is the equivalence class of x under the above equivalence relation. We will denote it by $\mathrm{Orb}_G(x)$ or simply $\mathrm{Orb}(x)$.

In view of Lemma 2.3.1 and the discussion following this lemma, it follows that X breaks into a disjoint union of orbits. Thus, there is $\Lambda \subset X$ such that

$$X = \bigsqcup_{x \in \Lambda} \mathrm{Orb}(x_i)\,.$$

Let us see some examples.

Example 4.2.1. Let $X = \{1, 2, \ldots, n\}$ and let $S_n = \mathrm{Aut}(X)$ act on X as we saw above. Then there is only one orbit. For example, if we apply $(1, j)$ on 1, then we get j. This proves that every $j \in X$ is in the orbit of 1.

Consider the cyclic subgroup generated by (123). That is, let $H = \{e, (123), (132)\}$. Then we may restrict the action of S_n on X to H. By this we simply mean that the map $\Phi : S_n \times X \to X$ can be restricted to $H \times X \subset S_n \times X \xrightarrow{\Phi} X$, and the restricted map continues to satisfy the defining conditions of a group action. This is obvious. Let us compute the

orbits in X under the action of H. By applying the powers of (123) on 1 we easily see that the orbit of 1 is $\{1,2,3\}$. If $j \notin \{1,2,3\}$ then it is clear that every element of H fixes j. Thus, the orbit of $j \notin \{1,2,3\}$ is $\{j\}$. Thus, the orbit decomposition of X under the action of H is

$$X = \{1,2,3\} \sqcup \bigsqcup_{j=4}^{n} \{j\}$$

Example 4.2.2. Let G be a group and let H be a subgroup. Consider the ***set*** of cosets G/H. Then G acts on G/H as follows. Define $\Phi(g, xH) = gxH$. It is easily checked that this defines a group action. It is clear in this case as well that there is only one orbit. For example, we can take the coset H, and every other coset gH is given by $\Phi(g, H)$.

Definition 4.2.3. *Let G act on a set X. We say the action is transitive if there is only one orbit.*

Example 4.2.4. Let G act on a set X and let $\mathrm{Orb}(x)$ be the orbit of an element $x \in X$. Notice that under the map $\Phi : G \times X \to X$, the set $G \times \mathrm{Orb}(x)$ gets mapped to $\mathrm{Orb}(x)$. This shows that G acts on $\mathrm{Orb}(x)$ and this action has only one orbit. Thus, the action of G on $\mathrm{Orb}(x)$ is transitive. Similarly, some of the earlier examples of actions were also transitive.

Example 4.2.5. Let G act on itself by conjugation. That is, take $X = G$ and define $\Phi(g, x) = gxg^{-1}$. If G is an abelian group then every orbit contains only one element, that is, $\mathrm{Orb}(x) = \{x\}$. In fact, it is clear that G is abelian iff for this action each orbit contains only one element.

For an arbitrary group G, not necessarily abelian, the orbit of the identity $\mathrm{Orb}(e) = \{e\}$.

Example 4.2.6. Let $Y := \{X \subset G \mid \#X = p^l\}$. For $X \in Y$ define $g \cdot X := \{gx \mid x \in X\}$. One checks easily that this defines an action on Y.

4.3 Stabilizers

Definition 4.3.1. *Let G act on a set X. The stabilizer of an element $x \in X$ is the set* $\mathrm{Stab}(x) := \{g \in G \mid gx = x\}$

It is trivial to check that the stabilizer is a subgroup of G. In fact, as we will see in the proof of the next result, the orbit of x is identified with the set $G/\mathrm{Stab}(x)$ in a natural way.

Proposition 4.3.2. *Let G be a finite group acting on X. For every $x \in X$ we have $\#\mathrm{Orb}(x) \cdot \#\mathrm{Stab}(x) = \#G$.*

Proof. Define a map $f : G \to \mathrm{Orb}(x)$ by $g \mapsto gx$. By the definition of orbit, this map is surjective. We claim the coset $g\mathrm{Stab}(x)$ maps to gx. This is clear since if $h \in \mathrm{Stab}(x)$ then $ghx = gx$. Conversely, if $gx = tx$ then we get that $g^{-1}tx = x$, that is, $g^{-1}t \in \mathrm{Stab}(x)$. This shows that $gx = tx$ iff $t \in g\mathrm{Stab}(x)$. This proves that $f^{-1}(gx) = g\mathrm{Stab}(x)$ for all $g \in G$. For any map of finite sets $f : X \to Y$ we have $\#X = \sum_{y \in Y} \#f^{-1}(y)$. Applying this to f, taking $X = G$ and $Y = \mathrm{Orb}(x)$ we get that

$$\#G = \sum_{y \in \mathrm{Orb}(x)} \#f^{-1}(y)\,.$$

Since the $\#f^{-1}(y) = \#\mathrm{Stab}(x)$ for every y we get that

$$\#G = \#\mathrm{Orb}(x) \cdot \#\mathrm{Stab}(x)\,.$$

This completes the proof of the proposition. □

Let us see an application of Proposition 4.3.2.

Definition 4.3.3. *Let G be a group. The center of G is the set of elements which commute with every other element, that is, $Z(G) := \{x \in G \mid gx = xg \ \ \forall g \in G\}$.*

It is clear that $Z(G)$ is a subgroup of G.

Theorem 4.3.4. *Let G be a p-group, that is, $\#G$ is a power of p, say p^l. Then $Z(G)$ is a non-trivial subgroup.*

Proof. To see this we make G act on itself by conjugation and analyse the orbits. Recall that the conjugation action is defined as follows. For $g, x \in G$ define $g \cdot x := gxg^{-1}$. Clearly, for every $x \in G$, the orbit of x contains x. It is clear that $\mathrm{Orb}(x) = \{x\}$ iff $gxg^{-1} = x$ for all $g \in G$, that is, iff $gx = xg$

for all $g \in G$, that is, iff $x \in Z(G)$. Thus, decomposing the set $X = G$ into disjoint orbits, we get

$$G = \bigsqcup_{x \in Z(G)} \mathrm{Orb}(x) \sqcup \bigsqcup_{x \notin Z(G)} \mathrm{Orb}(x)\,.$$

Suppose $x \notin Z(G)$. Then since $1 < \#\mathrm{Orb}(x) = \dfrac{\#G}{\#\mathrm{Stab}(x)}$ and $\#G = p^l$, we see that $\#\mathrm{Orb}(x)$ is a power of p and in particular is a multiple of p. Thus, computing cardinality we get that

$$p^l = \#G = \#Z(G) + p(*)\,.$$

If $Z(G) = \{e\}$ then we get a contradiction since p does not divide the RHS. This proves that $Z(G)$ is non-trivial. □

As an application of the above result let us show that every group of order p^2 is abelian. A group of order p is necessarily cyclic. In fact, any element $x \neq e$ will generate the group by Lagrange's Theorem 2.3.7.

Theorem 4.3.5. *Let G be a group or order p^2. Then G is abelian.*

Proof. The preceding theorem shows that $Z(G)$ is non-trivial. If $Z(G) = G$ then there is nothing to prove. Let us assume that $Z(G) \subsetneqq G$. Then it is forced to be a group of cardinality p. Clearly, $Z(G)$ is a normal subgroup. Let H be the group $G/Z(G)$. Then H is a group of order p and so is cyclic. Let $g_0 \in G \setminus Z(G)$ be any element. We claim that every element of G can be written as $g_0^i h$ for some $h \in Z(G)$. Consider the group homomorphism $G \to H$. The image of g_0 is non-trivial and so it generates the whole group H. Thus, if $g \in G$ is an element, then there is an i such that $gZ(G) = g_0^i Z(G)$. This proves that $g = g_0^i h$ for some $h \in Z(G)$. But by writing any two elements of G in this form it is clear that all elements of G commute with each other, proving that $Z(G) = G$. This is a contradiction. Thus, $Z(G) = G$ and so G is abelian. □

4.4 Sylow's Theorem

Recall the definition of the normalizer of a subset from Example 2.1.6. Note that if H is a subgroup of G and $N(H)$ is the normalizer of H, then H is

a normal subgroup of $N(H)$. This follows trivially from the definition of $N(H)$. We will use this observation in the following Lemma.

Let G be a group of order $p^l m$ with $\gcd(m, p) = 1$. A subgroup of G of order p^l will be called a p-Sylow subgroup.

Lemma 4.4.1. *Let $Q_1 \subset G$ be a p-Sylow subgroup. Let $Q_2 \subset G$ be a p-group. If $Q_2 \subset N(Q_1)$ then $Q_2 \subset Q_1$. Moreover, if Q_2 is also a p-Sylow subgroup then $Q_2 = Q_1$.*

Proof. Since $Q_1 \subset N(Q_1)$ is a normal subgroup, it follows that $N(Q_1)/Q_1$ is a group and the natural map $N(Q_1) \to N(Q_1)/Q_1$ is a group homomorphism. Let us consider the composite map

$$Q_2 \subset N(Q_1) \to N(Q_1)/Q_1 \,.$$

Since

$$\#(N(Q_1)/Q_1) = \frac{\#N(Q_1)}{\#Q_1} \,,$$

and the RHS divides $\#G/\#Q_1 = m$, it follows that $\#(N(Q_1)/Q_1)$ is not a multiple of p. If $f : A \to B$ is a group homomorphism between finite groups of coprime cardinality, then $f(A) = e$. This is an easy exercise which is left to the reader. But applying this to our specific situation we see that the image of Q_2 is trivial, or equivalently, Q_2 is contained in the kernel of the map $N(Q_1) \to N(Q_1)/Q_1$. But the kernel is precisely Q_1. This proves that $Q_2 \subset Q_1$. If Q_2 is a p-Sylow subgroup then both Q_1 and Q_2 have the same cardinality, it follows that $Q_1 = Q_2$. □

Theorem 4.4.2 (Sylow's Theorem)**.** *Let G be a group of order $p^l m$ with* $\gcd(m, p) = 1$. *Then*

(a) G contains a subgroup of order p^l.

(b) The number of p-Sylow subgroups is congruent to 1 mod p.

(c) All the p-Sylow subgroups are conjugates of each other.

(d) The number of p-Sylow subgroups divides m.

Proof. Let Y be the set consisting of all subsets of G of order p^l. Then

$$\begin{aligned}\#Y &= \binom{p^l m}{p^l} \\ &= \prod_{i=1}^{p^l-1} \frac{p^l m - p^l - i}{p^l - i}\,.\end{aligned}$$

It is clear that the highest power of p which divides $p^l m - p^l - i$ is exactly the highest power of p which divides $p^l - i$. From this it follows that $\#Y$ is not a multiple of p.

As we saw before, G acts on Y by left translation. More precisely, this is given as follows. Let $T \in Y$. Then T is a subset of G of order p^l.

$$g \cdot T := \{gt \mid t \in T\}\,.$$

There is at least one orbit $\mathrm{Orb}(T)$ such that $\#\mathrm{Orb}(T)$ is not divisible by p. On the contrary, suppose p divides each $\#\mathrm{Orb}(T)$, then since Y is a union of these orbits, p will divide $\#Y$, which is a contradiction. Let us fix T_0 such that p does not divide $\#\mathrm{Orb}(T_0)$.

We will prove (a) by induction on m. If $m = 1$ then there is nothing to prove. Let us assume that $m > 1$ and that (a) is true for all groups of size $p^l r$ where $1 \leq r < m$. Notice that G does not fix any $T \in Y$. In fact, choose a $t_0 \in T$ and an element $t_1 \notin T$. Then the set $t_1 t_0^{-1} \cdot T$ contains t_1 and so it is not equal to T. Thus, $\mathrm{Stab}(T)$ is a proper subgroup of G. By Theorem 4.3.2 we have that $\#\mathrm{Orb}(T_0) \cdot \#\mathrm{Stab}(T_0) = \#G$. Since p does not divide $\#\mathrm{Orb}(T_0)$ it follows that $\#\mathrm{Stab}(T_0) = p^l r$ for some $r < m$. By induction hypothesis the subgroup $\mathrm{Stab}(T_0)$ contains a subgroup of order p^l. Thus, G contains a subgroup of order p^l. This proves (a).

To prove (b), let S denote the set of all p-Sylow subgroups of G. Let $Q_0 \in S$. We make Q_0 act on S by conjugation, that is, for $x \in Q_0$ and $Q \in S$ define $x \cdot Q := xQx^{-1}$. Clearly, if $x \in Q_0$ then $xQ_0x^{-1} = Q_0$, and so $\mathrm{Orb}_{Q_0}(Q_0) = \{Q_0\}$. Here we have emphasized in the notation that we are looking at the orbit under the Q_0 action and not under the G action. Suppose $Q_1 \in S$ and $Q_1 \neq Q_0$. We claim that it is not possible that $\#\mathrm{Orb}_{Q_0}(Q_1) = 1$. If this happens, then we get that $xQ_1x^{-1} = Q_1$ for all $x \in Q_0$, that is, $Q_0 \subset N_G(Q_1)$. By Lemma 4.4.1 it follows that $Q_0 = Q_1$, which is a contradiction. Thus, if $Q_1 \neq Q_0$ then $\#\mathrm{Orb}_{Q_0}(Q_1) > 1$. By Theorem 4.3.2 it follows that $\#\mathrm{Orb}_{Q_0}(Q_1) \cdot \#\mathrm{Stab}_{Q_0}(Q_1) = \#Q_0 = p^l$. Thus, if $Q_1 \neq Q_0$ it follows that

$\#\mathrm{Orb}_{Q_0}(Q_1)$ is a multiple of p. Thus, S breaks into disjoint orbits under the action of Q_0, exactly one of these orbits has cardinality 1 while the others have cardinality multiples of p, that is,

$$\#S = 1 + p(*)\,.$$

This proves (b).

Now let us show that there is only one orbit in S. Let $S' \subset S$ denote the orbit of Q_0 under the G action by conjugation, that is, $S' = \mathrm{Orb}_G(Q_0)$. We need to show that $S' = S$. If possible let $Q_1 \in S \setminus S'$. We will consider the action of Q_1 on S' by conjugation. If $Q' \in S'$ then we claim that $\#\mathrm{Orb}_{Q_1}(Q') > 1$. If not, then $\#\mathrm{Orb}_{Q_1}(Q') = 1$, which means that $Q_1 \subset N_G(Q')$. By Lemma 4.4.1 we will get that $Q_1 = Q'$, which is a contradiction since $Q' \in S'$ and $Q_1 \notin S'$. By Theorem 4.3.2 we get that

$$\#\mathrm{Orb}_{Q_1}(Q') \cdot \#\mathrm{Stab}_{Q_1}(Q') = \#Q_1 = p^l$$

and this shows that $\#\mathrm{Orb}_{Q_1}(Q')$ is a multiple of p. Since this happens for all $Q' \in S'$, it follows that the cardinality of S' is a multiple of p, since S' is a disjoint union of its orbits.

Now let us consider the action of Q' on S' by conjugation. Clearly, if $x \in Q'$ then $xQ'x^{-1} = Q'$, and so $\mathrm{Orb}_{Q'}(Q') = \{Q'\}$. Suppose $H \in S'$ and $H \neq Q'$. We claim that it is not possible that $\#\mathrm{Orb}_{Q'}(H) = 1$. If this happens, then we get that $xHx^{-1} = H$ for all $x \in Q'$, that is, $Q' \subset N_G(H)$. By Lemma 4.4.1 it follows that $Q' = H$, which is a contradiction. Thus, if $H \neq Q'$ then $\#\mathrm{Orb}_{Q'}(H) > 1$. As we saw above, it follows that $\#\mathrm{Orb}_{Q'}(H)$ is a multiple of p. Thus, S' breaks into disjoint orbits under the action of Q', exactly one of these orbits has cardinality 1 while the others have cardinality multiples of p, that is,

$$\#S' = 1 + p(*)\,.$$

But this is a contradiction since we saw earlier that $\#S'$ is a multiple of p. This proves that $S' = S$, which proves (c).

To prove (d), fix a p-Sylow subgroup $Q \in S$. Since there is only one G-orbit, we have $S = \mathrm{Orb}_G(Q)$. By Theorem 4.3.2 we see that $\#S \cdot \#\mathrm{Stab}(Q) = \#G$. It is clear that $\mathrm{Stab}_G(Q) = N(Q) \supset Q$ and so it has cardinality $p^l r$. It follows that $\#S$ divides m.

This completes the proof of the Theorem. □

Corollary 4.4.3. *Let G be a group such that p divides $\#G$. Then G contains an element of order p.*

Proof. Let $\#G = p^l m$, where $\gcd(m, p) = 1$. Then G contains a subgroup Q of order p^l. Any element in Q will have order a power of p. From this one easily shows that there is an element of order p, and that is left to the reader as an exercise. □

Proposition 4.4.4. *Let $H \subset G$ be a p-group. Then H is contained in a p-Sylow subgroup.*

Proof. Let S denote the set of all p-Sylow subgroups of G. Let H act on S be conjugation. As we saw before, if $Q \in S$ and $\#\mathrm{Orb}_H(Q) > 1$, then by Theorem 4.3.2 we easily get the p divides $\#\mathrm{Orb}_H(Q)$. If this happens for all $Q \in S$ then we would get that p divides $\#S$, which we know is not true from the preceding theorem. Thus, there is a $Q \in S$ such that $\#\mathrm{Orb}_H(Q) = 1$, which is same as saying that $H \subset N(Q)$. Lemma 4.4.1 shows that $H \subset Q$, which proves the Proposition. □

4.5 Symmetric groups

In this section we will prove Theorem 1.4.7.

Theorem 4.5.1. *We have in the group S_n*

(1) If $\alpha = (a_1, a_2, \ldots, a_r)$ and $\beta = (b_1, b_2, \ldots, b_s)$ are two disjoint cycles then $\alpha\beta = \beta\alpha$.

(2) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then

$$(a_1, a_2, \ldots, a_r) = (a_1, a_2)(a_2, a_3)(a_3, a_4)\ldots(a_{r-1}, a_r)\,.$$

(3) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then its inverse is $(a_r, a_{r-1}, \ldots, a_3, a_2, a_1)$.

(4) If $\alpha = (a_1, a_2, \ldots, a_r)$ is a cycle then it has order r.

(5) Every element of S_n can be written as a product of disjoint cycles.

(6) If an element is written as a product of disjoint cycles $c_1 c_2 \ldots c_l$ and $c'_1 c'_2 \ldots c'_s$ in two ways, then $l = s$ and the cycles c_i are equal to the cycles c'_j up to permutation. In other words, every element is written as a product of disjoint cycles in a "unique" way.

Proof. The first four assertions are easy and are left to the reader. We will prove the last two assertions.

Let X denote the set $\{1, 2, \ldots, n\}$. Let $\gamma \in S_n$ be an element. Let $H_{\langle\gamma\rangle}$ denote the cyclic subgroup generated by γ in S_n. Let $a \in X$. By the *orbit of a under γ* we shall mean the subset

$$O(\gamma, a) := \{\gamma^i(a) \mid i \in \mathbb{Z}\} \subset X\,.$$

This is simply the orbit of a under the action of the cyclic subgroup $H_{\langle\gamma\rangle}$ generated by γ in S_n. Clearly, $a \in O(\gamma, a)$. There are distinct elements $a_1, a_2, \ldots, a_r$ such that

$$X = \bigsqcup_{i=1}^{r} O(\gamma, a_i)\,. \tag{4.5.2}$$

We have simply decomposed X into disjoint orbits for the action of the subgroup $H_{\langle\gamma\rangle}$.

Fix $a \in X$. Let $i > 0$ be the smallest positive integer such that $\gamma^i(a) = a$. Then we claim that

$$O(\gamma, a) := \{a, \gamma(a), \gamma^2(a), \ldots, \gamma^{i-1}(a)\}\,.$$

Moreover, all the above elements are distinct. If the elements are not distinct, then that will contradict the minimality of i. Given any integer l we can divide it by i and write $l = si + j$ where $0 \leq j < i$. Then it follows that

$$\gamma^l(a) = \gamma^j((\gamma^i)^s(a))\,.$$

But the map γ^i fixes a. Thus, all its powers also fix a. Then the above becomes $\gamma^l(a) = \gamma^j(a)$, which proves the claim.

In particular, the above shows that

$$(a, \gamma(a), \gamma^2(a), \ldots, \gamma^{i-1}(a))$$

defines a cycle in S_n. We apply this discussion to the elements $a_1, a_2, \ldots, a_r$ in equation (4.5.2). Then we get product of disjoint cycles

$$\gamma' := (a_1, \gamma(a_1), \ldots, \gamma^{i_1-1}(a_1))(a_2, \gamma(a_2), \ldots, \gamma^{i_2-1}(a_2)) \ldots (a_r, \gamma(a_r), \ldots, \gamma^{i_r-1}(a_r))$$

We claim that the above element in S_n represents the map γ. It suffices to show that for any $a \in X$, we have $\gamma'(a) = \gamma(a)$. From equation (4.5.2) there

is a unique a_l and unique j such that $0 \leq j < i_l$ and such that $a = \gamma^j(a_l)$. Then

$$\begin{aligned}\gamma(a) &= \gamma(\gamma^j(a_l)) \\ &= \gamma'(a)\end{aligned}$$

Recall that if $j = i_l - 1$ then by the definition of i_l we have $\gamma^{i_l}(a_l) = a_l$. This shows that $\gamma = \gamma'$. Thus, we have proved (5) which says that every element of S_n can be written as a product of disjoint cycles.

To prove that the above expression is unique, let us assume that

$$\gamma = c'_1 c'_2 \dots c'_s = c_1 c_2 \dots c_l$$

are two expressions for γ as product of disjoint cycles. Let $H_{\langle\gamma\rangle}$ denote the cyclic subgroup generated by γ. Consider the action of $H_{\langle\gamma\rangle}$ on X. Let us write $c'_1 = (b_1, b_2, \dots, b_t)$. Since applying γ is the same as applying $c'_1 c'_2, \dots c'_s$, and b_i occur only in c'_1, this shows that

$$O(\gamma, b_1) = \{b_1, b_2, \dots, b_t\} = \{b_1, \gamma(b_1), \gamma^2(b_1), \dots, \gamma^{t-1}(b_1)\}\,.$$

We easily conclude that there are exactly s orbits for the action of $H_{\langle\gamma\rangle}$ on X. In the same way, using the other expression for γ as product of disjoint cycles, we see that the number of orbits is l. This proves that $s = l$. Thus, we may write

$$\gamma = c'_1 c'_2 \dots c'_l = c_1 c_2 \dots c_l\,.$$

Next let us show that, after rearranging the indices if necessary, $c'_i = c_i$. Choose an $a \in X$. Then there are unique i and j such that a appears in the cycles c'_i and c_j. After renumbering the indices we may assume that a appears in the cycles c'_1 and c_1. Applying γ as above we see that c'_1 and c_1 are forced to be the cycle

$$(a, \gamma(a), \gamma^2(a), \dots, \gamma^{t-1}(a))\,,$$

where t is the smallest positive integer such that $\gamma^t(a) = a$. This completes the proof of the Theorem. □

4.6 Exercises

4.6.1. Let G be a finite group. G acts on itself by conjugation. If there are exactly two distinct orbits then prove that G has order 2.

4.6.2. Let $H \subset G$ be a normal subgroup of G. Let G act on itself by conjugation. Prove that H is a union of orbits. Is it true if the subgroup is not normal? If not, give an example to justify your claim.

4.6.3. Let G be a finite p-group, that is, order of G is a power of the prime p. Let H be a non-trivial normal subgroup of G. Then prove that $H \cap Z(G) \neq \{e\}$.

4.6.4. Define a map

$$\Psi : \{\text{Group actions } \eta : G \times X \to X\} \to \{\text{Group homomorphisms } \delta : G \to \text{Aut}(X)\}$$

as follows. Given a group action η define $\Psi(\eta)(g) : X \to X$ by

$$\big(\Psi(\eta)(g)\big)(x) = \eta(g, x)\,.$$

Show that $\Psi(\eta)(g)$ is in $\text{Aut}(X)$. Thus, we get a set map $\Psi(\eta) : G \to \text{Aut}(X)$. Show that this is a group homomorphism.

4.6.5. Now define a map

$$\Phi : \{\text{Group homomorphisms } \delta : G \to \text{Aut}(X)\} \to \{\text{Group actions } \eta : G \times X \to X\}$$

as follows. For a group homomorphism δ, define

$$\Phi(\delta)(g, x) = \big(\delta(g)\big)(x)\,.$$

Show that $\Phi(\delta)$ defines an action og G on X.

4.6.6. With Ψ and Φ as in the preceding exercises show that $\Phi \circ \Psi = Id$ and $\Psi \circ \Phi = Id$.

4.6.7. Let G be a group of order 6. Show that the 3-Sylow subgroup is normal in G. More generally, if G is a group of order pq and $p < q$ show that the q-Sylow subgroup is normal.

4.6.8. Consider the set of polynomials in n variable $R := \mathbb{C}[T_1, T_2, \ldots, T_n]$ with coefficients in complex numbers. Let S_n act on R as follows. For a polynomial $f(T_1, T_2, \ldots, T_n)$ define

$$\sigma \cdot f := f(T_{\sigma(1)}, T_{\sigma(2)}, \ldots, T_{\sigma(n)})\,.$$

For example, if $n = 3$ and we take $f(T_1, T_2, T_3) = T_1^2 + T_2^3 + 4T_1T_2T_3^5$, $\sigma = (132)$ then

$$\sigma \cdot f = T_3^2 + T_1^3 + 4T_3T_1T_2^5\,.$$

Show that this defines an action of S_n on R. Further, show that this action has the special property that $\sigma \cdot (f+g) = (\sigma \cdot f) + (\sigma \cdot g)$ and $\sigma \cdot (fg) = (\sigma \cdot f)(\sigma \cdot g)$. In other words this action of S_n on R preserves the addition and multiplication in R.

4.6.9. Continuing with the notation in the above exercise, let

$$P = \prod_{1 \le i < j \le n} (T_i - T_j)\,.$$

Show that for every $\sigma \in S_n$ we have $\sigma \cdot P = \pm P$. For every $\sigma \in S_n$ we denote this sign which appears as $\operatorname{sgn}(\sigma)$. Thus, we have defined a map $\operatorname{sgn} : S_n \to \{\pm 1\}$ and we may write $\sigma \cdot P = \operatorname{sgn}(\sigma) P$. Show that sgn is a surjective group homomorphism. Show that $\operatorname{sgn}(12) = -1$. The kernel of sgn is denoted A_n.

4.6.10. In view of Theorem 4.5.1 every element of S_n may be written as a product of transpositions. Recall that a transposition is a cycle of the form (a, b). Let $\gamma \in S_n$. Suppose we write $\gamma = \prod_{i=1}^{r} \alpha_i = \prod_{j=1}^{l} \beta_j$ as a product of transpositions in two ways. Use sgn to show that $r \equiv l \bmod 2$. Thus, it makes sense to say that an element of S_n is a product of an odd number of transpositions or an even number of transpositions. Clearly, the group A_n contains exactly those elements which are a product of an even number of transpositions.

4.6.11. A group which has no non-trivial normal subgroups is called a simple group. In a series of exercises we shall prove that if $n \ge 5$, then A_n is a simple group. Recall that we had defined the sign homomorphism from S_n to $\{\pm 1\}$ and A_n is the kernel of this homomorphism. Show that the image of a transposition under sgn is -1.

4.6.12. A 3-cycle is a permutation of the form (a_1, a_2, a_3). Show that a 3-cycle is a product of two transpositions.

4.6.13. Let α be a transposition. Show that α cannot be written as a product of 3-cycles. Let α and β be transpositions. Show that the product $\alpha\beta$ can be written as a product of 3-cycles.

4.6.14. Show that every element of A_n can be written as a product of 3-cycles.

4.6.15. For $n \ge 5$ show that there is $\gamma \in A_n$ such that $\gamma(a_1, a_2, a_3)\gamma^{-1} = (a_1, a_3, a_2)$. This is not true for $n = 4$, why? (WARNING: You have to find $\gamma \in A_n$ and not $\gamma \in S_n$)

4.6.16. For $n \geq 5$ show that there is $\gamma \in A_n$ such that $\gamma(a_1, a_2, a_3)\gamma^{-1} = (a_1, a_2, a_4)$.

4.6.17. Notice that $(a_1, a_2, a_3) = (a_2, a_3, a_1)$. Use this observation and the previous two exercises to show that for $n \geq 5$ and permutations $(a, b, c), (a', b', c')$ there is $\gamma \in A_n$ such that $\gamma(a, b, c)\gamma^{-1} = (a', b', c')$.

For the remaining exercises $n \geq 5$.

4.6.18. Let $N \neq \{e\}$ be a normal subgroup of A_n. Suppose there is an element $\alpha = \alpha_1\alpha_2 \dots \alpha_r \in N$ where the α_i are mutually disjoint cycles and $\alpha_1 = (a_1, a_2, a_3, a_4, \dots, a_i)$ with $i \geq 4$. Take $\gamma \in A_n$ to be $\gamma = (a_2, a_3, a_1)$. Show that $\gamma\alpha\gamma^{-1}\alpha^{-1} = (a_4, a_1, a_2)$. Since N is normal we get, using the previous exercises, that N contains all the 3-cycles and so $N = A_n$.

4.6.19. Let us assume that the hypothesis of the previous exercise is not satisfied. This means that every element of N is a product of mutually disjoint cycles of length ≤ 3. Since mutually disjoint cycles commute, we may assume that $\alpha = \alpha_1\alpha_2 \dots \alpha_r$, where the lengths are in decreasing order. If $r = 1$, then N contains α_1 which is either a transposition (this is not possible, why?) or it is a 3-cycle. Thus, if $r = 1$, then we are done, why?

4.6.20. So assume $r \geq 2$. There are three cases now. First, α_1 is a 3-cycle and α_2 is a 3-cycle. Second α_1 is a 3-cycle and α_2 is a transposition. Third, both α_1, α_2 are transpositions.

4.6.21. Consider the first case. Let $\alpha_1 = (a_1, a_2, a_3)$ and $\alpha_2 = (a_4, a_5, a_6)$. Let $\gamma = (a_2, a_3, a_4)$. Show that $\gamma\alpha\gamma^{-1}\alpha^{-1} = (a_1, a_4, a_2, a_3, a_5)$, so we are reduced to the case of exercise 4.6.18.

4.6.22. Consider the second case. Let $\alpha_1 = (a_1, a_2, a_3)$ and $\alpha_2 = (a_4, a_5)$. Let $\gamma = (a_2, a_3, a_4)$. Show that $\gamma\alpha\gamma^{-1}\alpha^{-1} = (a_1, a_4, a_2, a_3, a_5)$, so we are reduced to the case of exercise 4.6.18.

4.6.23. Consider the third case. Let $\alpha_1 = (a_1, a_2)$ and $\alpha_2 = (a_3, a_4)$. Let $\gamma = (a_2, a_3, a_4)$. Show that $\gamma\alpha\gamma^{-1}\alpha^{-1} = (a_1, a_4)(a_2, a_3)$. Thus, N contains $\beta = (a_1, a_4)(a_2, a_3)$. Let $\gamma = (a_1, a_2, a_5)$ and show that $\gamma\beta\gamma^{-1}\beta^{-1} = (a_1, a_4, a_3, a_5, a_2)$, so we are reduced to the case of exercise 4.6.18.

4.6.24. Consider the set

$$SL(2, \mathbb{R}) = G = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad - bc = 1, a, b, c, d \in \mathbb{R}\}.$$

G is the set of 2×2 matrices with real entries with determinant 1. Show that G is a group under matrix multiplication. Consider the set,

$$\mathcal{H} = \{z = x + iy \in \mathbb{C} \mid y > 0\}.$$

Define for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and $z \in \mathbb{C}$,

$$g \cdot z = \frac{az + b}{cz + d}.$$

Show that $g \cdot z$ defines an action on $\mathcal{H}$.

4.6.25. Find Stab(i) for the above action.

4.6.26. Let G be a group with a action on a set X. The action is called transitive if given $x, y \in X$ there exists an element $g \in G$ such that $g \cdot x = y$. Prove that the action defined in exercise 4.6.24 is transitive.

4.6.27. Is the above action transitive if you replace $SL(2, \mathbb{R})$ with

$$SL(2, \mathbb{Z}) = G = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | ad - bc = 1, a, b, c, d \in \mathbb{Z}\}?$$

Chapter 5

Products

5.1 Products

Suppose we are given a collection of groups G_i, indexed by a set I. Then we may form the group

$$\prod_{i \in I} G_i \,.$$

The multiplication is the obvious coordinate wise multiplication. For example, for $G_1 \times G_2$ we multiply

$$(a, \alpha) \cdot (b, \beta) = (ab, \alpha\beta) \,.$$

5.2 Semi-direct products

Let G be a a group and suppose there are two subgroups H and K such that K is normal in G. Then consider the subset

$$KH := \{kh \mid k \in K, h \in H\} \,.$$

We claim that KH is a subgroup of G. Let us first check that it is closed under multiplication. Suppose we are given two elements k_1h_1 and k_2h_2 then we have

$$k_1h_1k_2h_2 = k_1(h_1k_2h_1^{-1})h_1h_2$$

Since K is normal, we have that $h_1k_2h_1^{-1} \in K$ and so the above is also an element of KH. Now assume that the pair of subgroups H and K satisfy the following additional conditions

1. $H \cap K = \{e\}$
2. $KH = G$.

These two conditions force that every element in the group G can be written uniquely as a product kh. We only need to check the uniqueness of this representation as a product. Suppose $k_1h_1 = k_2h_2$ then we get $k_2^{-1}k_1 = h_2h_1^{-1}$. But since the LHS is in K and the RHS is in H, it follows that

$$k_2^{-1}k_1 = h_2h_1^{-1} = e\,,$$

which shows that $h_1 = h_2$ and $k_1 = k_2$. We see that G, as a set, is like a product of H and K. The group structure, however, is different from that of $H \times K$. Moreover, for each element $h \in H$ we get an automorphism of K given by $k \mapsto hkh^{-1}$.

Motivated by this we may define the semi-direct product of two groups as follows.

Definition 5.2.1. *Suppose H and K are groups and suppose we are given a group homomorphism $\varphi : H \to \mathrm{Aut}(K)$. Here $\mathrm{Aut}(K)$ denotes the group of bijective group homomorphisms from K to itself. Then we may form the semi-direct product $K \rtimes_\varphi H$ as follows. The elements of $K \rtimes_\varphi H$ are given by tuples (k, h). Multiplication is defined as*

$$(k_1, h_1) \cdot (k_2, h_2) := \big(k_1\big(\varphi(h_1)(k_2)\big), h_1h_2\big)\,.$$

One easily checks that this product is associative and that it defines a group structure. Suppose we are given two homomorphisms $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(K)$ then we may ask when the resulting groups $K \rtimes_{\varphi_1} H$ and $K \rtimes_{\varphi_2} H$ are isomorphic. In this direction we give two results. Suppose $f : H \to H$ is a group automorphism. Then the groups $K \rtimes_\varphi H$ and $K \rtimes_{\varphi\circ f} H$ are isomorphic. Define a map

$$K \rtimes_{\varphi\circ f} H \to K \rtimes_\varphi H \qquad (k, h) \mapsto (k, f(h))\,. \tag{5.2.2}$$

One easily checks that this defines a group isomorphism. Similarly, suppose $f : K \to K$ is a group automorphism. Then we get the composite $H \xrightarrow{\varphi} \mathrm{Aut}(K) \xrightarrow{c_f} \mathrm{Aut}(K)$. Here c_f is conjugation by f. Precisely,

$$(c_f \circ \varphi)(h) = f \circ \varphi(h) \circ f^{-1}\,.$$

In this case too we have a map defined as follows

$$K \rtimes_\varphi H \to K \rtimes_{c_f\circ\varphi} H \qquad (k, h) \mapsto (f(k), h)\,.$$

One checks easily that this map defines a group isomorphism.

5.3 Exercises

5.3.1. Show that the semi-direct product $K \rtimes_\varphi H$ is a product iff φ is the trivial homomorphism.

5.3.2. Let G and H be finite groups such that there is a prime p such that $p|\#G$ and $p|\#H$. Show that $G \times H$ is not cyclic. (HINT: A cyclic group has a unique subgroup of order d if d divides the order of the group.)

5.3.3. Let G be a finite group. Let R be a normal p-subgroup of G (not necessarily a Sylow subgroup).

1. Show that R is contained in every p-Sylow subgroup of G.

2. Suppose that S is another normal p-subgroup of G then RS is also a normal p-subgroup of G.

3. Show that the subgroup $O_p(G)$, defined as the subgroup generated by all the normal p subgroups of G, is the largest normal p subgroup of G. Show that $O_p(G)$ equals the intersection of all the Sylow p subgroups of G.

4. Prove that $\bar{G} = G/O_p(G)$ has no non-trivial normal p subgroups.

5.3.4. Let K be a group. Consider the set $\mathrm{Aut}(K)$ of bijective group homomorphisms from K to itself. Show that this forms a group under composition of homomorphisms. Let p be a prime. For $l \in (\mathbb{Z}/p\mathbb{Z})^\times$ let m_l denote the multiplication by l map on $\mathbb{Z}/p\mathbb{Z}$. Show that the natural map

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \qquad\qquad l \mapsto m_l$$

is an isomorphism.

5.3.5. Let G be a group of order pq, with $p < q$. Use Sylow's Theorem to conclude that the q-Sylow subgroup is normal. Let K denote the q-Sylow subgroup. Conjugation defines a group homomorphism $\varphi : G \to \mathrm{Aut}(K)$.

1. Show that K is contained in the kernel of φ.

2. If p does not divide $q - 1$, then show that G is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

3. Assume that p divides $q-1$ and that G is not abelian. The map φ factors to give a map $\bar{\varphi} : G/K \to \mathrm{Aut}(K)$. Show that there is a non-trivial homomorphism $\bar{\varphi} : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(K)$ such that G is isomorphic to a semi-direct product $\mathbb{Z}/p\mathbb{Z} \rtimes_{\bar{\varphi}} K$.

4. The group $(\mathbb{Z}/q\mathbb{Z})^\times$ is always cyclic. Although this is not too hard to prove, we will not prove this assertion. Assume that p divides $q-1$. Suppose that there are two non-abelian groups G_1 and G_2 of cardinality pq. Use (5.2.2) to show that G_1 and G_2 are isomorphic. This proves that when p divides $q-1$ there is only one non-abelian group of cardinality pq.

Chapter 6

Finitely generated abelian groups

A group G is said to be finitely generated if there is a finite set $S \subset G$ such that every element of G can be written as a product $\prod_{i=1}^{l} x_i$, where $x_i \in S$. We do not require that the x_i's are distinct. In this chapter we will write abelian groups additively and the identity element will be denoted 0.

6.1 Direct products and direct sums

We have already seen the definition of a direct product of groups, which we now recall. Given groups G_i, for $i \in I$, the direct product of the G_i is the group $\prod_{i\in I} G_i$ with coordinate wise multiplication. Now consider the situation where A_i's are abelian groups. Inside the product $\prod_{i\in I} A_i$ there is a subgroup, which we denote

$$\bigoplus_{i\in I} A_i \subset \prod_{i\in I} A_i$$

and defined as follows. The elements of the set $\bigoplus_{i\in I} A_i$ are precisely those elements of $\prod_{i\in I} A_i$ which are nonzero only in finitely many coordinates. Clearly, this is a subgroup. This group is called the direct sum of the A_i's. When each of the A_i's is isomorphic to $\mathbb{Z}$, then the resulting group is called a free abelian group. Equivalently, an abelian group A is said to be free if there is a collection of elements $a_i \in A$ indexed by a set I such that the

natural map

$$\bigoplus_{i\in I}\mathbb{Z}[e_i]\to A \qquad\qquad \sum_{i\in I} n_i[e_i]\mapsto \sum_{i\in I} n_i a_i$$

is an isomorphism. (The e_i simply indicates the i'th coordinate.) Note that the sum is actually a finite sum since only finitely many of the n_i are non-zero, by the definition of elements in $\bigoplus_{i\in I}\mathbb{Z}[e_i]$.

6.2 Finitely generated torsion free abelian groups

Let A be an abelian group. An element $a\in A$ is called a torsion element if $a\neq 0$ and there is an $n>0$ such that $na=0$. If there is no torsion element in A then we say that A is torsion free. The group $\mathbb{Q}$ under addition is torsion free. Similarly, every free abelian group is torsion free. In this section we will show that a finitely generated and torsion free abelian group is free. First we will define the "rank" of a free abelian group.

Definition 6.2.1. *Let A and B be abelian groups. Let $\mathrm{Hom}(A,B)$ denote the set of homomorphisms of abelian groups $f:A\to B$.*

Using the addition in B we may define a group structure on $\mathrm{Hom}(A,B)$. Given $f,g\in\mathrm{Hom}(A,B)$ define $(f+g)(a):=f(a)+g(a)$. The inverse $(-f)$ is defined as $(-f)(a):=-f(a)$, where $-f(a)$ is the inverse of $f(a)$ in B. One easily checks that $\mathrm{Hom}(A,B)$ is an abelian group with the identity element being the trivial homomorphism, that is, the homomorphism $f:A\to B$ with $f(a)=0$ for all $a\in A$.

Lemma 6.2.2. *Let A be an abelian group and consider the additive group $\mathbb{Q}$. Then $\mathrm{Hom}(A,\mathbb{Q})$ is a $\mathbb{Q}$ vector space.*

Proof. The proof is left as an exercise to the reader. □

Definition 6.2.3. *Let A be an abelian group. The rank of A is defined to be the dimension of the vector space $\mathrm{Hom}(A,\mathbb{Q})$.*

Remark 6.2.4. Now we make the following simple observations.

(1) Let A,B,C be abelian groups. Then there is a natural map

$$\Phi:\mathrm{Hom}(A,C)\oplus\mathrm{Hom}(B,C)\to\mathrm{Hom}(A\oplus B,C)$$

and this is an isomorphism of abelian groups.

(2) Given an abelian group C, there is a natural isomorphism of abelian groups
$$C \to \mathrm{Hom}(\mathbb{Z}, C)\,.$$

(3) Let $\psi : A \to B$ be a group homomorphism. Then it induces a map $\mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ given by $f \mapsto f \circ \psi$.

(4) Let V be a $\mathbb{Q}$ vector space. Then it is also an abelian group under the operation of vector addition. It is easily checked (using the definition of a vector space) that V is a torsion free abelian group. If W is another $\mathbb{Q}$ vector space and $T : V \to W$ is a group homomorphism, then T is also a $\mathbb{Q}$-linear map.

Let us check the first assertion. Suppose we are given $f \in \mathrm{Hom}(A, C)$ and $g \in \mathrm{Hom}(B, C)$. Then we define $\Phi(f, g) \in \mathrm{Hom}(A \oplus B, C)$ as follows
$$\Phi(f, g)(a, b) := f(a) + g(b)\,.$$
It is trivial to check that Φ is a group homomorphism, and this is left to the reader. Clearly, A sits inside $A \oplus B$ as $(a, 0)$. Thus, if $\Phi(f, g) = 0$ then restricting it to A it follows that $f = 0$. Similarly, we get that $\Phi(f, g) = 0$ implies that $g = 0$. This shows that Φ is an inclusion. Suppose we are given $h \in \mathrm{Hom}(A \oplus B, C)$ then let f be the restriction of h to A and let g be the restriction of h to B. It can be checked easily that $\Phi(f, g) = h$, which shows that Φ is surjective.

The second assertion is also easily checked using the fact that a homomorphism from $\mathbb{Z} \to C$ is defined completely by the image of 1. We leave it to the reader to check (2), and the remaining assertions. □

By $\mathbb{Z}^{\oplus r}$ we mean the group $\bigoplus_{i=1}^{r} \mathbb{Z}[e_i]$.

Lemma 6.2.5. *Suppose there is an isomorphism $\phi : \mathbb{Z}^{\oplus r} \xrightarrow{\sim} \mathbb{Z}^{\oplus s}$. Then $r = s$.*

Proof. In view of the isomorphism ϕ we get an isomorphism of groups
$$\mathrm{Hom}(\mathbb{Z}^{\oplus s}, \mathbb{Q}) \to \mathrm{Hom}(\mathbb{Z}^{\oplus r}, \mathbb{Q})\,.$$
As observed above, both these are vector spaces and this group homomorphism is actually a vector space homomorphism. Since this map is bijective, it follows that these vector spaces are isomorphic. However, by the observations above we get that the ranks are s and r, respectively. Thus, it follows that $r = s$. □

The following theorem is the key input in proving the main result in the chapter.

Theorem 6.2.6. *Let $A \subset B$ be abelian groups. Then the induced map* $\mathrm{Hom}(B, \mathbb{Q}) \to \mathrm{Hom}(A, \mathbb{Q})$ *is surjective.*

Proof. Let $f : A \to \mathbb{Q}$ be an element of $\mathrm{Hom}(A, \mathbb{Q})$. Consider pairs (C, g) where $A \subset C \subset B$ and $g : C \to \mathbb{Q}$ is a map whose restriction to A is f. Our aim is to show that there is a pair (B, h). This is a standard argument using Zorn's lemma and we briefly sketch the argument. Introduce a partial order on the pair $(C, g) \leq (C', g')$ iff $C \subset C'$ and the restriction of g' to C is g. Arguing "as usual" we see that maximal elements exist.

Let (C, g) be a maximal pair with respect to this ordering. Assume that $C \subsetneqq B$. Choose $b \in B \setminus C$.

Suppose there is an $n > 0$ such that $nb \in C$, then let n be the smallest such positive integer. Consider the map

$$C \oplus \mathbb{Z} \to B$$

given by $(c, l) \mapsto c + lb$. The image of this is precisely the subgroup of B generated by C and b. Let us denote this subgroup by C'. Suppose (c, l) is in the kernel. Then this means that $lb = -c \in C$. It is easily checked, using Proposition 3.3.1, that n divides l. Thus, writing $l = kn$ we see that the kernel exactly contains elements of the type $(-knb, kn)$. Next we define a homomorphism from $C \oplus \mathbb{Z} \to \mathbb{Q}$. Using the bijection Φ it follows that we only need to specify homomorphisms $C \to \mathbb{Q}$ and $\mathbb{Z} \to \mathbb{Q}$. Take $g : C \to \mathbb{Q}$ and define $h : \mathbb{Z} \to \mathbb{Q}$ by sending 1 to $\frac{1}{n}g(nb)$. It is trivial to check that $(-knb, kn) \mapsto 0$. Thus, using Theorem 3.4.2 it follows that we get a homomorphism $g' : C' \to \mathbb{Q}$. The restriction of this homomorphism to C is clearly g. This contradicts the maximality of the pair (C, g). Thus, it is forced that $C = B$.

Now consider the second case when there is no $n > 0$ such that $nb \in C$. This implies that the natural map $C \oplus Z \to B$ given by $(c, n) \mapsto c + nb$ has no kernel. Thus, it is an isomorphism onto its image, which is precisely the subgroup generated by C and b, and denoted as C'. As before, we may define a homomorphism $C' \to \mathbb{Q}$ by specifying it to be g on C and, for example, 0 on $\mathbb{Z}$. Again, this produces a pair (C', g') which contradicts the maximality of (C, g). Thus, it is forced that $C = B$.

This completes the proof of the Theorem. □

Lemma 6.2.7. *Let A be a torsion free group who rank is 0. Then $A = 0$.*

Proof. Note that an element $a \in A$ is torsion free iff the map from $\mathbb{Z} \to A$ given by sending $1 \mapsto a$ is injective. Suppose there is such an $a \in A$. Then we have an inclusion $0 \to \mathbb{Z} \to A$. From the previous Theorem we get that there is a surjection $\mathrm{Hom}(A, \mathbb{Q}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Q})$. But note that $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) = \mathbb{Q}$. But if the rank of A is 0, then this is not possible. Thus, it is forced that $A = 0$. □

Proposition 6.2.8. *Let $A \subset \mathbb{Z}^{\oplus r}$ be a subgroup. Then A is free. Moreover $A \cong \mathbb{Z}^{\oplus s}$ where $s = \mathrm{rank}(A)$.*

Proof. We will prove this proposition by induction on the rank of A. The base case for induction is when the rank of A is 0. But then the preceding Lemma shows that $A = 0$, and so the proposition is true in this case. From now on we assume that $\mathrm{rank}(A) = s \geq 1$ and that the proposition is true when rank $< s$.

We may assume that the projection $A \subset \mathbb{Z}^{\oplus r} \xrightarrow{\pi} \mathbb{Z}$ onto the first coordinate is non-zero. Let B denote the image of A. By exercise 2.4.1 it follows that B is generated by one element, say b, that is, $B \cong \mathbb{Z}$. In terms of a diagram this means that the following commutes

$$\begin{array}{ccc} A & \xhookrightarrow{i} & \mathbb{Z}^{\oplus r} \\ {\scriptstyle \pi \circ i}\downarrow & & \downarrow{\scriptstyle \pi} \\ b\mathbb{Z} & \hookrightarrow & \mathbb{Z} \end{array}$$

Thus, we have a surjective map $A \to b\mathbb{Z} \cong \mathbb{Z}$. Apply exercise 3.5.16 we see that $A \cong K \times \mathbb{Z}$, where K denotes the kernel of this map. Since A is torsion free, it easily follows that K is torsion free. We saw in Remark 6.2.4 that

$$\mathrm{Hom}(A, \mathbb{Q}) = \mathrm{Hom}(K, \mathbb{Q}) \oplus \mathrm{Hom}(\mathbb{Z}, \mathbb{Q})\,.$$

In view of this $\mathrm{rank}(K) = s - 1 < s$. It is clear that $K \subset \mathbb{Z}^{\oplus r-1} = (0, \alpha_2, \alpha_3, \ldots, \alpha_r) \subset \mathbb{Z}^{\oplus r}$. By induction we see that K is free and $K \cong \mathbb{Z}^{\oplus s-1}$. Since $A \cong K \times \mathbb{Z}$ it follows that $A \cong \mathbb{Z}^{\oplus s}$. This completes the proof of the proposition. □

Theorem 6.2.9. *Let A be a finitely generated and torsion free abelian group of rank s. Then A is isomorphic to $\mathbb{Z}^{\oplus s}$.*

Proof. The idea of the proof is to reduce to the case of the previous proposition. Since A is finitely generated there is an r and a surjective group homomorphism $\phi : \mathbb{Z}^{\oplus r} \to A$. One easily checks that the map

$$\mathrm{Hom}(A, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}^{\oplus r}, \mathbb{Z})$$

induced by ϕ is an inclusion. As explained in Remark 6.2.4, it is easily checked that $\mathrm{Hom}(\mathbb{Z}^{\oplus r}, \mathbb{Z}) \cong \mathbb{Z}^{\oplus r}$. Thus, we are in the situation of the previous proposition, which yields that $\mathrm{Hom}(A, \mathbb{Z}) \cong \mathbb{Z}^{\oplus l}$.

Next we claim that there is a natural map

$$ev : A \to \mathrm{Hom}(\mathrm{Hom}(A, \mathbb{Z}))$$

which is an inclusion when A torsion free. This map is defined as follows

$$ev(a)(f) := f(a)\,.$$

Consider the map from $\mathbb{Z} \to A$ which sends $1 \mapsto a$. Since A is torsion free this map is an inclusion. From Theorem 6.2.6 we know that the induced map $\mathrm{Hom}(A, \mathbb{Q}) \to \mathrm{Hom}(\mathbb{Z}, \mathbb{Q})$ is surjective. Let $f \in \mathrm{Hom}(A, \mathbb{Q})$ be such that the image of f is non-zero. Let $a_1, a_2, \ldots, a_r$ be a set of generators for A. Write $f(a_i) = m_i/n_i$ and let n be the lcm of the n_i's. Then the image of f lands inside $\frac{1}{n}\mathbb{Z} \subset \mathbb{Q}$. Since multiplication by n defines an isomorphism $\frac{1}{n}\mathbb{Z} \cong \mathbb{Z}$, it follows that the map $(nf) : A \to \mathbb{Z}$ is such that $(nf)(a) \neq 0$. This shows that $ev(a) \neq 0$. Thus, ev is an inclusion. This shows that

$$A \xrightarrow{\sim} ev(A) \subset \mathbb{Z}^{\oplus l}\,.$$

Finally applying the previous proposition again we see that A is free. If we write $A \cong \mathbb{Z}^{\oplus t}$, then using $\mathrm{Hom}(A, \mathbb{Q}) \cong \mathrm{Hom}(\mathbb{Z}^{\oplus t}, \mathbb{Q})$ we see that $t = s = \mathrm{rank}(A)$. This completes the proof of the Theorem. □

Remark 6.2.10. For a free abelian group $\mathbb{Z}^{\oplus r}$ it is easily checked that ev defined above is an isomorphism. Thus, it follows that for a torsion free and finitely generated abelian group the map ev is an isomorphism.

6.3 Exercises

6.3.1. Let V be a $\mathbb{Q}$ vector space. Then it is also an abelian group under the operation of vector addition. Show that (using the definition of a vector space) V is a torsion free abelian group.

6.3.2. In continuation with the above exercise, if W is another $\mathbb{Q}$ vector space and $T : V \to W$ is a group homomorphism, show that T is also a $\mathbb{Q}$-linear map.

Structure theorem for finite abelian groups.

6.3.3. Let G be an abelian group. From Sylow's theorem it is clear that for every prime dividing the order of G, there is a unique p-Sylow subgroup of G, call this $G(p)$. Suppose $\#G = \prod_{i=1}^{n} p_i^{r_i}$. Since G is abelian, there is an obvious group homomorphism

$$\Psi : \prod_{i=1}^{n} G(p_i) \to G. \tag{6.3.4}$$

What is this group homomorphism?

6.3.5. Suppose H and H' are subgroups of G such that $gcd(\#H, \#H') = 1$, then show that $H \cap H' = \{e\}$. Use this to show that the map Ψ above is an inclusion and so an isomorphism.

In view of the above exercise, it suffices to understand the structure of abelian groups of order p^n. In the next several exercises G will be a group of order p^n. A character of G is a group homomorphism $\chi : G \to S^1 := \{z \in \mathbb{C} \,|\, |\, z \,| = 1\}$.

6.3.6. Let $H \subset G$ be a subgroup. Let $x \in G \setminus H$ and let a be the smallest positive integer such that $ax \in H$. Show that a is a power of p.

6.3.7. Show that the kernel of the natural map $H \times \langle x \rangle \to G$, given by $(h, mx) \mapsto h + mx$, is cyclic and generated by the element $(-ax, ax)$. Here $\langle x \rangle$ is the subgroup of G generated by x.

6.3.8. Let χ be a character of H. Show that we can extend χ to a character of the subgroup generated by H and x. Show that we can extend χ to a character of G. (HINT: Define a character of $H \times \langle x \rangle$ which is trivial on $(-ax, ax)$ and is equal to χ when restricted to H)

6.3.9. Show that any finite subgroup of S^1 is cyclic. In particular, for any character χ, the image $\chi(G)$ is cyclic.

6.3.10. Let x_0 be an element of G of largest possible order, say p^m. Consider the character of $\langle x_0 \rangle$ defined by imposing $\chi(x_0) := e^{2\pi i/p^m}$. Extend this to a character χ of G. Show that $\chi(G)$ is equal to the subgroup of S^1 generated by $e^{2\pi i/p^m}$. Apriori, $\chi(G)$ could have been a larger subgroup than the one generated by $e^{2\pi i/p^m}$.

6.3.11. Show that $\langle x_0\rangle \cap \mathrm{Ker}(\chi) = \{0\}$. Show that the natural map $\mathrm{Ker}(\chi) \times \langle x_0\rangle \to G$ is an isomorphism. Conclude the proof of the following. Let G be a finite abelian group of size p^n. Then $G \cong \mathbb{Z}/p^{r_1} \times \ldots \times \mathbb{Z}/p^{r_t}$ with $\sum_{i=1}^{t} r_i = n$. We may further assume that $r_1 \leq r_2 \leq \ldots \leq r_t$.

6.3.12. Show that there exist characters $\chi_1, \chi_2, \ldots, \chi_t$ such that the map

$$g \mapsto (\chi_1(g), \chi_2(g), \ldots, \chi_t(g))$$

induces an isomorphism

$$G \xrightarrow{\sim} \chi_1(G) \times \chi_2(G) \times \ldots \times \chi_t(G)\,.$$

6.3.13. Let $g \in G \setminus pG$. Show that there is an i such that $\chi_i(\langle g\rangle) = \chi_i(G)$. Show that $\mathrm{Ker}(\chi_i) \times \langle g\rangle \to G$ is an isomorphism.

6.3.14. Let H be a non-trivial and proper subgroup of G. Let a be the largest positive integer such that $H \subset p^a G$. Define

$$H' := \{g \in G \,|\, p^a g \in H\}$$

Show that $p^a H' = H$.

6.3.15. Show that $H' \not\subset pG$.

6.3.16. Let $h \in H' \setminus pG$. From exercise 6.3.13, we can find χ such that $\mathrm{Ker}(\chi) \times \langle h\rangle \to G$ is an isomorphism. Show that $\mathrm{Ker}(\chi|_{H'}) \times \langle h\rangle \to H'$ is an isomorphism. Conclude by induction on the size of G that there is an isomorphism

$$\Phi : G \xrightarrow{\sim} \mathbb{Z}/p^{r_1}\mathbb{Z} \times \mathbb{Z}/p^{r_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

such that the image of H' is a subgroup of the type

$$p^{a_1}\mathbb{Z}/p^{r_1}\mathbb{Z} \times p^{a_2}\mathbb{Z}/p^{r_2}\mathbb{Z} \times \cdots \times p^{a_t}\mathbb{Z}/p^{r_t}\mathbb{Z}\,.$$

Since $H = p^a H'$ it follows that H is also of the same type.

6.3.17. Now let G be any finite abelian group, not necessarily a p-group. Use equation (6.3.4) to show that there are integers $1 < n_1 \leq n_2 \leq \ldots \leq n_r$ such that n_i divides n_{i+1} and

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}\,.$$

6.3.18. Let G be a finite abelian group. Show that the set of characters of G is a finite set. This set is often denoted $\hat{G}$. There is a natural group structure on $\hat{G}$, what is it?

6.3.19. Let G be a finite group. Show that the set of characters of G is a finite group.

6.3.20. Show that the set of characters of $\mathbb{Q}$ is not a finite group.

6.3.21. Let A be an abelian group. Let $\mathrm{Tors}(A)$ denote the set which contains all torsion elements of A and 0. Show that $\mathrm{Tors}(A)$ is a subgroup of A. Show that the quotient $A/\mathrm{Tors}(A)$ has no torsion.

6.3.22. In the remaining exercises let A be a finitely generated abelian group. Then $A/\mathrm{Tors}(A)$ is a finitely generated and torsion free abelian group, and so is free. Show that we get a surjective map $A \to \mathbb{Z}^{\oplus r}$ whose kernel is exactly $\mathrm{Tors}(A)$.

6.3.23. Let $a_1, \ldots, a_r \in A$ be elements which map to $e_i \in \mathbb{Z}^{\oplus r}$. Let $H \subset A$ be the subgroup of A generated by the a_i's. Show that $H \cong \mathbb{Z}^{\oplus r}$.

6.3.24. Show that the obvious map $\mathrm{Tors}(A) \oplus H \to A$ is an isomorphism. In particular, this shows that there is a surjection $A \to \mathrm{Tors}(A)$, proving that $\mathrm{Tors}(A)$ is a finitely generated torsion abelian group. Show that $\mathrm{Tors}(A)$ is a finite abelian group.

6.3.25. Show that every finitely generated abelian group is isomorphic to

$$\mathbb{Z}^{\oplus r} \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

where $1 \leq n_1$ and n_i divides n_{i+1}.