PMATH 336 Course Notes - Spring 2019

Max Zhu

August 5, 2019

Contents

1 Groups

1.1 Definition and simple examples

Groups are used for describing symmetries of objects, and for finding solutions to equations. Before formally defining what a group is, we will start with some examples and note their properties.

Example 1.1: Integers with addition

$(\mathbb{Z}, +)$, the integers with usual addition, is a group. We notice the following properties.

- For all $a, b \in \mathbb{Z}$ we have $a + b \in \mathbb{Z}$. **(closure)**
- There is an identity $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, we have $a + 0 = 0 + a = a$. **(identity)**
- Every integer $a \in \mathbb{Z}$ has an inverse $a^{-1} \in \mathbb{Z}$ such that $a + a^{-1} = a^{-1} + a = 0$. Here, $a^{-1} = -a$. **(inverses)**
- Let $a, b, c \in \mathbb{Z}$. Then, $(a + b) + c = a + (b + c)$. **(associativity)**

Example 1.2: Rationals with addition

$(\mathbb{Q}, +)$, rational numbers with usual addition, is a group. Similarly to the integers,

- For all $a, b \in \mathbb{Q}$ we have $a + b \in \mathbb{Q}$. **(closure)**
- There is an identity $0 \in \mathbb{Q}$ such that for all $a \in \mathbb{Q}$, we have $a + 0 = 0 + a = a$. **(identity)**
- Every integer $a \in \mathbb{Q}$ has an inverse $a^{-1} \in \mathbb{Q}$ such that $a + a^{-1} = a^{-1} + a = 0$. Here, $a^{-1} = -a$. **(inverses)**
- Let $a, b, c \in \mathbb{Q}$. Then, $(a + b) + c = a + (b + c)$. **(associativity)**

Example 1.3: Real and complex numbers with addition

$(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are also groups, and these properties can be easily verified.

Example 1.4

$(\{1, 1, i, -i\}, \cdot)$ is a group. We can create a table to show the result of the operation on any two elements of the set:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

This kind of table is called a Cayley table.

- Note that each row and column contains each element exactly once.
- From the Cayley table, the set is closed under $\cdot$.
- The identity is 1.
- Each element has an inverse in the set:

$$\begin{aligned}(1)^{-1} &= 1\\(-1)^{-1} &= -1\\(i)^{-1} &= -i\\(-i)^{-1} &= i\end{aligned}$$

Definition 1.5: Group

Let G be a set, and $\star : G \times G \to G$ be a binary operation on G. We say $(G, \star)$ is a group if it satisfies the following conditions:

(i) Associativity: Let $a, b \in G$. Then, $(a \star b) \star c) = a \star (b \star c)$.

(ii) Identity: There exists $e \in G$ such that for all $a \in G$, we have $a \star e = e \star a = a$.

(iii) Inverses: For all $a \in G$, there exists $a \in\in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

Remark 1.6

- When proving a set G with an operation $\star$ is a group, we must also show G is closed under $\star$.
- We often refer to a group $(G, \star)$ as simply G.
- We often write ab instead of $a \star b$ for some operation $\star$.
- We usually denote the identity element of a group with e.

Proposition 1.7: Nonzero rationals with multiplication is a group

$(\mathbb{Q}\backslash\{0\}, \cdot)$, nonzero rationals with usual multiplication, is a group.

Proof. We use the notation $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$.
Let $a, b, c, d, e, f \in \mathbb{Z}$ so $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}^*$. Then,

(i) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}^*$ **(closure)**

(ii) $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$ **(associativity)**

(iii) $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1} = \frac{a}{b}$ **(identity)**

(iv) $\frac{a}{b} \cdot \frac{b}{a} = \frac{b}{a} \cdot \frac{a}{b} = \frac{1}{1}$, and $\frac{b}{a} \in \mathbb{Q}^*$ **(inverses)**

So, $(\mathbb{Q}^*, \cdot)$ has all required properties of a group. □

Example 1.8: Integers modulo n with addition

$(\mathbb{Z}_n, +)$, integers modulo n with addition is a group.
Here, $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$ where $[a] = \{b \in \mathbb{Z} : b$ has remainder a when dividing by n$\}$, and $[a] + [b] = [a + b]$. To save space, we may write a instead of $[a]$. Let us use $\mathbb{Z}_5$ as an example.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Here is the Cayley table for $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

We can quickly verify the 4 properties. Let $[a], [b], [c] \in \mathbb{Z}_5$. Then,

(i) Closure: obvious from the Cayley table.

(ii) Associativity: $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + c = ([a] + [b]) + c$

(iii) Identity: $[0] + [a] = [0 + a] = [a] = [a + 0] = [a] + [0]$

(iv) Inverses: $[a]^{-1} = [-a] = [n - a]$

Example 1.9: "Integers modulo n" with multiplication

$(\mathbb{Z}_n^*, \cdot)$, where $\mathbb{Z}_n^* := \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ and $[a] \cdot [b] = [ab]$, is a group. Let us use $\mathbb{Z}_6^*$ as an example.

$\mathbb{Z}_6^* = \{1, 5\}$. Note, $4 \notin \mathbb{Z}_6^*$ since $2|4$ and $2|6$, so $\gcd(4, 6) = 2 \neq 1$. Here is the Cayley table for $\mathbb{Z}_6^*$:

$\cdot$	1	5
1	1	5
5	5	1

Here, the identity is 1 and the inverses are $(5)^{-1} = 5$ and $(1)^{-1} = 1$.

Example 1.10: General linear group in $\mathbb{R}$

We define the group $GL_n(\mathbb{R})$ to be the set $\{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$ with usual matrix multiplication. We can easily verify the properties. Let $A, B \in GL_n(\mathbb{R})$. Then,

(i) Closure: $\det(AB) = \det(A)\det(B) \neq 0$ so $AB \in GL_n(\mathbb{R})$.

(ii) Associativity: matrix multiplication is known to be associative.

(iii) Identity: $\det(I) = 1 \neq 0$ where $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ is the identity matrix.

(iv) Inverses: usual matrix inverses, since $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$ so $A^{-1} \in GL_n(\mathbb{R})$.

Definition 1.11: Abelian groups

A group $(G, \star)$ is <u>abelian</u> if for all $a, b \in G$ we have $a \star b = b \star a$. Otherwise, the group is <u>non-abelian</u>.

Example 1.12: Some abelian groups

$(\mathbb{Z}, +), (\mathbb{Q}^*, \cdot), (\mathbb{Z}_n, +), (\mathbb{Z}_n^*)$ are all abelian.

Example 1.13: Dihedral groups

Dihedral groups $(D_n, \cdot)$ are a family of groups of symmetries of a regular n-gon. The operations can be thought of as operations that change places of the vertices but not the overall shape of the polygon. Let us use D_4 as an example.

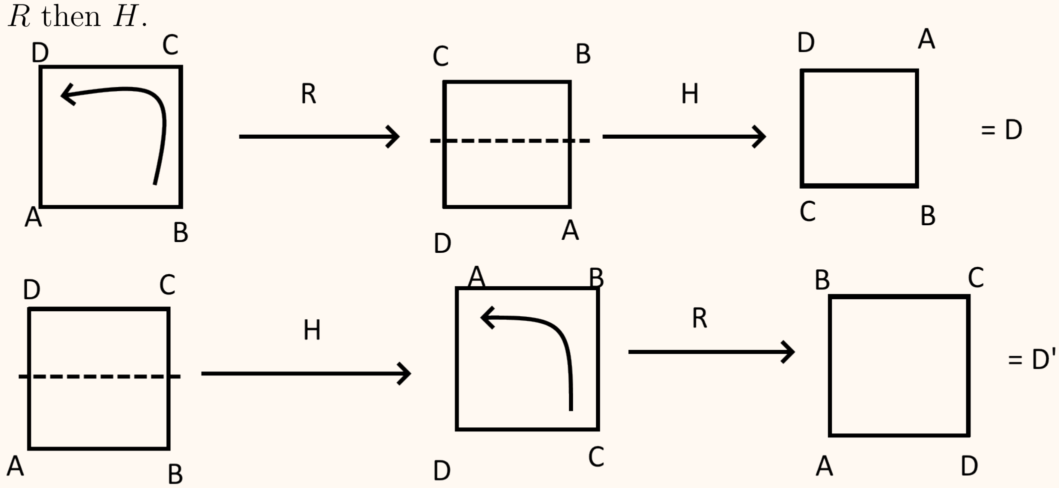
D_4 is the group of symmetries of a square. Elements of D_4 include:

- e, rotation by 0°.
- R, rotation by 90°counter-clockwise.
- R^2, rotation by 180°counter-clockwise.
- R^3, rotation by 270°counter-clockwise.

We also have flips:

- H, flip through horizontal axis.
- V, flip through vertical axis.
- D, flip through top-left bottom-right diagonal axis.
- D', flip through top-right bottom-left diagonal axis.

The elements are functions from a set of vertices to itself which preserves distance and adjacent-ness. The operator is composition of functions. For example, HR is application of R then H.



From this MS Paint illustration of some operations in D_4, it is clear that D_4 is non-abelian.

Definition 1.14: Order of a group

Let $(G, \star)$ be a group. The order of G is the number of elements in G, which is denoted $|G|$. If G is infinite, we say $|G| = \infty$.

Example 1.15: Orders of some groups

$$\begin{aligned} |Z_n| &= n \\ |Z_n^*| &= \phi(n) \text{ (Euler's totient function)} \\ |(\mathbb{Z}, +)| &= \infty \\ |D_n| &= 2n \end{aligned}$$

1.2 Properties of groups

Proposition 1.16: Uniqueness of identity

In a group G, there is only one identity element.

Proof. Assume there are 2 identities $e, f \in G$. Since e is an identity,

$$ef = fe = f$$

And since f is an identity,

$$fe = ef = e$$

Therefore $e = f$. □

Proposition 1.17: Uniqueness of inverses

Let G be a group. If b, c are both inverses of a then $b = c$.

Proof. Suppose $e = ab = ac$. Then,

$$\begin{aligned} ab &= ac \\ b(ab) &= b(ac) \\ (ba)b &= (ba)c \text{ [associativity]} \\ eb &= ec \text{ [by hypothesis]} \\ b &= c \text{ [identity]} \end{aligned}$$

as required. □

Proposition 1.18: Cancellation

If G is a group, for all $a, b, c \in G$ we have:

$$ab = ac \implies b = c \text{ [Left cancellation]}$$
$$ba = ca \implies b = c \text{ [Right cancellation]}$$

Proof. Let $a, b, c \in G$ such that $ab = ac$. Then,

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \text{ [associativity]} \\ eb &= ec \text{ [inverses]} \\ b &= c \text{ [identity]} \end{aligned}$$

As required. Right cancellation has similar proof. $\square$

Remark 1.19

Cancellation should be on the same side. For example in D_4, $RH = D' = VR$ but $H \neq V$.

Proposition 1.20: Socks-shoes

Let G be a group with $a, b \in G$. Then, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a(ea^{-1}) \\ &= aa^{-1} \\ &= e \end{aligned}$$

so $(ab)^{-1} = b^{-1}a^{-1}$ as required. $\square$

Definition 1.21: Exponentiation

Let $(G, \star)$ be a group, with $a \in G$, $n \in \mathbb{Z}$. Then,

$$a^n := \begin{cases} \underbrace{a \star \cdots \star a}_{\text{n times}}, & n > 0 \\ e, & n = 0 \\ \underbrace{a^{-1} \star \cdots \star a^{-1}}_{\text{n times}}, & n < 0 \end{cases}$$

Note: some exponential properties work. For example,

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

However, in general $(ab)^n \neq a^n b^n$ for $a.b \in G$ unless G is abelian.

Definition 1.22: Order of an element

Let G be a group with $a \in G$. The <u>order</u> of a is the smallest positive integer such that $a^k = e$. We denote this by $|a| = k$. If $a^k \neq e$ for all $k \in \mathbb{Z}$, we say $|a| = \infty$.

Example 1.23: Some orders of group elements

- In all groups, $|e| = 1$
- In D_4, $|V| = 2$
- In $\mathbb{Z}_{15}^*$, $|2| = 4$
- In $\mathbb{Z}$, all nonzero elements have order ∞
- In $\mathbb{Q}^*$, $|1| = 1$ and $|-1| = 2$

Definition 1.24: Direct products

Let $(G, \star), (H, \cdot)$ be groups. Then, the set $G \times H = \{(g, h) : g \in G, h \in H\}$ with operation $(g_1, h_1)\Delta(g_2, h_2) := (g_1 \star g_2, h_1 \cdot h_2)$ is a group. $(G \times H, \Delta)$ is called the <u>direct product</u> of G and H.

1.3 Subgroups

Definition 1.25: Subgroup

Let $(G, \star)$ be a group, and $H \subseteq G$. Then H is a subgroup of G if $(H, \star)$ is a group.

If H is a subgroup of G, we say $H \leq G$ and if $H \subsetneq G$, we say $H < G$.

If $(H, \star)$ is not a group, we say $H \nleq G$.

Example 1.26: Some easy subgroups

For all groups $(G, \star)$, we know $\{e\} \leq G$ and $G \leq G$.

Example 1.27: Subgroups of $\mathbb{Z}$

Define $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$. Then, $(n\mathbb{Z}, +)$ is a group, so $n\mathbb{Z} \leq \mathbb{Z}$.

Proposition 1.28: One-step test

Let G be a group, and $\emptyset \neq H \subseteq G$. If for all $a, b \in H$ we have $ab^{-1} \in H$, then $H \leq G$.

Proof. Let $a, b \in H$, since $H \neq \emptyset$.

(i) Associativity: follows from G being a group.

(ii) Identity: By hypothesis $aa^{-1} \in H$, so $e \in H$.

(iii) Inverses: We know $e \in H$, so by hypothesis $ea^{-1} \in H$ so $a^{-1} \in H$.

(iv) Closure: By inverses $b^{-1} \in H$, so by hypothesis $a(b^{-1})^{-1} \in H$ thus $ab \in H$.

So H satisfies all requirements of a group. □

Proposition 1.29: Two-step test

Let $(G, \star)$ be a group, and $\emptyset \neq H \subseteq G$. If $a, b \in H \implies ab \in H$ and $a \in H \implies a^{-1} \in H$, then $H \leq G$.
In other words, $H \leq G$ iff H is closed under $\star$ and closed under inverses.

Proof. Let $a, b \in H$, since $H \neq \emptyset$.

(i) Associativity: follows from G being a group.

(ii) Identity: by hypothesis, $a^{-1} \in H$. Therefore, $aa^{-1} = e \in H$.

(iii) Inverses: by hypothesis.

(iv) Closure: by hypothesis.

So H satisfies all requirements of a group. □

Example 1.30: Center of a group

The center of a group G is defined

$$Z(G) := \{a \in G : ag = ga \text{ for all } g \in G\}$$

and is a subgroup of G.

Proof. Let $g \in G$ and $a, b \in Z(G)$. We know $eg = ge$ for all $g \in G$, so $Z(G) \neq \emptyset$. Now,

$$\begin{aligned}
(ab)g &= a(bg) \\
&= a(gb) \\
&= (ag)b \\
&= (ga)b \\
&= g(ab)
\end{aligned}$$

So $ab \in Z(G)$. Also, since $a \in Z(G)$,

$$\begin{aligned}
ax &= xa \\
a^{-1}(ax) &= a^{-1}(xa) \\
(a^{-1}a)x &= a^{-1}(xa) \\
ex &= a^{-1}(xa) \\
x &= a^{-1}(xa) \\
xa^{-1} &= a^{-1}(xa)a^{-1} \\
xa^{-1} &= (a^{-1}x)(aa^{-1}) \\
xa^{-1} &= (a^{-1}x)e \\
xa^{-1} &= a^{-1}x
\end{aligned}$$

So $a^{-1} \in Z(G)$. By two-step test, $Z(G) \leq G$. $\square$

Note: A group G is abelian iff $Z(G) = G$.

Example 1.31: Centralizer of a group element

The centralizer of an element of a group $g \in G$ is defined

$$C(g) := \{a \in G : ag = ga\}$$

and is a subgroup of G.

Proof. Let $g \in G$ and $a, b \in C(g)$. Then,

$$\begin{aligned} bg &= gb \\ b^{-1}bg &= b^{-1}gb \\ b^{-1}bgb^{-1} &= b^{-1}gbb^{-1} \\ gb^{-1} &= b^{-1}g \\ \therefore b^{-1} &\in C(g) \end{aligned}$$

so $C(g)$ is closed under inverses. Also,

$$\begin{aligned} (ab)g &= a(bg) \\ &= a(gb) \\ &= (ag)b \\ &= (ga)b \\ &= g(ab) \\ \therefore ab &\in C(g) \end{aligned}$$

so $C(g)$ is closed under the group operation. By two-step test, $C(g) \leq G$ for all $g \in G$. $\square$

Note: $Z(G) = \bigcap_{g \in G} C(g)$.

Remark 1.32: Aside

The definition of centralizer was not given here in the original notes but it is used later and makes most sense to be here.

Definition 1.33: Generator of a group

Let G be a group, with $a \in G$. Then, $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$. This is the (sub)group generated by a and a is called the generator of this group.

Remark 1.34

Not all subgroups are generated by a single element. For example, if $H = \{(0,0), (0,2), (2,0), (2,2)\}$ then $H \leq \mathbb{Z}_4 \times \mathbb{Z}_4$ but H is not generated by any of its elements.

2 Lagrange's theorem

2.1 Cosets

Definition 2.1: Coset

Let G be a group and $H \leq G$.
For any $a \in G$,

$$aH := \{ah : h \in H\}$$

is the <u>left coset of H containing a in G</u> and

$$Ha := \{ha : h \in H\}$$

is the <u>right coset of H containing a in G</u>. We denote the number of left cosets of H in G by $|G : H|$, and call it the <u>index of H in G</u>.

Example 2.2: Cosets of $\mathbb{Z}_9$

Let $G = \mathbb{Z}_9$, $H = \{0, 3, 6\} = \langle 3 \rangle$. Then,

$$\begin{aligned} 0 + H &= \{0, 3, 6\} = 3 + H = 6 + H \\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H \\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H \end{aligned}$$

We can make several observations.

- aH may not be a group.
- aH may be equal to bH even if $a \neq b$.
- All cosets are the same size.
- No element is in two different cosets.

We will use some of these observations to prove Lagrange's theorem.

Lemma 2.3

Let G be a group and $H \leq G$. Every element of G is in some left coset of H.

Proof. Let $a \in G$. Then, $a = ae$ and $e \in H$ so $a \in aH$. $\square$

Lemma 2.4

Let G be a group and $H \leq G$. Let $a, b \in G$. Then, $aH = bH$ or $aH \cap bH = \emptyset$.

Proof. Assume $aH \cap bH \neq \emptyset$. We will show that $aH = bH$.
By hypothesis there is $c \in aH \cap bH$, so $c = ah_1 = bh_2$ for $h_1, h_2 \in H$. Let $ah \in aH$ for some $h \in H$. Then,

$$\begin{aligned} ah &= aeh \\ &= a(h_1 h_1^{-1})h \\ &= (ah_1)(h_1^{-1}h) \\ &= bh_2 h_1^{-1} h \end{aligned}$$

So $ah \in bH$ since $h_2 h_1^{-1} h \in H$. Thus $aH \subseteq bH$ and similarly $bH \subseteq aH$. Therefore, $aH = bH$. $\square$

Lemma 2.5

Let G be a group and $H \leq G$. Any left coset of H has the same number of elements as H.

Proof. Let $a \in G$. We will show $|aH| = |H|$.
Let $f : H \to aH$ be defined $f(h) := ah$ for all $h \in H$. Then,

- f is injective: Let $h_1, h_2 \in H$. Then, $f(h_1) = f(h_2) \implies ah_1 = ah_2 \implies h_1 = h_2$ by cancellation.
- f is surjective: Let $ah \in aH$. Then, $f(h) = ah$.

So f is a bijection between H and aH, so $|aH| = |H|$. $\square$

2.2 Lagrange's theorem and its corollaries

Theorem 2.6: Lagrange's theorem

Let G be a finite group, and $H \leq G$. Then, $|H|$ divides $|G|$.

Proof. By lemmas 2.3 and 2.4, there exist $a_1, \dots, a_k \in G$ such that G is a disjoint union of cosets: $G = a_1 H \cup \cdots \cup a_k H$. By lemma 2.5,

$$\begin{aligned} |G| &= |a_1 H| + \cdots + |a_k H| \\ &= |H| + \cdots + |H| \\ &= kH \end{aligned}$$

Therefore $|H|$ divides $|G|$. $\square$

Corollary 2.7

Let G be a finite group. Then,

(i) Let $H \leq G$. The index $|G : H| = \frac{|G|}{|H|}$.

(ii) Let $a \in G$. Then, $|a|$ divides $|G|$.

(iii) If $|G|$ is prime, then $G = \langle a \rangle$ for some $a \in G$.

(iv) Let $a \in G$. Then, $a^{|G|} = e$.

(v) **(Fermat's little theorem.)** Let $a \in \mathbb{Z}$, and p be prime. then, $a^p \equiv a \mod p$.

Proof.

(i) Follows immediately from proof of Lagrange's theorem.

(ii) We know $\langle a \rangle \leq G$. Since $|\langle a \rangle| = |a|$, the statement follows from Lagrange's theorem.

(iii) Let $a \in G$ with $a \neq e$. This is possible since $|G| \geq 2$. Then, $|a|$ divides $|G|$ by (ii). Since $a \neq e$ and $|G|$ is prime, $|a| = |G|$. So, since $|\langle a \rangle| = |G|$ and $\langle a \rangle \leq G$, we have $\langle a \rangle = G$.

(iv) By (ii) we have $k|a| = |G|$ for some $k \in \mathbb{Z}$. So,

$$\begin{aligned} a^{|G|} &= a^{k|a|} \\ &= (a^{|a|})^k \\ &= e^k \\ &= e \end{aligned}$$

(v) Let $a \in \mathbb{Z}$. Then, if $p|a$ then $p|a^p \implies a^p \equiv 0 \mod p$. If $p \nmid a$ then $\gcd(a, p) = 1$. So, $a \equiv n \mod p$ for some $n \in \mathbb{Z}_p^*$. Now, $|\mathbb{Z}_p^*| = p - 1$. By (iv) we have

$$\begin{aligned} n^{p-1} &\equiv 1 \mod p \\ n^p &\equiv n \mod p \\ a^p &\equiv a \mod p \end{aligned}$$

$\square$

3 Cyclic groups

Definition 3.1: Cyclic group

Let G be a group. G is <u>cyclic</u> if there exists $a \in G$ such that $\langle a \rangle = G$. a is then a <u>generator</u> of G.

Example 3.2: Some cyclic groups

- $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- $\mathbb{Z}_6$ is cyclic, since $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$.
- $\mathbb{Z}_9^*$ is cyclic, since $\mathbb{Z}_9^* = \langle 2 \rangle$.

Proposition 3.3: Cyclic groups are abelian

Let $G = \langle a \rangle$ be a cyclic group. Then G is abelian.

Proof. Let $a^n, a^m \in G$ where $n, m \in \mathbb{Z}$. Then,

$$\begin{aligned} a^n a^m &= a^{n+m} \\ &= a^m a^n \end{aligned}$$

□

Proposition 3.4: Subgroups of a cyclic group are cyclic

Let $G = \langle a \rangle$ be a cyclic group, and $H \leq G$. Then H is also cyclic.

Proof. If $G = \{e\}$, clearly $H = G$ so we're done. Thus assume $G \neq \{e\}$. So, $G = \langle a \rangle$ where $a \neq e$.

Let k be the smallest positive integer such that $a^k \in H$. Now, it is clear that $\langle a^k \rangle \subseteq H$ since H is a group. Let $a^n \in H$ for some integer n. By division algorithm, $n = qk + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < k$. So, $a^n = a^{kq+r} = (a^k)^q(a^r)$ which implies $(a^k)^{-q}a^n = a^r$. Since $a^k, a^n \in H$ we have $a^r \in H$. However, $r < k$ so $r = 0$, since k is the minimal positive integer such that $a^k \in H$. Therefore, $a^n = (a^k)^q$ so $H = \langle a^k \rangle$. □

Theorem 3.5: Criterion for $a^i = a^j$

Let G be a group with $a \in G$.

- If $|a| = \infty$, then $a^i = a^j \iff i = j$.
- If $|a| = n \in \mathbb{N}$, then
  (i) $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$
  (ii) $a^i = a^j \iff n | i - j$.

Proof.

- Suppose $a \in G$ such that $a^i = a^j$ and $|a| = \infty$. Then, $a^{i-j} = e$. However since $|a| = \infty$, we know $a^k \neq e$ for all $k \in \mathbb{N}$. So, $i - j = 0$ and $i = j$. Trivially, $i = j \implies a^i = a^j$.
- Suppose $a \in G$ and $|a| = n \in \mathbb{N}$.
  (i) We must prove that $\langle a \rangle \subseteq \{e, a, \dots, a^{n-1}\}$ (*) and $\{e, a, \dots, a^{n-1}\} \subseteq \langle a \rangle$ (**). (**) is trivial from definition of $\langle a \rangle$, so we will prove (*).

  Let $a^k \in \langle a \rangle$ for some $k \in \mathbb{N}$. If $k < n$ then clearly $a^k \in \{e, a, \dots, a^{n-1}\}$. Otherwise, there exists $q, r \in \mathbb{Z}$ such that $k = qn + r$ with $0 \leq r < n$, by division algorithm. So, we have

$$
\begin{aligned}
a^k &= a^{nq+r} \\
&= a^{nq} a^r \\
&= (a^n)^q a^r \\
&= e^q a^r \\
&= a^r
\end{aligned}
$$

  So since $0 \leq r < n$, we have $a^k \in \{e, a, \dots, a^{n-1}\}$ so (i) holds.

  (ii) ($\Longrightarrow$) We know $a^i = a^j \implies a^{i-j} = e$. By division algorithm, $i - j = nq + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. So,

$$
\begin{aligned}
i - j &= nq + r \\
a^{i-j} &= (a^n)^q a^r \\
e &= a^r
\end{aligned}
$$

  Since $|a| = n$, we know n is the smallest positive integer such that $a^n = e$, and we know $r < n$, therefore $r = 0$ and $i - j = nq$ for some $q \in \mathbb{Z}$.
  ($\Longleftarrow$) If $i - j = nq$ for some $q \in \mathbb{Z}$, then $a^{i-j} = (a^n)^q = e \implies a^i = a^j$.

$\square$

Corollary 3.6

Suppose $|a| = n$. Then, $a^k = e$ iff $n|k$.

Proof. $a^k = e \iff a^k = a^n \iff n|k$ by theorem 3.5 $\square$

Remark 3.7

Note that $a^k = e$ does not imply $k = |a|$. It does, however, imply $|a|$ divides k.

Theorem 3.8

Suppose G is a cyclic group, with $G = \langle a \rangle$ and $|G| = |a| = n$. If $k \in \mathbb{Z}$, then

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $|\langle a^k \rangle| = \frac{n}{\gcd(n,k)}$

Proof.

(i) Let $d = \gcd(n,k)$. We want to prove $\langle a^k \rangle = \langle a^d \rangle$, and thus $\langle a^k \rangle \subseteq \langle a^d \rangle$ (*) and $\langle a^d \rangle \subseteq \langle a^k \rangle$ (**). By definition of gcd, we know $k = rd$ for some $r \in \mathbb{Z}$. Then,

$$\begin{aligned} a^k &= a^{rd} \\ &= (a^d)^r \in \langle a^d \rangle \end{aligned}$$

so (*) holds. To prove (**), it is enough to show $a^d \in \langle a^k \rangle$ since $d|k$. By Bézout's identity, there exist $s, t \in \mathbb{Z}$ such that $d = ns + kt$. So,

$$\begin{aligned} a^d &= a^{ns+kt} \\ &= a^{ns}a^{kt} \\ &= (a^n)^s(a^k)^t \\ &= (a^k)^t \end{aligned}$$

Thus (**) holds and $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

(ii) We want to prove $|a^d| = \frac{n}{d}$. Clearly $(a^d)^{\frac{n}{d}} = a^n = e$, so $|a^d| \leq \frac{n}{d}$. For contradiction suppose $|a^d| = \alpha < \frac{n}{d}$. Then,

$$\begin{aligned} (a^d)^\alpha &= e \\ a^{d\alpha} &= e \\ \alpha &< \frac{n}{d} \\ d\alpha &< n \end{aligned}$$

But this contradicts $|a| = n$ so (ii) holds.

$\square$

Example 3.9

Suppose $G = \langle a \rangle$ and $|a| = 30$. What is $\langle a^{26} \rangle$?

$$\begin{aligned} \langle a^{26} \rangle &= \langle a^{\gcd(26,30)} \rangle \\ &= \langle a^2 \rangle \end{aligned}$$

What about $\langle a^{23} \rangle$?

$$\begin{aligned} \langle a^{23} \rangle &= \langle a^{\gcd(23,30)} \rangle \\ &= \langle a \rangle \end{aligned}$$

Also, $|\langle a^{26} \rangle| = \frac{30}{2} = 15$.

Corollary 3.10

$\mathbb{Z}_n$ is a cyclic group of order n, and $i \in \mathbb{Z}_n$ generates $\mathbb{Z}_n \iff \gcd(i, n) = 1$.

Proof. $(\Rightarrow)$ Suppose $\mathbb{Z}_n = \langle i \rangle$. Then, $|\langle i \rangle| = n$. By theorem 3.8 this implies $\gcd(n, i) = 1$.
$(\Leftarrow)$ Suppose $\gcd(n, i) = 1$. By theorem 3.8 $|\langle i \rangle| = n$ so $\mathbb{Z}_n = \langle i \rangle$. $\square$

Theorem 3.11: Fundamental theorem of cyclic groups

Let G be a finite cyclic group with $G = \langle a \rangle$ and $|G| = n$. Then,

1. Every subgroup of G is cyclic.
2. If $H \leq G$ then $|H|$ divides $|G|$.
3. If k is a divisor of n then there is a unique subgroup $H \leq G$ such that $|H| = k$ and $H = \langle a^{\frac{n}{k}} \rangle$.

Proof.

1. Proposition 3.4
2. Lagrange's theorem 2.6
3. Suppose k divides n. We need to prove there is a subgroup $H \leq G$ with $|H| = k$ (i) and that H is the unique such subgroup (ii).
   (i) Consider $H = \langle a^{\frac{n}{k}} \rangle$. From theorem 3.8, $|H| = |\langle a^{\frac{n}{k}} \rangle| = \frac{n}{\gcd(n, \frac{n}{k})}$. Since $\frac{n}{k}|n$, we have $\gcd(n, \frac{n}{k}) = \frac{n}{k}$. So, $|H| = \frac{n}{(n/k)} = k$.
   (ii) Suppose $P \leq G$ with $|P| = k$. From proposition 3.4, $P = \langle a^m \rangle$ for some $m \in \mathbb{N}$. By theorem 3.8, $P = \langle a^{\gcd(n,m)} \rangle$. Since $|P| = k$ we have $\frac{n}{k} = \gcd(n, m)$ so $P = \langle a^{\frac{n}{k}} \rangle = H$.

$\square$

Example 3.12: Subgroups of $\mathbb{Z}_12$

We know $\mathbb{Z}_{12} = \langle 1 \rangle$ and $|\mathbb{Z}_{12}| = 12$. Here are the subgroups of $\mathbb{Z}_{12}$.

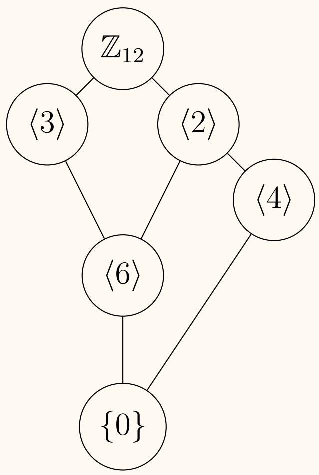
Order	Subgroup
1	$\langle 1^{12} \rangle = \{0\}$
2	$\langle 1^6 \rangle = \{0, 6\}$
3	$\langle 1^4 \rangle = \{0, 4, 8\}$
4	$\langle 1^3 \rangle = \{0, 3, 6, 9\}$
6	$\langle 1^2 \rangle = \{0, 2, 4, 6, 8, 10\}$
12	$\langle 1^1 \rangle = \mathbb{Z}_{12}$

4 Subgroup lattices

Definition 4.1: Subgroup lattice

Let G be a group. A subgroup lattice is an illustration which describes all relationships between subgroups of G. All subgroups of G are drawn, and is connected to each subgroup of it.

Example 4.2: Subgroup lattice of $\mathbb{Z}_{12}$



5 Permutation groups

Definition 5.1: Permutation group

Let $B = \{1, \dots, n\}$. A permutation of B is a bijection from B to itself. That is to say, a function $\sigma : B \to B$ which is one-to-one and onto.
Let $n \in \mathbb{N}$. Then, S_n is the permutation group of order n, the set of all permutations on $\{1, \dots, n\}$ with the operation being function composition.
Elements σ of S_n can be denoted $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Remark 5.2: Order of S_n

- What is $|S_n|$? Let $\sigma \in S_n$. There are n possibilities for $\sigma(1)$. Given $\sigma(1)$, there are $n-1$ possibilities for $\sigma(2)$, and so on. Thus, $|S_n| = n(n-1)(n-2)\dots 1 = n!$.
- S_n is a non-abelian group. (Prove this!)

5.1 Cycle notation

Definition 5.3: Cycles and transpositions

An expression of the form $(a_1 \dots a_m)$ is a cycle length m, and if $m = 2$, a transposition. For some $\sigma \in S_n$ we denote $\sigma = (a_1 \dots a_m)$ to mean $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_m) = a_1$.

Example 5.4: Cycle notation for elements of S_3

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then, $\sigma = (12)(3)$ since $\sigma(1) = 2$ and $\sigma(2) = 1$ and $\sigma(3) = 3$.
Let $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Then, $\beta = (132) = (321) = (213)$.

Example 5.5: Cycle notation for an element of S_6

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$. Then, $\sigma = (136)(24) = (24)(136)$.

Theorem 5.6: Permutations are products of disjoint cycles

Let $\sigma \in S_n$. Then, σ can be written as a cycle or a product of disjoint cycles.

Proof. If σ is a cycle we're done, so suppose it's not. Then, let $a_1 \in \{1, \dots, n\}$ and $a_2 = \sigma(a_1), \dots, a_k = \sigma(a_{k-1}), a_1 = \sigma(a_k)$. This is always possible since $\{1, \dots, n\}$ is a finite set. Let $b_1 \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ and $b_2 = \sigma(b_1), \dots, b_m = \sigma(b_{m-1}), b_1 = \sigma(b_m)$. We claim the cycles $(a_1 \dots a_k)$ and $(b_1 \dots b_m)$ are disjoint.
For contradiction suppose $a_i = b_j$ for some i, j. Then,

$$\begin{aligned} \sigma^{i-1}(a_1) &= \sigma^{j-1}(b_j) \\ b_1 &= \sigma^{j-1-i+1}(a_1) \in \{a_1, \dots, a_k\} \end{aligned}$$

which is impossible since $b_1 \notin \{a_1, \dots, a_k\}$.
Since $\{1, \dots, n\}$ is finite, this process stops eventually, and gives a representation of σ as a product of disjoint cycles. $\square$

Example 5.7

Let $\tau = (124)$, $\sigma = (1235)$. What are $\tau\sigma$ and $\sigma\tau$ as a product of disjoint cycles?

$$\begin{aligned} \tau\sigma &= (124)(1235) = (14)(235) \\ \sigma\tau &= (135)(24) \end{aligned}$$

Remark 5.8: Aside

If $m \leq n$ then S_m is "isomorphic" to a subgroup of S_n. Section 8 introduces what it means for groups to be isomorphic.

It is not technically true that $S_m \leq S_n$ because the elements of S_m and elements of S_n are functions on different sets so S_m is not a subset of S_n.

Theorem 5.9: Disjoint cycles commute

Let $\sigma = (a_1 \dots a_k)$, $\tau = (b_1 \dots b_l)$ be disjoint cycles. Then $\sigma\tau = \tau\sigma$.

Proof. We know $\{1, \dots, n\} = \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\} \cup \{c_1, \dots, c_m\}$
where $\{c_1, \dots, c_m\} = \{1, \dots, n\} \setminus (\{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\})$. So,

- For all $i \in \{1, \dots, k\}$, we have $\tau(\sigma(a_i)) = \tau(a_{i+1}) = a_{i+1} = \sigma(a_i) = \sigma(\tau(a_i))$ since $\tau(a_i) = a_i$.
- For all $i \in \{1, \dots, l\}$, we have $\sigma(\tau(b_i)) = \sigma(b_{i+1}) = b_{i+1} = \tau(b_i) = \tau(\sigma(b_i))$ since $\sigma(b_i) = b_i$.
- For all $i \in \{1, \dots, m\}$, we have $\sigma(\tau(c_i)) = \sigma(c_i) = c_i = \tau(c_i) = \tau(\sigma(c_i))$ since $\sigma(c_i)\tau(c_i) = c_i$.

Therefore in all cases, $\sigma\tau = \tau\sigma$. $\square$

Remark 5.10

Let σ be a k-cycle. Then $|\sigma| = k$.

Theorem 5.11: Order of a permutation

Let $\alpha \in S_n$. Then $|\alpha|$ is the least common multiple of the lengths of the disjoint cycles representing α.

Proof. Let $\sigma, \tau \in S_n$ be disjoint cycles, with σ being an m-cycle and τ being a k-cycle. Let $l = \text{lcm}(k, m)$. We claim $|\sigma\tau| = l$. Let $n = |\sigma\tau|$.
Since $l = \text{lcm}(k, m)$, we have $k|l$ and $m|l$. So,

$$\begin{aligned}(\sigma\tau)^l &= \sigma^l \tau^l \\ &= (\sigma^m)^t (\tau^k)^s\end{aligned}$$

for some $s, t \in \mathbb{Z}$. Thus,

$$\begin{aligned}\tau^k &= e = \sigma^m \\ (\sigma\tau)^l &= e\end{aligned}$$

so $n \leq l$. Now, suppose $(\sigma\tau)^a = e$ for some $a \in \mathbb{Z}$. Then,

$$a = q_1 m + r_1 = q_2 k + r_2$$

for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1 < m$, $0 \leq r_2 < k$. So,

$$\begin{aligned}e = (\sigma\tau)^a &= \sigma^a \tau^a \\ &= (\sigma^m)^{q_1} \sigma^{r_1} (\tau^k)^{q_2} \tau^{r_2} \\ &= \sigma^{r_1} \tau^{r_2} \\ \sigma^{-r_1} &= \tau^{r_2}\end{aligned}$$

But since σ and τ are disjoint, the only way this can happen is if $\sigma^{-r_1} = \tau^{r_2} = e$. But $r_2 < k$ so r_2 must be 0. Similarly, $r_1 = 0$ as well. So, any integer a such that $e = (\sigma\tau)^a$ is a multiple of both k and m, and l is the least such multiple by definition. Thus $|\sigma\tau| = l$. $\square$

Example 5.12

Find number of elements of order 3 in S_7.
Suppose $\sigma \in S_7$ such that $|\sigma| = 3$. So, $\sigma = (a_1 a_2 a_3)$ or $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6)$ where $a_i \neq a_j$ for all $i \neq j$. Thus, there are $\binom{7}{3} + \binom{7}{3}\binom{4}{3}$ such elements.

5.2 Transpositions and A_n

Remark 5.13

Recall that transpositions are 2-cycles. They are special because they generate S_n.

Example 5.14

Consider $(1234) \in S_n$. Now, $(1234) = (14)(13)(12)$.

Theorem 5.15

Let $\sigma = (a_1 \dots a_m)$ be a cycle of length $m \geq 2$. Then m can be written as a product of transpositions.

Proof. Only a proof sketch is given.

$$(a_1 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_2)$$

□

Corollary 5.16

Let $\sigma \in S_n$. Then σ can be written as a product of transpositions.

Proof. Directly follows from theorems 5.6 and 5.15. □

Example 5.17

Consider $(123) \in S_4$.

$$\begin{aligned}(123) &= (13)(12)\\ &= (13)(24)(13)(24)(13)(12)\end{aligned}$$

Lemma 5.18

Let e be the identity in S_n. If $e = \beta_1 \dots \beta_k$ for transpositions $\beta_1, \dots, \beta_k$, then k is even.

Proof. Shamelessly stolen from the textbook.

Clearly, $r \neq 1$, since a 2-cycle is not the identity. If $r = 2$, we are done. So, we suppose that $r > 2$, and we proceed by induction. Suppose that the rightmost 2-cycle is (ab). Then, since $(ij) = (ji)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right:

$$\begin{aligned} \varepsilon &= (ab)(ab), \\ (ab)(bc) &= (ac)(ab), \\ (ac)(cb) &= (bc)(ab), \\ (ab)(cd) &= (cd)(ab). \end{aligned}$$

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\varepsilon = \beta_1\beta_2 \cdots \beta_{r-2}$, and therefore, by the Second Principle of Mathematical Induction, $r - 2$ is even. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart on the left to obtain a new product of r 2-cycles that is still the identity, but where the rightmost occurrence of the integer a is in the second-from-the-rightmost 2-cycle of the product instead of the rightmost 2-cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r - 2)$ 2-cycles equal to the identity or a new product of r 2-cycles, where the rightmost occurrence of a is in the third 2-cycle from the right. Continuing this process, we must obtain a product of $(r - 2)$ 2-cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurrence of the integer a is in the leftmost 2-cycle, and such a product does not fix a, whereas the identity does. Hence, by the Second Principle of Mathematical Induction, $r - 2$ is even, and r is even as well. □

Theorem 5.19

Let $\sigma \in S_n$. If $\sigma = \beta_1 \dots \beta_m = \gamma_1 \dots \gamma_k$ for transpositions $\beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_k$, then $m \equiv k \mod 2$.

Proof. Let $\beta_i = (a_i b_i)$ and $\gamma = (c_j d_j)$ for $i = 1 \dots m$, $j = 1 \dots k$. Then,

$$\begin{aligned} \sigma &= (a_1 b_1) \dots (a_m b_m) = (c_1 d_1) \dots (c_k d_k) \\ \sigma\sigma^{-1} = e &= (c_1 d_1) \dots (c_k d_k)(a_m b_m)^{-1} \dots (a_1 b_1)^{-1} \\ &= (c_1 d_1) \dots (c_k d_k)(a_m b_m) \dots (a_1 b_1) \end{aligned}$$

Thus by Lemma 5.18 we know $k + m$ is even, so k and m must have the same parity. □

Definition 5.20: Even and Odd permutations

Let $\sigma \in S_n$. If σ is a product of an even number of permutations, then σ is even. Otherwise σ is odd.

We define $A_n := \{\sigma \in S_n : \sigma \text{ is even}\}$, and this is called the alternating group of order n.

Example 5.21

In S_3 $e, (123), (132)$ are even while $(12), (13), (23)$ are odd.

Theorem 5.22: Alternating groups are groups

$A_n \leq S_n$.

Proof. We know $e \in A_n$ so $A_n \neq \emptyset$. Let $\sigma, \tau \in A_n$. Then,

$$\sigma = \sigma_1 \dots \sigma_{2n}$$
$$\tau = \tau_1 \dots \tau_{2k}$$

for integers k, n and transpositions $\sigma_1, \dots, \sigma_{2n}, \tau_1, \dots, \tau_{2k}$. So, $\sigma\tau^{-1} = \sigma_1 \dots \sigma_{2n}\tau_{2k} \dots \tau_{2k}$ is even since it is the product of $2k + 2n = 2(k + n)$ transpositions. Hence $A_n \leq S_n$ by one-step-test. $\square$

6 Normal subgroups

6.1 Introduction

Remark 6.1

Let G be a group, and $H \leq G$. We know given $a \in G$, the left coset aH does not always equal the right coset Ha. Subgroups whose left cosets are equal to their right cosets are given a special name.

Definition 6.2: Normal subgroup

Let G be a group, and $H \leq G$. H is normal if for all $a \in G$ we have $aH = Ha$. We denote this by $H \lhd G$.

Remark 6.3

If $H \lhd G$, we have $ah = h'a$ for all $a \in G$ and $h, h' \in H$. However ah is not necessarily equal to ha.

Theorem 6.4

Let G be a group, and $H \leq G$. Then $H \lhd G$ iff for all $a \in G$, $aHa^{-1} \subseteq H$.

Proof. ($\Longrightarrow$) Suppose $H \lhd G$. Let $a \in G$. Then

$$\begin{aligned} aHa^{-1} &= Haa^{-1} \\ &= He \\ &= H \subseteq H \end{aligned}$$

($\Longleftarrow$) Suppose for all $a \in G$, $aHa^{-1} \subseteq H$. Then,

$$aH \subseteq Ha$$

by right cancellation. Also since $a^{-1} \in G$, we have $a^{-1}Ha \subseteq H$ so

$$Ha \subseteq H$$

Thus $aH = Ha$ and by definition $H \lhd G$. □

Example 6.5: Abelian groups have only normal subgroups

Let G be abelian. Then, all subgroups of G are normal.

Proof. Let $H \leq G$. Then for all $a \in G$ and $h \in H$, $ah = ha$, so $aH = Ha$. □

Example 6.6: Center of group is normal

$Z(G) \lhd G$.

Proof. Let $a \in G$. Then, $aZ(G)a^{-1} = aa^{-1}Z(G) = Z(G) \subseteq Z(G)$. □

Example 6.7: Alternating group is normal subgroup of symmetric group

$A_n \lhd S_n$.

Proof. Let $\sigma = \sigma_1 \dots \sigma_k \in S_n$, $\alpha = \alpha_1 \dots \alpha_{2q} \in A_n$ where $n, k, q \in \mathbb{Z}$ and $\sigma_1, \dots, \sigma_k$, $\alpha_1, \dots, \alpha_{2q}$ are transpositions. Then, $\sigma\alpha\sigma^{-1}$ is a product of $k + 2q + k$ transpositions, which is an even number. □

Example 6.8

Consider $3\mathbb{Z} \leq \mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $3\mathbb{Z} \lhd \mathbb{Z}$. Consider the cosets of $3\mathbb{Z}$ in $\mathbb{Z}$.

$$\begin{aligned}
0 + 3\mathbb{Z} &= \{\dots, -3, 0, 3, \dots\} \\
1 + 3\mathbb{Z} &= \{\dots, -2, 1, 4, \dots\} \\
2 + 3\mathbb{Z} &= \{\dots, -1, 2, 5, \dots\}
\end{aligned}$$

Let $F = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$. Define $(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z}$ where $a, b \in \mathbb{Z}_3$. Note that F "looks like" $\mathbb{Z}_3$.

6.2 Quotient groups

Theorem 6.9: Quotient groups are groups

Let G be a group, and $H \leq G$. Then, $H \lhd G$ iff $G/H := \{gH : g \in G\}$ is a group under operation $(aH)(bH) := (ab)H$ for $a, b \in G$.
The group G/H is called the quotient group of G by H, or factor group.

Proof. ($\Longrightarrow$) Suppose $H \lhd G$. First, check the operation is well-defined. We need to show if $aH = a'H$ and $bH = b'H$ for some $a, a', b, b' \in G$ then $(aH)(bH) = (ab)H = (a'b')H = (a'H)(b'H)$.

$$\begin{aligned}
(aH)(bH) &= (ab)H \\
&= a(bH) \\
&= a(b'H) \\
&= a(Hb') \\
&= (aH)b' \\
&= (a'H)b' \\
&= a'(Hb') \\
&= a'b'H \\
&= (a'H)(b'H)
\end{aligned}$$

Thus, $(aH)(bH) = (a'h_1H)(b'h_2H) = (a'H)(b'H)$ so the operation is well-defined.

(Identity.) $eH = H$ is the identity element since $(eH)(gH) = gH = (gH)(eH)$ for all $g \in G$.

(Inverses.) Let $a \in G$. Then, $(aH)(a^{-1}H) = eH = (a^{-1}H)(aH)$.

(Closure.) Follows from closure of G.

(Associativity.) Follows from associativity of G.
So G/H is a group.
($\Longleftarrow$) Suppose G/H is a group, and therefore its operation is well-defined. Let $g \in G$. It will be shown that $gHg^{-1} \subseteq H$.
Let $h \in H$. Then,

$$\begin{aligned}
g^{-1}H &= (eg^{-1})H \\
&= eHg^{-1}H \\
&= hHg^{-1}H \\
&= (hg^{-1})H \\
H &= (ghg^{-1})H
\end{aligned}$$

Therefore $ghg^{-1} \in H$ and hence $gHg^{-1} \subseteq H$ so $H \lhd G$. $\square$

Remark 6.10: Aside

For this operation to be well defined it is not sufficient to show if $aH = a'H$ and $bH = b'H$ then $(aH)(bH) = (a'H)(b'H)$. One also needs to show $(ab)H = (a'b')H$. These notes present a correct proof.

Corollary 6.11

Let G be a group, and $H \lhd G$. Then, $|G/H| = |G : H| = \frac{|G|}{|H|}$.

Example 6.12

$|\mathbb{Z}_{10}/\langle 6\rangle| = \frac{|\mathbb{Z}_{10}|}{|\langle 6\rangle|} = \frac{10}{5} = 2$
We can therefore deduce that $\mathbb{Z}_{10}/\langle 6\rangle = \{\langle 6\rangle, 1 + \langle 6\rangle\}$

Theorem 6.13: G/Z theorem

Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Let $x, y \in G$. Since $G/Z(G)$ is cyclic, we have $\langle [a]\rangle := \langle aZ(G)\rangle = G/Z(G)$ for some $a \in G$. So,

$$\begin{aligned} xZ(G) &= a^m Z(G) \\ yZ(G) &= a^n Z(G) \end{aligned}$$

for some $m, n \in \mathbb{Z}$. Therefore for some $z_1, z_1', z_2, z_2' \in Z(G)$ we have

$$\begin{aligned} xz_1 &= a^m z_1' \\ x &= a^m z_1' z_1^{-1} \end{aligned}$$

So $x = a^m z_x$ for some $z_x \in Z(G)$. Similarly $y = a^n z_y$ for some $z_y \in Z(G)$. Thus,

$$\begin{aligned} xy &= a^m z_x a^n z_y \\ &= z_x a^{m+n} z_y \\ &= z_x a^n a^m z_y \\ &= a^n z_y a^m z_x \\ &= yx \end{aligned}$$

since z_x, z_y commute with all elements of G. Therefore G is abelian. $\square$

Theorem 6.14: Cauchy's theorem for abelian groups

Let G be a finite abelian group, with $|G| = n$. If p is a prime number which is a factor of n, then there exists $H \leq G$ such that $|H| = p$.

Proof. (The general, non-abelian case is proven in theorem 8.19.)
By strong induction on n.

Base case: The statement is trivially true for the groups of order 1 and 2.

Inductive step: Suppose the statement is true for all groups of order less than n. Let $g \in G$ such that $g \neq e$ and let $|g| = m = qs$ for some $q, s \in \mathbb{Z}$ with q prime. Let $a = g^s$. So, $|a| = q$.

If $q = p$ then $\langle a \rangle \leq G$ with $|\langle a \rangle| = p$ so we're done.

Since G is assumed to be abelian, we know $\langle a \rangle \lhd G$. Then, $|G/\langle a \rangle| = \frac{n}{q}$. We also know $\frac{n}{q} < n$ and p is a factor of $\frac{n}{q}$. Therefore by inductive hypothesis, $G/\langle a \rangle$ has a subgroup H such that $|H| = p$. So, H is cyclic: there exists $y \in G$ such that $H = \langle [y] \rangle$ where $[y] = y\langle a \rangle$.

We know that $[y]^p = [e] = \langle a \rangle$. Therefore $y^p \in \langle a \rangle$. So $y^p = a^k$ for some $k \in \mathbb{Z}$, and

$$\begin{aligned} y^{pq} &= a^{kq} \\ &= (a^q)^k \\ &= e \end{aligned}$$

Thus the possible orders of y are $1, p, q, pq$ by Lagrange's theorem.

- If $|y| = 1$ then H is a trivial subgroup, which contradicts $|H| = p$, so this is impossible.
- If $|y| = p$ then $|\langle y \rangle| = p$ as desired.
- If $|y| = q$ then $[y]^q = y^q H = eH = H = [y]^p$ since $|[y]| = p$. So, p is a proper factor of q, which contradicts p and q being prime.
- If $|y| = pq$ then $|y^q| = p$ so $|\langle y^q \rangle| = p$ as desired.

□

7 Isomorphisms and homomorphisms

7.1 Isomorphisms

Remark 7.1: $\mathbb{Z}_2$ and $\mathbb{Z}_6^*$ have the same structure

Consider the Cayley tables of the groups $\mathbb{Z}_2$ and $\mathbb{Z}_6^*$.

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	5
1	1	5
5	5	1

Clearly, one can simply relabel the elements of one group as follows, and obtain the other group: $0 \leftrightarrow 1, 1 \leftrightarrow 5$.

Definition 7.2: Isomorphism

Let G, G' be groups. Then a function $\phi : G \to G'$ is an <u>isomorphism</u> if:

1. ϕ is one-to-one.
2. ϕ is onto.
3. ϕ preserves group operation. That is, for all $a, b \in G$ we have $\phi(ab) = \phi(a)\phi(b)$.

If there exists an isomorphism between G and G' then we say G is <u>isomorphic to</u> G', with notation $G \cong G'$. If G is not isomorphic to G' we say $G \ncong G'$.

Remark 7.3

Isomorphisms represent "equality" of groups up to relabelling the elements.

Example 7.4

All infinite cyclic groups are isomorphic to $\mathbb{Z}$.

Proof. Let $G = \langle a \rangle$ be an infinite cyclic group. So, for all $g \in G$ we have $g = a^k$ for some $k \in \mathbb{Z}$. Define $\phi : G \to \mathbb{Z}$ by $\phi(a^n) = n$. Then,

(One-to-one.) Suppose $\phi(g) = \phi(g')$ for $g, g' \in G$. Therefore, $g = a^m, g' = a^{m'}$ for $m, m' \in \mathbb{Z}$. Thus,

$$\begin{aligned} \phi(a^m) &= \phi(a^{m'}) \\ m &= m' \\ a^m &= a^{m'} \\ g &= g' \end{aligned}$$

So ϕ is one-to-one.

(Onto.) Let $n \in \mathbb{Z}$. Then $\phi(a^n) = n$ so ϕ is onto.

(Preserves group operation.) We have $\phi(gg') = \phi(a^m a^{m'}) = \phi(a^{m+m'}) = m + m'$ so ϕ preserves group operation. $\square$

Example 7.5

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

Proof. Let $G = \langle a \rangle$. Then, for all $g \in G$ we have $g = a^k$ for some $k \in \mathbb{Z}$. Define $\phi : G \to \mathbb{Z}_n$ by $\phi(g) = \phi(a^k) = k$. We can show ϕ is an isomorphism by an argument similar to that in the previous example. $\square$

Theorem 7.6: Properties of isomorphisms

Let $\phi : G \to H$ be an isomorphism of groups G, H. Let $e_G \in G, e_H \in H$ be the identities of G and H respectively. Then,

1. $\phi(e_G) = e_H$
2. For any $n \in \mathbb{Z}$, we have $\phi(a^n) = (\phi(a))^n$ where $a \in G$.
3. If $G = \langle a \rangle$ then $H = \langle \phi(a) \rangle$.
4. For all $a \in G$ we have $|a| = |\phi(a)|$.
5. If G is finite then $|G| = |H|$.

Proof.

1. We have $\phi(e_G)\phi(g) = \phi(e_G g) = \phi(g)$ for all $g \in G$. Therefore $\phi(e_G)$ must be the identity element.
2. Follows by induction on n since ϕ preserves group operations.
3. Follows from (2).
4. Follows from (2).
5. Follows from ϕ being a bijection.

□

Example 7.7: Non-example of isomorphism

Let G be a group and $g \in G$. Define $\phi_g : G \to G$ by $\phi_g(x) = gx$ for all $x \in G$. Then ϕ_g is a bijection, but not necessarily an isomorphism, since $\phi_G(xy) = gxy \neq gxgy$ in general.

Theorem 7.8: Cayley's theorem

Let G be a group. Then G is isomorphic to a group of permutations.

Proof. Define $\overline{G} := \{\phi_g : g \in G\}$. First it will be shown that $\overline{G}$ is a group under the operation of composition. Note that $\overline{G}$ is a set of bijections of G.

(Closure.) Let $\phi_{g_1}, \phi_{g_2} \in \overline{G}$. Then $(\phi_{g_1} \circ \phi_{g_2})(x) = \phi_{g_1}(\phi_{g_2}(x)) = g_1g_2x = \phi_{g_1g_2}$ for all $x \in G$ so $\overline{G}$ is closed under composition.

(Associativity.) Let $\phi_{g_1}, \phi_{g_2}, \phi_{g_3} \in \overline{G}$. Then, $(\phi_{g_1} \circ \phi_{g_2}) \circ \phi_{g_3}(x) = \phi_{g_1}(\phi_{g_2}(\phi_{g_3}(x))) = \phi_{g_1} \circ (\phi_{g_2} \circ \phi_{g_3})(x)$ for all $x \in G$ so composition is associative.

(Identity.) $(\phi_e \circ \phi_g)(x) = \phi_e(\phi_g(x)) = egx = gx = gex = \phi_g(\phi_e(x)) = (\phi_g \circ \phi_e)(x)$ for all $g, x \in G$. Therefore ϕ_e, the identity mapping, is the identity element in $\overline{G}$.

(Inverses.) For all $\phi_g \in \overline{G}$ we have $(\phi_{g^{-1}} \circ \phi_g)(x) = gg^{-1}x = x = g^{-1}gx = (\phi_g \circ \phi_{g^{-1}})(x)$ so all elements of $\overline{G}$ have an inverse.

So $\overline{G}$ is a group. Now it will be shown that $G \cong \overline{G}$. Define $\psi : \overline{G} \to G$ by $\psi(\phi_g) = g$.

(One-to-one.) Let $\phi_{g_1}, \phi_{g_2} \in \overline{G}$ such that $\psi(\phi_{g_1}) = \psi(\phi_{g_2})$. Then by definition $g_1 = g_2$ so $\phi_{g_1} = \phi_{g_2}$. Hence ψ is one-to-one.

(Onto.) Let $g \in G$. Then $\psi(\phi_g) = g$ so ψ is onto.

(Preserves group operation.) Let $\phi_{g_1}, \phi_{g_2} \in \overline{G}$ and $x \in G$. Then

$$\begin{aligned}\psi(\phi_{g_1} \circ \phi_{g_2})x &= g_1g_2x \\ &= \psi(\phi_{g_1})\psi(\phi_{g_2})x\end{aligned}$$

Therefore $G \cong \overline{G}$. □

7.2 Homomorphisms

Definition 7.9: Homomorphism

Let G, H be groups. A map $\phi : G \to H$ is a <u>homomorphism</u> if ϕ preserves the group operation. That is, if

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2)$$

for all $g_1, g_2 \in G$.

Example 7.10

Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(k) = k \mod n$. Let $k, l \in \mathbb{Z}$. Then,

$$\begin{aligned}\phi(k+l) &= k + l \mod n \\ &= k \mod n + l \mod n \\ &= \phi(k) + \phi(l)\end{aligned}$$

so ϕ is a homomorphism.

Example 7.11: Trivial homomorphism

Define $\phi : G \to H$ by $\phi(g) = e$ for all $g \in G$. Then G is a homomorphism.

This shows there is a homomorphism between any groups G and H, so it makes no sense to call two groups "homomorphic".

Example 7.12

Recall, $\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$ with multiplication is a group. Now, $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ defined by $x \mapsto |x|$ is a homomorphism since $|xy| = |x||y|$ for all $x, y \in \mathbb{R}^*$.

Example 7.13

Recall the set of invertible real matrices of size n, $GL_n(\mathbb{R})$. Now, $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det(A)$ is a homomorphism, since $\det(AB) = \det(A)\det(B)$ for all $A, B \in GL_n(\mathbb{R})$.

Example 7.14: Non-example of a homomorphism

Consider $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $x \mapsto x^2$. This is not a homomorphism since $\phi(1+1) = 4 \neq 2 = \phi(1) + \phi(1)$.

Example 7.15

Define $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2$ by $x \mapsto x^2$. This is a homomorphism because

$$\begin{aligned}\varphi(x+y) &= x^2 + 2xy + y^2 \\ &= x^2 + y^2 \\ &= \varphi(x) + \varphi(y)\end{aligned}$$

since $2xy = 0$ for all $x, y \in \mathbb{Z}_2$.

Definition 7.16: Kernel and Image

Let $\varphi : G \to H$ be a homomorphism between groups G, H.
The kernel of φ is $\ker \varphi := \{g \in G : \varphi(g) = e\}$ where e is the identity in H.
The image of φ is $\text{Im } \varphi := \{\varphi(g) : g \in G\}$.

Example 7.17

If φ is the trivial homomorphism then $\ker \varphi = G$ and $\text{Im } \varphi = \{e\}$.

Example 7.18

If $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ is defined by $\varphi(k) = k \mod n$ then $\ker \varphi = n\mathbb{Z}$ and $\text{Im } \varphi = Z_n$.

Example 7.19

If $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ is defined by $\varphi(x) = |x|$ then $\ker \varphi = \{-1, 1\}$ and
$\text{Im } \varphi = \{x \in \mathbb{R} : x > 0\} =: \mathbb{R}^+$.

Example 7.20

If $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is defined by $\varphi(A) = \det(A)$, then $\ker \varphi = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$ and $\text{Im } \varphi = \mathbb{R}^*$.

Theorem 7.21

Let $\varphi : G \to H$ be a homomorphism from G to H. Then:

1. $\varphi(e_G) = e_H$ where e_G, e_H are the identity elements in G and H respectively.
2. For all $a \in G$ we have $\varphi(a^{-1}) = \varphi(a)^{-1}$.
3. $\text{Im } \varphi \leq H$
4. $\ker \varphi \leq G$
5. $\ker \varphi \lhd G$

Proof.

1. Let $g \in G$. Then $\varphi(g) = \varphi(e_G g) = \varphi(e_G)\varphi(g)$ so $\varphi(e_G)$ must be the identity in H.
2. We have $\varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = e_H$ so $\varphi(a^{-1}) = \varphi(a)^{-1}$.
3. Notice $\text{Im } \varphi \neq \emptyset$ since $e_H \in \text{Im } \varphi$. Let $a, b \in \text{Im } \varphi$. Then $\varphi(g_1) = a$ and $\varphi(g_2) = b$ for some $g_1, g_2 \in G$. So,

$$\begin{aligned} ab^{-1} &= \varphi(g_1)\varphi(g_2)^{-1} \\ &= \varphi(g_1)\varphi(g_2^{-1}) \\ &= \varphi(g_1 g_2^{-1}) \end{aligned}$$

   Since $g_1 g_2^{-1} \in G$ we have $ab^{-1} \in \text{Im } \varphi$ so by one-step test, $\text{Im } \varphi \leq H$.

4. Notice $\ker \varphi \neq \emptyset$ since $\varphi(e_G) = e_H$ so $e_G \in \ker \varphi$. Let $a, b \in \ker \varphi$. Then,

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= e_H e_H^{-1} \\ &= e_H \end{aligned}$$

   Therefore, $ab^{-1} \in \ker \varphi$ so by one-step test, $\ker \varphi \leq G$.

5. It will be shown that for all $a \in G$ we have $a(\ker \varphi)a^{-1} \subseteq \ker \varphi$. Let $a \in G$, $g \in \ker \varphi$. Then,

$$\begin{aligned} \varphi(aga^{-1}) &= \varphi(a)\varphi(g)\varphi(a^{-1}) \\ &= \varphi(a)e_H\varphi(a)^{-1} \\ &= e_H \end{aligned}$$

   Therefore $a(\ker \varphi)a^{-1} \subseteq \ker \varphi$ so $\ker \varphi \lhd G$.

$\square$

7.3 Automorphisms

Definition 7.22: Automorphism

Let G be a group. An isomorphism $\varphi : G \to G$ is called an automorphism and the set of automorphisms of G is denoted $Aut(G)$.
A mapping $\phi_a : G \to G$ defined by $g \mapsto aga^{-1}$ for some $a \in G$ is called an inner automorphism and the set of inner automorphisms of G is denoted $Inn(G)$.

Example 7.23: Identity automorphism

For any groups G the identity mapping $id : G \to G$ defined by $g \mapsto g$ is an automorphism.

Example 7.24: Conjugation automorphism

The mapping $\varphi : \mathbb{C} \to \mathbb{C}$ defined by $a + bi \mapsto a - bi$ is an automorphism on $\mathbb{C}$.

Theorem 7.25

Let G be a group.

1. $Aut(G)$ is a group under composition.
2. $Inn(G) \leq Aut(G)$
3. $Inn(G) \lhd Aut(G)$

Remark 7.26

In $Aut(G)$ the identity is the identity mapping and the inverse of an element is the element's inverse function (which exists since all elements of $Aut(G)$ are bijections).

Example 7.27

Find $Inn(D_4)$.

Recall, $D_4 = \{e, R, R^2, R^3, H, V, D, D'\}$. Notice that if $g \in Z(D_4)$ then $\phi_g(x) = x$ for all $x \in D_4$, meaning $\phi_g = id$. Also recall that $Z(D_4) = \{e, R^2\}$. Let $x \in D_4$. Then,

$$\begin{aligned}
\phi_{R^3}(x) &= R^3x(R^3)^{-1} \\
&= (RR^2)x(RR^2)^{-1} \\
&= R(R^2xR^2)R^{-1} \\
&= RxR^{-1} \\
&= \phi_R(x)
\end{aligned}$$

So $\phi_{R^3} = \phi_R$. Now, $VR^2 = H$ so

$$\begin{aligned}
\phi_H(x) &= HxH \\
&= (VR^2)x(VR^2)^{-1} \\
&= V(R^2xR^2)V \\
&= VxV \\
&= \phi_V(x)
\end{aligned}$$

So $\phi_V = \phi_H$. Similarly $\phi_D = \phi_{D'}$. So, $Inn(D_4) = \{id, \phi_R, \phi_H, \phi_D\}$.

Now, $D_4/Z(D_4) = \{[e], [R], [H], [D]\}$. It turns out that $D_4/Z(D_4) \cong Inn(D_4)$.

Example 7.28: Automorphisms on finite cyclic groups

What is $Aut(\mathbb{Z}_n)$?

Let $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ be an isomorphism. Since $\mathbb{Z}_n = \langle 1 \rangle$, we can determine ϕ if we know $\phi(1)$. Also, since ϕ is an isomorphism, $\mathbb{Z}_n = \langle \phi(1) \rangle$. The set of generators of $\mathbb{Z}_n$ is $\mathbb{Z}_n^*$, so $\phi(1) \in \{m \in \mathbb{Z}_n : \gcd(m, n) = 1\}$.

Theorem 7.29

$Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

Proof. Define $F : Aut(\mathbb{Z}_n) \to \mathbb{Z}_n^*$ by $\phi \mapsto \phi(1)$. F is well-defined since $F(\phi) \in \mathbb{Z}_n^*$ for all $\phi \in Aut(\mathbb{Z}_n)$. It will be shown that F is an isomorphism.

(One-to-one.) Let $\phi_1, \phi_2 \in Aut(\mathbb{Z}_n)$ such that $F(\phi_1) = F(\phi_2)$. Then for all $x \in \mathbb{Z}_n$,

$$\begin{aligned}
\phi_1(x) &= \phi_1(\underbrace{1 + \cdots + 1}_{x}) \\
&= \underbrace{\phi_1(1) + \cdots + \phi_1(1)}_{x} \\
&= \underbrace{\phi_2(1) + \cdots + \phi_2(1)}_{x} \\
&= \phi_2(\underbrace{1 + \cdots + 1}_{x}) \\
&= \phi_2(x)
\end{aligned}$$

so $\phi_1 = \phi_2$.

(Onto.) Let $k \in \mathbb{Z}_n^*$. Then the function $\phi \in Aut(\mathbb{Z}_n)$ defined by $\phi(1) = k$ is such that $F(\phi) = k$, so F is onto.

(Homomorphism.) Let $\phi_1, \phi_2 \in Aut(\mathbb{Z}_n)$. Then,

$$\begin{aligned}
F(\phi_1 \circ \phi_2) &= (\phi_1 \circ \phi_2)(1) \\
&= \phi_1(\phi_2(1)) \\
&= \phi_1(\underbrace{1 + \cdots + 1}_{\phi_2(1)}) \\
&= \underbrace{\phi_1(1) + \cdots + \phi_1(1)}_{\phi_2(1)} \\
&= \phi_1(1)\phi_2(1) \\
&= F(\phi_1)F(\phi_2)
\end{aligned}$$

Therefore $Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$. □

Example 7.30

Let p be prime. Then, $|Aut(\mathbb{Z}_p)| = p - 1$.

7.4 First isomorphism theorem

Example 7.31

Recall $\ker\phi$ is a normal subgroup for any homomorphism ϕ. In particular, $A_n \triangleleft S_n$. Notice that $|S_n/A_n| = 2$ so $S_n/A_n \cong \mathbb{Z}_2$.

Theorem 7.32: First isomorphism theorem

Let $\phi : G \to H$ be a homomorphism. Then, $G/\ker\phi \cong \text{Im }\phi$.

Proof. Let $K = \ker\phi$. Define $\psi : G/K \to \text{Im }\phi$ by $gK = [g] \mapsto \phi(g)$. It will be shown that this is an isomorphism.

(Well-defined.) Let $[g_1] = [g_2]$. Then, $g_1 = g_2 k$ for some $k \in K$.

$$\begin{aligned}\psi([g_1]) &= \phi(g_1)\\ &= \phi(g_2 k)\\ &= \phi(g_2)\phi(k)\\ &= \phi(g_2)\\ &= \psi([g_2])\end{aligned}$$

so $[g_1] = [g_2] \implies \psi([g_1]) = \psi([g_2])$ and thus ψ is well-defined.

(One-to-one.) Suppose $[g_1], [g_2] \in G/K$ such that $\psi([g_1]) = \psi([g_2])$. Then,

$$\begin{aligned}\phi(g_1) &= \phi(g_2)\\ \phi(g_1)\phi(g_2)^{-1} &= e\\ \phi(g_1 g_2^{-1} &= e\\ \therefore g_1, g_2^{-1} &\in K\\ \therefore g_1 &= g_2 k \text{ for some } k \in K\\ \therefore g_1 &\in g_2 K\\ \therefore [g_1] &= [g_2]\end{aligned}$$

so ψ is one-to-one.

(Onto.) Let $h \in \text{Im }\phi$. Since ϕ is surjective, there exists $g \in G$ such that $\phi(g) = h$. So, $\psi([g]) = h$ and ψ is onto.

(Homomorphism.) Let $[g_1], [g_2] \in G/K$. Then,

$$\begin{aligned}\psi([g_1][g_2]) &= \psi([g_1 g_2])\\ &= \phi(g_1 g_2)\\ &= \phi(g_1)\phi(g_2)\\ &= \psi([g_1])\psi([g_2])\end{aligned}$$

so ψ is a homomorphism and hence an isomorphism. $\square$

Corollary 7.33

1. Let $\phi : G \to H$ be a homomorphism, with G, H both finite. Then $|\text{Im } \phi|$ divides both $|G|$ and $|H|$.
2. Let G be a group. Then, $G/Z(G) \cong Inn(G)$.

Proof.

1. We know $\text{Im } \phi \leq H$ so $|\text{Im } \phi|$ divides $|H|$ by Lagrange's theorem. Also $G/\ker\phi \cong \text{Im } \phi$ so $|G| = |\ker\phi||\text{Im } \phi|$ therefore $|\text{Im } \phi|$ divides $|G|$.
2. Define $\phi : G \to Inn(G)$ by $g \mapsto \phi_g$ where $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Then for all $x, y \in G$ we have

$$\begin{aligned}\phi_g(xy) &= gxyg^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= \phi_g(x)\phi_g(y)\end{aligned}$$

so ϕ is a homomorphism. Also, $\ker\phi = Z(G)$ and $\text{Im } \phi = Inn(G)$ so by first isomorphism theorem 7.32 $G/Z(G) \cong Inn(G)$.

□

7.5 Correspondence theorem

Theorem 7.34: Normal subgroups are kernels

Let G be a group, and $N \lhd G$. Then $N = \ker\phi$ where $\phi : G \to G/N$ is defined by $g \mapsto [g]$. This is called the natural homomorphism of N in G.

Proof. Since $N \lhd G$, we know G/N is a group. Let $a, b \in G$. Then,

$$\begin{aligned}\phi(ab) &= [ab] \\ &= [a][b] \\ &= \phi(a)\phi(b)\end{aligned}$$

so ϕ is a homomorphism.

Let $k \in \ker\phi$. Then, $\phi(k) = [e] = N$ so $k \in N$.

Let $n \in N$. Then, $\phi(n) = nN = N$ so $n \in \ker\phi$. □

Definition 7.35: Image and pre-image

Let $\phi : G \to H$ be a homomorphism, and let $S \subseteq G$. Define $\phi(S) := \{\phi(x) : x \in S\}$ to be the image of S.
Let $T \in H$. Define $\phi^{-1}(T) := \{x \in G : \phi(x) \in T\}$ to be the pre-image or inverse image of T.

Lemma 7.36

Let $\phi : G \to H$ be a homomorphism. Then:

1. If $G_1 \leq G$ then $\phi(G_1) \leq H$.
2. If $H_1 \leq H$ then $\phi^{-1}(H_1) \leq G$.

Theorem 7.37: Correspondence theorem

Let $\phi : G_1 \to G_2$ be a surjective homomorphism and let $K = \ker \phi$. Then there is a bijective correspondence between $U := \{H \leq G_1 : K \leq H\}$ and $V := \{\overline{H} : \overline{H} \leq G_2\}$ defined by $H \mapsto \phi(H)$ and $\overline{H} \mapsto \phi^{-1}(\overline{H})$. Moreover,

1. For $H_1, H_2 \in U$ we have $H_1 \leq H_2$ iff $\phi(H_1) \leq \phi(H_2)$.
2. For $H \in U$, we have $|G_1 : H| = |G_2 : \phi(H)|$.
3. For $H \in U$, we have $H \lhd G$ iff $\phi(H) \lhd G$.

Proof. It will be shown that $\phi(\phi^{-1}(\overline{H})) = \overline{H}$ and $\phi^{-1}(\phi(H)) = H$ for all $\overline{H} \in V$ and $H \in U$. This implies the bijection. The rest of the proof is given in the solution to A4.

Let $h \in \phi(\phi^{-1}(\overline{H}))$. Then, $h = \phi(g)$ for some $g \in \phi^{-1}(\overline{H})$. So, $\phi(g) \in \overline{H}$ by definition of ϕ^{-1}, therefore $h \in \overline{H}$ and $\phi(\phi^{-1}(\overline{H})) \subseteq \overline{H}$.

Let $h \in \overline{H}$. Then since ϕ is surjective, there exists $g \in G_1$ such that $\phi(g) = h$. So, $g \in \phi^{-1}(\overline{H})$. Therefore, $h \in \phi(\phi^{-1}(\overline{H}))$ so $\phi(\phi^{-1}(\overline{H})) = \overline{H}$. $\square$

Example 7.38

How many subgroups of $\mathbb{Z}_{100}$ contain 15?

Solution 1. If $H \geq \langle 15 \rangle$ then $|\langle 15 \rangle| = 20$ is a factor of $|H|$ and $|H|$ is a factor of 100. There are two such numbers, 20 and 100. Therefore there are two such subgroups.

Solution 2. By Correspondence theorem, the number of subgroups containing $\langle 15 \rangle$ is equal to the number of subgroups of $\mathbb{Z}_{100}/\langle 15 \rangle$. The natural homomorphism is $\phi : \mathbb{Z}_{100} \to \mathbb{Z}_{100}/\langle 15 \rangle$ defined by $x \mapsto [x]$. We have $\ker \phi = \langle 15 \rangle$ and $\mathbb{Z}_{100}/\langle 15 \rangle \cong \mathbb{Z}_5$. $\mathbb{Z}_5$ has two subgroups, so there are two subgroups of $\mathbb{Z}_{100}$ containing $\langle 15 \rangle$.

Corollary 7.39

Let G be a group, and $N \lhd G$. Then the subgroups of G/N correspond to subgroups of G that contain N.

8 Group Actions

8.1 Introduction

Remark 8.1

We want to generalize Cayley's theorem (7.8). We shall view a group as a set of permutations on a set $X \neq \emptyset$.

Let G be a group, $X \neq \emptyset$ be a set, such that the elements of G are bijective functions (that is, permutations) from X to X.

Example 8.2: Symmetric group

S_n is a group acting on $X = \{1, 2, \ldots, n\}$ since all $\sigma \in S_n$ is a permutation. We say S_n acts on X.

Example 8.3: Dihedral group

D_4 acts on $X = \{1, 2, 3, 4\}$, where elements of X can be seen as the vertices of a square. We already know that $D_4 \leq S_4$. In general, D_n acts on vertices of a regular n-gon.

Example 8.4: General linear group

$GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$. If $A \in GL_n(\mathbb{R})$ then A induces a linear transformation $L_A : \mathbb{R}^n \to \mathbb{R}^n$ defined by $v \mapsto Av$. Since A is invertible, L_A is bijective.

Definition 8.5: Group action

Let $X \neq \emptyset$ be a set. $S_X := (\{f : X \to X | f \text{ is bijective}\}, \circ)$ is the group of permutations of X under composition. Now, two definitions will be given which turn out to be equivalent.

1. Let G be a group, $X \neq \emptyset$ be a set. G acts on X with action $\cdot : G \times X \to X$ defined by $(g, x) \mapsto g \cdot x$ if $e \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$ for all $x \in X$, $g, h \in G$.

2. Let G be a group, $X \neq \emptyset$ be a set. Let $\cdot : G \times X \to X$ be a function and define $\varphi : G \to S_X$ by $\varphi(g)(x) := g \cdot x$ for all $(g, x) \in G \times X$. Then G acts on X with action $\cdot$ if φ is a homomorphism.

If G acts on X with some given action we write $G \curvearrowright X$.

Proposition 8.6

Definitions 1 and 2 of a group action are equivalent.

Proof. Suppose we have a function $\cdot : G \times X \to X$ which is an action by definition 1. Now, define a function $\varphi : G \to S_X$ where $\varphi(g) : X \to X$ maps x to $g \cdot x$ for all $g \in G$. Let $g_1, g_2 \in G$. Then,

$$\begin{aligned} \varphi(g_1 g_2)(x) &= (g_1 g_2) \cdot x \\ &= g_1 \cdot (g_2 \cdot x) \\ &= \varphi(g_1)(\varphi(g_2)(x)) \\ &= (\varphi(g_1) \circ \varphi(g_2))(x) \end{aligned}$$

for all $x \in X$ so φ is a homomorphism, and so $\cdot$ satisfies definition 2.

Suppose we have a function $\cdot : G \times X \to X$ which is an action by definition 2. So, φ is a homomorphism. Let $g_1, g_2 \in G$ and $x \in X$. Then,

$$\begin{aligned} (g_1 g_2) \cdot x &= \varphi(g_1 g_2)(x) \\ &= (\varphi(g_1) \circ \varphi(g_2))(x) \\ &= \varphi(g_1)(\varphi(g_2)(x)) \\ &= g_1 \cdot (g_2 \cdot x) \end{aligned}$$

Also,

$$\begin{aligned} e \cdot x &= \varphi(e)(x) \\ &= id(x) \\ &= x \end{aligned}$$

since the identity element in S_X is id and φ is a homomorphism. Therefore $\cdot$ satisfies definition 1. $\square$

Example 8.7: Trivial action

Let G be a group and $X \neq \emptyset$ be a set. Then $\cdot : G \times X \to X$ defined by $(g, x) \mapsto x$ is an action since

$$e \cdot x = x$$

and

$$\begin{aligned}(gh) \cdot x &= x \\ &= g \cdot (h \cdot x)\end{aligned}$$

for all $g, h \in G$.

Example 8.8: Left multiplication

Let G be a group. $G \curvearrowright G$ by the action $\cdot : G \times G \to G$ defined by $(g, h) \mapsto gh$. The proof of this follows quickly from the identity and associativity properties of a group.

Example 8.9: Conjugation

Let G be a group. $G \curvearrowright G$ by the action $\cdot : G \times G \to G$ defined by $(g, h) \mapsto ghg^{-1}$.

Proof.

$$\begin{aligned}e \cdot x &= exe^{-1} \\ &= x\end{aligned}$$

and

$$\begin{aligned}(gh) \cdot x &= ghx(gh)^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= g(h \cdot x)g^{-1} \\ &= g \cdot (h \cdot x)\end{aligned}$$

for all $g, h \in G$. □

8.2 Orbits and stabilizers

Definition 8.10: Orbit and stabilizer

Let G be a group and $X \neq \emptyset$ be a set such that $G \curvearrowright X$ with action $\cdot$. Let $x \in X$.

The orbit of x is $O_x := \{g \cdot x : x \in G\}$.

The stabilizer of x is $\text{Stab}(x) := \{g \in G : g \cdot x = x\}$.

Remark 8.11

Note that $O_x \subseteq X$ and $\text{Stab}(x) \subseteq G$.

Proposition 8.12: Stabilizer is a subgroup

Let G be a group and $X \neq \emptyset$ such that $G \curvearrowright$ with action $\cdot$. For all $x \in X$, $\text{Stab}(x) \leq G$.

Proof. Let $g, h \in \text{Stab}(x)$. Then,

$$\begin{aligned}
h \cdot x &= e \cdot x \\
h^{-1} \cdot (h \cdot x) &= h^{-1} \cdot (e \cdot x) \\
(h^{-1}h) \cdot x &= h^{-1} \cdot x \\
x &= h^{-1} \cdot x \\
\therefore h^{-1} &\in \text{Stab}(x)
\end{aligned}$$

so $\text{Stab}(x)$ is closed under inverses.

$$\begin{aligned}
(gh) \cdot x &= g \cdot (h \cdot x) \\
&= g \cdot x \\
&= x
\end{aligned}$$

so $\text{Stab}(x)$ is closed under the group operation. Therefore by two-step test, $\text{Stab}(x) \leq G$. $\square$

Example 8.13: Trivial action

Let G be a group and $X \neq \emptyset$ be a set, such that $G \curvearrowright X$ by the trivial action. Then, $O_x = \{x\}$ and $\text{Stab}(x) = G$ for all $x \in X$.

Example 8.14: Left multiplication

Let G be a group. Consider the action $\cdot : G \times G \to G$ defined by $(g, h) \mapsto gh$. Then $O_g = G$ and $\text{Stab}(g) = \{e\}$ for all $g \in G$.

Example 8.15: Conjugation

Let G be a group and $G \curvearrowright G$ by conjugation. That is, $g \cdot x = gxg^{-1}$ for all $g \in G$ and $x \in X$. Then, $gxg^{-1} = x \iff gx = xg$ so $\text{Stab}(g) = C(G)$, the centralizer of g.

Theorem 8.16: Orbit-stabilizer theorem

Let G be a group acting on a set X by action $\cdot$. Let $x \in X$. Then, $|G : \text{Stab}(x)| = |O_x|$. If G is finite then $|G| = |O_x||\text{Stab}(x)|$.

Proof. Define $C := \{[g] : g \in G\}$ where $[g] := g\text{Stab}(x)$. Define $T : C \to O_x$ by $[g] \mapsto g \cdot x$. It will be shown that T is a bijection.

(Well-defined.) Let $[g], [h] \in C$ such that $[g] = [h]$. Then, $h^{-1}g \in \text{Stab}(x)$ so $(h^{-1}g) \cdot x = x$. We will show $T([g]) = T([h])$.

$$\begin{aligned}
(h^{-1}g) \cdot x &= x \\
h \cdot ((h^{-1}g) \cdot x) &= h \cdot x \\
(hh^{-1}g) \cdot x &= h \cdot x \\
g \cdot x &= h \cdot x \\
T([g]) &= T([h])
\end{aligned}$$

(One-to-one.) Suppose $T([g]) = T([h])$ for some $[g], [h] \in C$. Then,

$$\begin{aligned}
g \cdot x &= h \cdot x \\
h^{-1} \cdot (g \cdot x) &= h^{-1} \cdot (h \cdot x) \\
(h^{-1}g) \cdot x &= x \\
\therefore h^{-1}g &\in \text{Stab}(x) \\
\therefore g &\in h\text{Stab}(x) \\
\therefore [g] &= [h]
\end{aligned}$$

(Onto.) Let $y \in O_x$. So, $y = g \cdot x$ for some $g \in G$. Therefore, $y = T([g])$.

Hence T is a bijection between C and O_x so $|C| = |O_x|$. This proves $|G : \text{Stab}(x)| = |O_x|$. If $|G|$ is finite, this implies $|G| = |O_x||\text{Stab}(x)|$ by part (i) of corollary 2.7. $\square$

Proposition 8.17

Let G be a group and $X \neq \emptyset$ be a set such that $G \curvearrowright X$ by action $\cdot$. Then, the set $\{O_x : x \in X\}$ is a partition of X.

Proof. It will be shown that the relation $\sim$ defined by $x \sim y$ iff $O_x = O_y$ is an equivalence relation.

(Reflexive.) We have $e \cdot x = x$ so $x \sim x$ for all $x \in X$.

(Symmetric.) Suppose $x \sim y$ where $x, y \in X$. Then $O_x = O_y$ so clearly, $y \sim x$.

(Transitive.) Suppose $x, y, z \in X$ such that $x \sim y$ and $y \sim z$. Then, $O_x = O_y = O_z$ so $x \sim z$.

This proves $\{O_x : x \in X\}$ is a partition of X. □

Remark 8.18

The fact that the orbits partition the set X implies that $|X| = \sum_{i=1}^{n} |O_{x_i}|$, where $x_1, \ldots, x_n$ are representatives from each distinct orbit in X.

Theorem 8.19: Cauchy's theorem

Let G be a finite group, with $|G| = n$. If p is a prime number which is a factor of n, then there exists $H \leq G$ such that $|H| = p$.

Proof. Consider $X = \{(g_1, \ldots, g_p) \in G^p : g_1 \ldots g_p = e\}$. Note that $(e, \ldots, e) \in X$ so $X \neq \emptyset$.

Define an action $\cdot$ of $\mathbb{Z}_p$ on X by

$$\begin{aligned} 0 \cdot (g_1, \ldots, g_p) &= (g_1, \ldots, g_p) \\ 1 \cdot (g_1, \ldots, g_p) &= (g_2, \ldots, g_p, g_1) \\ 2 \cdot (g_1, \ldots, g_p) &= (g_3, \ldots, g_p, g_2) \end{aligned}$$

that is, $n \cdot (g_1, \ldots, g_p) = (g_{1+n \mod p}, \ldots, g_{p+n \mod p})$ for all $n \in Z_p$. Now, $|X| = |G|^{p-1}$ since $g_1, \ldots, g_{p-1}$ can be any element of G leaving only one choice for g_p. Since p divides $|G|$ it also divides $|G|^{p-1}$ and therefore p divides $\sum_{i=1}^{n} |O_{x_i}|$.

Thus either all orbits have size p or there is a multiple of p number of orbits of size 1, since by orbit-stabilizer theorem

$$\begin{aligned} p &= |\mathbb{Z}_p| \\ &= |O_x||\text{Stab}(x)| \\ \therefore |O_x| &= 1 \text{ or } |O_x| = p \end{aligned}$$

for all $x \in X$. Now, $|O_{(e,\ldots,e)}| = 1$ so there exists $x \in X$ such that $x \neq (e, \ldots, e)$ and $|O_x| = 1$. Let $x = (x_1, \ldots, x_p)$.

But since $|O_x| = 1$, $x_1 = \cdots = x_p = g$ for some $g \in G$ by the definition of the action. Since $x \in X$, $g^p = e$ so $|g| = p$. Hence take $\langle g \rangle$. $\square$

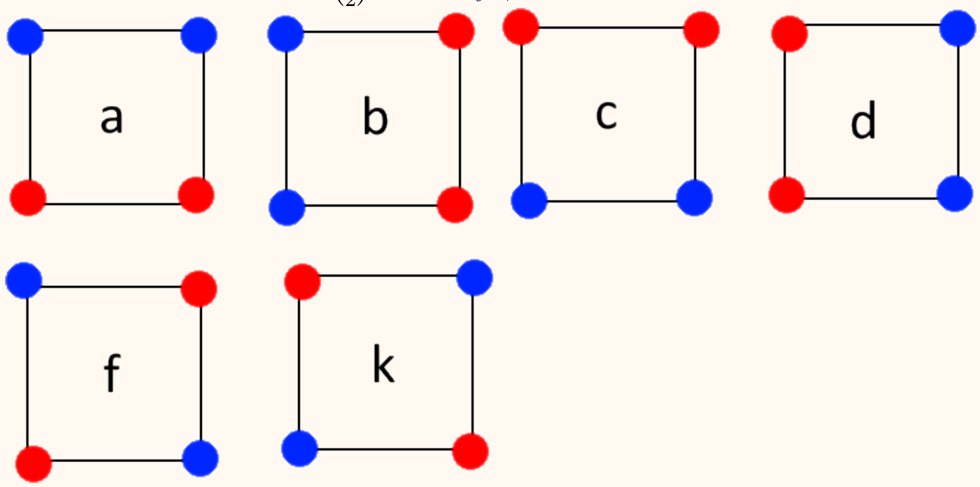
Corollary 8.20

Let G be an abelian group such that $|G| = pq$ for distinct primes p, q. Then, G is cyclic.

Proof. By Cauchy's theorem, there exist $g, h \in G$ such that $|g| = p$ and $|h| = q$. Then $G = \langle gh \rangle$ since $\gcd(|g|, |h|) = 1$. $\square$

Example 8.21

How many ways can we colour the vertices of a square such that two vertices are blue and two are red? There are $\binom{4}{2} = 6$ ways, as shown here:



How many ways are there, if we consider flips and rotations of each colouring to be equivalent?

Let X be the set of colourings, and $x, y \in X$. We let $D_4 \curvearrowright X$, and consider two elements $x, y \in X$ to be equivalent iff there exists $g \in D_4$ such that $g \cdot x = y$. It can be seen that there are only two colourings up to equivalence, which are the two rows of this illustration.

Definition 8.22: Fixed set

Let G be a group acting on a set X with action $\cdot$. We define $X_g := \{x \in X : g \cdot x = x\}$ and call it the <u>fixed set of g</u>.

Example 8.23

In our colouring example, $G = \{e, R, R^2, R^3, H, V, D, D'\}$.

$$\begin{aligned} X_e = X &= \{a, b, c, d, f, k\} \\ X_R = X_{R^3} &= \{\} \\ X_{R^2} = X_D = X_{D'} &= \{f, k\} \\ X_H &= \{b, d\} \\ X_V &= \{a, c\} \end{aligned}$$

Notice that $\frac{|X_e|+\cdots+|X_V}{|D_4|} = \frac{16}{8} = 2$ which is the number of distinct orbits of the action (that is, colourings up to equivalence).

Lemma 8.24: "Burnside's" lemma

Let G be a finite group acting on a finite set X. Let N be the number of distinct orbits of the action. Then, $N = \frac{1}{|G|}\sum_{g\in G}|X_g|$.

Proof. Let $T = \{(x,g) : x \in X, g \in G \text{ such that } g \cdot x = x\}$. We will determine $|T|$ in two ways. We note that $|T| = \sum_{x\in X}|\mathrm{Stab}(x)|$ and $|T| = \sum_{g\in G}|X_g|$. By orbit-stabilizer theorem, $|\mathrm{Stab}(x)| = \frac{|G|}{|O_x|}$ for all $x \in X$. Combining these equations, we get

$$\sum_{g\in G}|X_g| = |G|\sum_{x\in X}\frac{1}{|O_x|}$$

So we need to show $N = \sum_{g\in G}|X_g|$ to conclude the proof. Recall that the set of orbits partitions X. Let $O_{y_1}, \dots, O_{y_N}$ be the distinct orbits of X.

$$\begin{aligned}
\sum_{x\in X}\frac{1}{|O_x|} &= \left(\sum_{x\in O_{y_1}}\frac{1}{|O_x|}\right) + \cdots + \left(\sum_{x\in O_{y_N}}\frac{1}{|O_x|}\right)\\
&= \left(\sum_{x\in O_{y_1}}\frac{1}{|O_{y_1}|}\right) + \cdots + \left(\sum_{x\in O_{y_N}}\frac{1}{|O_{y_N}|}\right)\\
&= \underbrace{1 + \cdots + 1}_{N}\\
&= N
\end{aligned}$$

□

Example 8.25

Find the number of ways to number sides of an 8-sided die shaped like a regular octahedron.

Solution. Let G be the set of rotational symmetries of the octahedron. Let Y be the set of vertices of the octahedron. Let $v \in Y$. Then, $|O_v| = 6$ since there are 6 vertices v can move to under some rotation. Also $|\text{Stab}(v)| = 4$ since there are 4 distinct rotations which do not change the location of v. Therefore, $|G| = 6(4) = 24$ by Orbit-stabilizer theorem.

Now, $|X_e| = 8!$ since all 8! numberings are unchanged under the identity rotation. Also $|X_g| = 0$ for all $g \neq e$ since all non-identity rotations will change at least one face. By Burnside's lemma,

$$\begin{aligned} N &= \frac{1}{24}\sum_{g\in G}|X_g| \\ &= \frac{1}{24}8! \\ &= 1680 \end{aligned}$$

Example 8.26

How many necklaces can be made with 5 beads using only black and white beads?

Solution. Consider the necklace as a regular pentagon, with vertices coloured black or white, where two colourings are equivalent if they are the same under some flips and/or rotations. The identity rotation leaves 32 colourings the same; the 4 non-identity rotations leave two colourings the same(all black and all white); the 5 flips leave 8 colourings the same. Therefore $N = \frac{1}{10}(32 + 4(2) + 5(8)) = 8$.

Example 8.27

How many ways to colour a square's edges with 6 colours such that each edge is a distinct colour?

Solution. Consider colourings to be equivalent if they are the same under some transformation in D_4. Let X be the set of colourings. Let N be the numbers of orbits on the action of D_4 on X.

We have $|D_4| = 8$ and $|X_e| = |X| = \binom{6}{4} = 360$. Only the 6 colourings where every edge is the same colour is unchanged by R and by R_3. There are $6(6) = 36$ colourings unchanged by R^2, or the 4 flips. Therefore, there are $\frac{1}{8}(360 + 2(6) + 5(36)) = 69$ ways.

Definition 8.28: Conjugacy class

Let G be a group and consider the action of G on itself by conjugation. Let $g \in G$. The conjugacy class of g is the orbit of g: $O_g = \{hgh^{-1} : h \in G\}$.

Example 8.29

What are conjugacy classes of $S_3 = \{e, (12), (13), (23), (123), (132)\}$?

$$\begin{aligned} O_e &= \{e\} \\ O_{(12)} = O_{(13)} = O_{(23)} &= \{(12), (23), (13)\} \\ O_{(123)} = O_{(132)} &= \{(123), (132)\} \end{aligned}$$

Proposition 8.30

Let G be a group, and let $G \curvearrowright G$ by conjugation. Then, $g \in Z(G)$ iff $O_g = \{g\}$.

Proof. ($\Rightarrow$) If $g \in Z(G)$ then for all $h \in G$,

$$\begin{aligned} hgh^{-1} &= hh^{-1}g \\ &= g \end{aligned}$$

So, $O_g = \{g\}$.

($\Leftarrow$) If $O_g = \{g\}$, then $hgh^{-1} = g$ for all $h \in G$. Therefore, $hg = gh$ so $g \in Z(G)$. $\square$

Definition 8.31: Class equation

Let G be a finite group, and let $G \curvearrowright G$ by conjugation. We have $|G| = \sum_{i=1}^{n} |O_{g_i}|$ where g_i is a representative from each distinct conjugacy class. We can rewrite this as

$$|G| = |Z(G)| + \sum_{g_i \notin Z(G)} |O_{g_i}|$$

By orbit-stabilizer theorem,

$$\begin{aligned} |O_{g_i}| &= \frac{|G|}{|\mathrm{Stab}(g_i)|} \\ &= \frac{|G|}{|C(g_i)|} \end{aligned}$$

so we can rewrite the equation as

$$|G| = |Z(G)| + \sum_{g_i \notin Z(G)} \frac{|G|}{|C(g_i)|}$$

This equation is called the class equation of G.

Example 8.32: Class equation of S_3

x	O_x	$C(x)$
e	$\{e\}$	S_3
(12)	$\{(12), (13), (23)\}$	$\{e, (12)\}$
(123)	$\{(123), (132)\}$	$\{(123), (132)\}$

So, the class equation of S_3 is $|S_3| = 6 = 1 + \frac{6}{2} + \frac{6}{3}$.

9 Classification of finite abelian groups

9.1 Initial results

Theorem 9.1: p-groups have nontrivial center

Let G be a group such that $|G| = p^n$ where p is prime and $n \in \mathbb{Z}$ with $n \geq 1$. Then, $Z(G) \neq \{e\}$.

Proof. For contradiction suppose $|Z(G)| = 1$. By class equation,

$$\begin{aligned} p^n &= |Z(G)| + \sum_{g_i \notin Z(G)} \frac{p^n}{|C(g_i)|} \\ &= 1 + \sum_{g_i \notin Z(G)} \frac{p^n}{|C(g_i)|} \end{aligned}$$

Now, $C(g_i) \neq G$ since $g_i \notin Z(G)$ and also $C(g_i) \leq G$. So, $|C(g_i)|$ divides p^n and $|C(g_i)| < p^n$. Therefore, $\frac{p^n}{|C(g_i)|} = p^{k_i}$ for some $1 \leq k_i < n$.

Thus p divides $\sum_{g_i \notin Z(G)} \frac{p^n}{|C(g_i)|}$, so p does not divide $1 + \sum_{g_i \notin Z(G)} \frac{p^n}{|C(g_i)|} = p^n$, which is a contradiction. $\square$

Corollary 9.2

Let G be a group. If $|G| = p^2$ for some prime p, then G is abelian.

Proof. We know $Z(G) \neq \{e\}$ so $|Z(G)| \in \{p, p^2\}$ by Lagrange's theorem.

If $|Z(G)| = p$ then $|G/Z(G)| = \frac{p^2}{p} = p$ so $|G/Z(G)|$ is cyclic. By G/Z theorem 6.13 G is abelian.

If $|Z(G)| = p^2$ then $Z(G) = G$ so G is abelian. $\square$

Remark 9.3

Let G be a group with $N \lhd G$. What are the subgroups of G/N?

Recall correspondence theorem 7.37. Let $\phi : G \to G/N$ defined by $g \mapsto gN$ be the natural homomorphism. Note that ϕ is surjective and that $\ker \phi = N$. So, the subgroups of G/N correspond to subgroups of G that contain N.

If $T \leq G/N$ then there is $H \leq G$ such that $N \lhd H$ and $T = \phi(H) = H/N$. So, all subgroups of G/N are H/N where $N \lhd H$.

Example 9.4

What are the subgroups of $\mathbb{Z}/12\mathbb{Z}$?

The subgroups are $H/12\mathbb{Z}$ where $12\mathbb{Z} \subseteq H$. If $n \in 12\mathbb{Z}$ then $n = 12k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n &= 4(3k) \in 4\mathbb{Z} \\ &= 3(4k) \in 3\mathbb{Z} \\ &= 2(6k) \in 2\mathbb{Z} \\ &= 6(2k) \in 6\mathbb{Z} \end{aligned}$$

These represent all non-trivial ways to write 12 as a product of positive integers. The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are therefore $12\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}, 4\mathbb{Z}/12\mathbb{Z}, 3\mathbb{Z}/12\mathbb{Z}, 2\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$.

Theorem 9.5

Let G be a group such that $|G| = p^n$ for some prime p and positive integer n. Then for each integer k such that $0 \leq k \leq n$, there exists a subgroup $H \leq H$ such that $|H| = p^k$.

Proof. By strong induction on n.

Base case. Suppose $n = 1$. Then $\{e\} \leq G$ with $|\{e\}| = p^0$ and $G \leq G$ with $|G| = p^1$. Thus the statement holds in the base case.

Inductive step. Suppose for all $i < n$, all groups of order p^i contains a subgroup of order p^j for all $0 \leq j \leq i$. It will be shown that if G is a group of order p^n then it has a subgroup of order p^k for all $0 \leq k \leq n$.

By theorem 9.1 $|Z(G)| \neq 1$. So, $|Z(G)| = p^a$ for some $a \in \mathbb{Z}$. By Cauchy's theorem, there exists an element $x \in Z(G)$ such that $|x| = p$. Therefore, $\langle x \rangle \lhd Z(G) \lhd G$.

Consider $G/\langle x \rangle$. We have $|G/\langle x \rangle| = p^{n-1}$. For each k such that $0 \leq k \leq n-1$ there exists a subgroup $H_k \leq G/\langle x \rangle$ such that $|H_k| = p^k$ by inductive hypothesis.

Now, $H_k = B_k/\langle x \rangle$ where $\langle x \rangle \leq B_k \leq G$ by remark 9.3. So, $|B_k| = p^{k+1}$. Hence $B_0, \ldots, B_{n-1}$ are subgroups of G with order $p^1, \ldots, p^n$ respectively. $\square$

9.2 Fundamental theorem of finite abelian groups

Remark 9.6

We know of some families of finite abelian groups: $\{e\}, \mathbb{Z}_n, \mathbb{Z}_n^*, \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ for example.

- We know that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \iff \gcd(n, m) = 1$.
- If $H \leq G$ and $K \leq G$ are finite then $|HK| = \frac{|H \times K|}{|H \cap K|}$.
- If G, H are abelian then $G \times H$ is abelian.

Proposition 9.7

Let G be a group. If $H \triangleleft G$ and $N \triangleleft G$ with $H \cap N = \{e\}$ and $|H||N| = |G|$ then $G \cong H \times N$.

Theorem 9.8: Fundamental theorem of finite abelian groups

Let G be a finite abelian group. Then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

where $p_1, \ldots, p_k$ are prime and $n_1, \ldots, n_k$ are positive integers. Moreover, this presentation is unique up to ordering.

Example 9.9: Abelian groups of order 8

There are three abelian groups of order 8 up to isomorphism: $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Remark 9.10: Abelian p-groups

Let G be an abelian group such that $|G| = p^n$ where p is prime. Note that $|G| = p^{n_1} \ldots p^{n_k}$ where $n_1 + \cdots + n_k = n$. In other words, $n_1, \ldots, n_k$ form a partition of n.

Thus, G is isomorphic to $\mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$ for some $n_1 + \cdots + n_k = n$.

Example 9.11: Abelian groups of order 40

Find all abelian groups of order 40 up to isomorphism.

We know $40 = 2^3 \cdot 5$. By fundamental theorem of finite abelian groups, the only abelian groups of order 40 are

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_5 \cong \mathbb{Z}_{40}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_{10}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{10}$$

Lemma 9.12

Let G be a group such that $G \cong G_1 \times \cdots \times G_k$ where $G_1, \ldots, G_k$ are all groups. Suppose $H_1 \leq G_1, \ldots, H_k \leq G_k$. Then, $H_1 \times \cdots \times H_k \leq G$.

Proof. Let $a = (a_1, \ldots, a_k), b = (b_1, \ldots, b_k) \in H_1 \times \cdots \times H_k$. Then,

$$\begin{aligned} ab^{-1} &= (a_1, \ldots, a_k)(b_1, \ldots, b_k)^{-1} \\ &= (a_1, \ldots, a_k)(b_1^{-1}, \ldots, b_k^{-1}) \\ &= (a_1 b_1^{-1}, \ldots, a_k b_k^{-1}) \in H_1 \times \cdots \times H_k \end{aligned}$$

since H_i is a group for all $1 \leq i \leq k$. Therefore by one-step test, $H_1 \times \cdots \times H_k \leq G$. $\square$

Corollary 9.13

Let G be an abelian group and $|G| = n$. Then if d is a divisor of n then there exists $H \leq G$ such that $|H| = d$.

Proof. By fundamental theorem of finite abelian groups, $G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$ where $p_1, \ldots, p_k$ are primes and $n_1, \ldots, n_k$ are positive integers. Since d is a factor of n, $d = p_1^{m_1} \ldots p_k^{m_k}$ where $m_i \leq n_i$ for all $1 \leq i \leq k$.

Now, for all $1 \leq i \leq k$ there is a subgroup of $\mathbb{Z}_{p_i^{n_i}}$ of order $p_i^{m_i}$ by theorem 9.5. Let these subgroups be $H_1, \ldots, H_k$. Hence $H = H_1 \times \ldots H_k$ meets the desired conditions by lemma 9.12. $\square$

Example 9.14: Abelian groups of order 72

Up to isomorphism, find all abelian groups of order 72.

Note that $72 = 2^3 \cdot 3^2$. Up to ordering the partitions of 2 are $1+1$ and 2 and the partitions of 3 are $1+1+1$, $1+2$, 3. Between these, there are $2(3) = 6$ possible abelian groups of order 72.

$$\begin{aligned}
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2 &=: G_1 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_6 \times \mathbb{Z}_{12} &=: G_2 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \cong \mathbb{Z}_3 \times \mathbb{Z}_{24} &=: G_3 \\
\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{18} \times \mathbb{Z}_2 \times \mathbb{Z}_2 &=: G_4 \\
\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \cong \mathbb{Z}_{18} \times \mathbb{Z}_4 &=: G_5 \\
\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \cong \mathbb{Z}_9 \times \mathbb{Z}_8 \cong \mathbb{Z}_{72} &=: G_6
\end{aligned}$$

Now, find a subgroup of order 12 of each of $G_1, \ldots, G_6$.

$$\begin{aligned}
\{0\} \times \mathbb{Z}_6 \times \mathbb{Z}_2 &\leq G_1 \\
\{0\} \times \mathbb{Z}_{12} &\leq G_2 \\
\{0\} \times \langle 2 \rangle &\leq G_3 \\
\langle 3 \rangle \times \mathbb{Z}_2 \times \{0\} &\leq G_4 \\
\langle 6 \rangle \times \mathbb{Z}_4 &\leq G_5 \\
\langle 6 \rangle &\leq G_6
\end{aligned}$$