10 Further Group Theory

We discuss further properties of groups, giving a brief introduction to the notions of group isomorphism, cyclic groups, cosets and Lagrange’s theorem.

We start with a fundamental theorem.

Lemma 10.1. Let \((G, \ast)\) be a group. Then

(i) \(e\), the identity element of \(G\) is unique,

(ii) every element of \(G\) has a unique inverse,

(iii) given any \(a, b \in G\) there is a unique solution \(x\) to the equation \(a \ast x = b\) and the equation \(x \ast a = b\),

(iv) \((ab)^{-1} = b^{-1}a^{-1}\) for any pair \(a, b \in G\).

Proof. We leave (i) and (ii) as exercises. To see that (iii) holds, note that \(x = a^{-1}b\) (respectively \(x = ba^{-1}\)) is a solution to the equation \(a \ast x = b\) (respectively \(x \ast a = b\)). To see that this solution is unique, observe that if \(x_1, x_2\) are both solutions to \(a \ast x = b\) then \(a \ast x_1 = b = a \ast x_2 \Rightarrow x_1 = x_2 = a^{-1}b\), which we obtain upon multiplying by \(a^{-1}\).

To see that (iv) holds, note that

\[(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e,
\]

and similarly \((b^{-1}a^{-1})(ab) = e\) so \(b^{-1}a^{-1}\) is the inverse of \(ab\).

The conditions of (iii) that hold in a group are called the left and right cancellation laws. If \(S\) is a set with an associative operation but is not a group (such as \(\mathbb{Z}\) wrt multiplication), then given arbitrary \(a, b\), we may not be able to solve an equation of the type \(ax = b\) for \(x\) in \(\mathbb{Z}\).

10.1 Cyclic Groups

Let \(k\) be a positive integer. Given a group \((G, \ast)\) we write \(a^k\) to denote the composition of \(a\) with itself \(k\) times:

\[a^k = a \ast a \ast \cdots \ast a.\]

We define \(a^{-k}\) to be the composition of \(a^{-1}\) with itself \(k\) times:

\[a^{-k} = a^{-1} \ast a^{-1} \ast \cdots \ast a^{-1}.\]

By convention, we write \(a^0 = e\), where \(e\) is the identity element of \(G\) wrt \(a\).

The standard rules of logarithms and exponents holds in the case of a group:

\[a^u a^v = a^{u+v}, \quad (a^u)^v = a^{uv}, \quad (a^{-1})^k = a^{-k}\]

In the case of an additive group, such as \((\mathbb{Z}, +)\) or \((\mathbb{Z}_n, +)\), it is common to write \(k \cdot a\) in place of \(a^k\). Then

\[k \cdot a = a + a + \cdots + a, \quad \text{and} \quad -k \cdot a = k \cdot (-a) = (-a) + (-a) + \cdots + (-a).\]

The additive identity of a group is usually denoted by \(0\). As expected, \(0 \cdot a = 0(a) = 0\).

The standard associative and distributive laws of \(\mathbb{Z}\) hold wrt this notation:

\[u \cdot a + v \cdot a = (u + v) \cdot a, \quad u \cdot (v \cdot a) = (uv) \cdot a, \quad (-k) \cdot a = -(k \cdot a)\]

The order of an element \(a \in G\) is the least positive integer \(t\) such that \(a^t\) is the identity element of \(G\). We write \(o(a) = t\). If no such integer exists, we say that \(a\) has infinite order, and write \(o(a) = \infty\).
The order of a group is the number of elements contained in it.

Given a nonempty subset $A$ of a group $G$, we denote by $\langle A \rangle$ the subgroup of $G$ generated by $A$. $\langle A \rangle$ is the smallest subgroup of $G$ that contains $A$ (it is the intersection of all subgroups of $G$ that contain $A$). By "smallest" we mean that if $H < G$ and $A \subseteq H$ then $\langle A \rangle < H$. If $A$ is finite, we say that $\langle A \rangle$ is finitely generated.

Example 10.1. Let $A = \{(1234),(12)\} \subset S_4$. Then the subgroup of $S_4$ generated by $A$ is found by computing all possible products of the elements of $A$.

Example 10.2. Let $A = \{(1234),(24)\}$. $(1234)^2 = (13)(24)$, $(1234)^3 = (1432)$ are all contained in $\langle A \rangle$. Note that $(1234)^4 = (1)$, so $\text{ord}(1234) = 4$, and $\text{ord}(24) = 2$, so we need not compute $(1234)^k(12)^t$ for $k \geq 5, t \geq 2$. Then $(1234)(24) = (12)(34), (1432)(24) = (14)(23) \in \langle A \rangle$. In fact these are all of the elements of $\langle A \rangle$.

Definition 10.1. A group generated by a single element is called a cyclic group.

If $G = \langle a \rangle$, then $G = \{a^k : k \in \mathbb{Z}\}$.

Example 10.3.

- $(\mathbb{Z}, +)$ is a cyclic group generated by $1$.
- $(\mathbb{Z}_n, +)$ is a cyclic group generated by $[1]$. In fact $(\mathbb{Z}_n, +) = \langle [x] \rangle$ for any $[x] \in \mathbb{Z}_n$ such that $\gcd(x, n) = 1$.
- $C_n$, the set of $n$ complex $n-th$ roots of unity is a cyclic group generated by $z = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. In fact $C_n$ is generated by $z^k$ for any $k$ for which $\gcd(k, n) = 1$.
- The 5-cycle $(12345)$ generates a cyclic subgroup of order 5.
- If $G$ is a group and $a \in G$ then $\langle a \rangle$ is a cyclic subgroup of $G$ and $|\langle a \rangle| = \text{ord}(a)$.

Lemma 10.2. Any subgroup of a cyclic group is also cyclic.

Proof. Let $G$ be a cyclic group generated by $a$ and let $H < G$. Since every element of $G$ can be expressed in the form $a^k$ for some integer $k$. Suppose that $H$ has 2 distinct generators $x, y$. Since $G$ is cyclic, it is also abelian, so $H = \langle x, y \rangle = \{x^iy^j : i, j \in \mathbb{Z}\}$. Now $x = a^s, y = a^t$ for some integers $s, t$. Consider the element $x^iy^j$ in $H$. Let $d = \gcd(s, t)$. Then, as $d$ is a common divisor of $s$ and $t$,

$$x^iy^j = a^{si}a^{tj} = a^{si+tj} = a^{dm} = (a^d)^m,$$

where $m$ is some integer satisfying $dm = si + tj$. Moreover, since $d = \gcd(s, t)$ there exist $i, j \in \mathbb{Z}$ such that $d = si + tj$. It follows that $H$ is generated by $a^d$.

Cyclic groups are the most fundamental of all groups, and form the building blocks of other groups. We’ll look at this class of groups again when we study Lagrange’s theorem.

10.2 Group Isomorphism

A group homomorphism is a map that identifies equations between groups. A bijective homomorphism between groups indicates that the groups in question are structurally identical.

Definition 10.2. Let $(G_1, *)_1, (G_2, *)_2$ be groups. A map $\theta : G_1 \to G_2$ is called a group homomorphism if

$$\theta(a *_1 b) = \theta(a) *_2 \theta(b),$$

for every $a, b \in G_1$. If $\theta$ is $1-1$ and onto we call it a group isomorphism.
Example 10.4. Consider the groups \((G_i, \ast_i), i = 1, ..., 4\), listed below.

- \(G_1 = C_4 = \{1, i, -1, -i\}\), \(\ast_1 = \text{complex multiplication}\)
- \(G_2 = \mathbb{Z}_4 = \{[0], [1], [2], [3]\}\), \(\ast_2 = \text{addition modulo } 4\)
- \(G_3 = \langle (1234) \rangle = \{(1), (1234), (13)(24), (1432)\}\), \(\ast_3 = \text{composition of functions}\)
- \(G_4 = V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}\), \(\ast_4 = \text{composition of functions}\)

Then \(G_1, G_2, G_3\) are all isomorphic as groups, but none are isomorphic to \(G_4\). Note that \(a^2 = (1)\) for each \(a \in G_4\), but \(i^3 = -1\). So if \(\theta\) is a group homomorphism from \(G_1\) into \(G_4\) then \(\theta(-1) = \theta(i^3) = \theta(i)^2 = (1)\) and \(\theta(1) = \theta(i^4) = \theta(i)^4 = (1)^2 = (1)\), which means that \(\theta\) cannot be a group isomorphism. Note that \(G_1, G_2, G_3\) are all cyclic groups, while \(G_4\) requires at least a pair of generators. We construct an explicit isomorphism between \(G_1, G_2\). Let \(\theta : G_1 \to G_2\) be the correspondence defined by \(\theta(i) = [1]\), and extend \(\theta\) to a group isomorphism:

\[
\theta(i^2) = \theta(i)^2 = 2 \cdot [1] = [2], \quad \theta(i)^3 = 3 \cdot [1] = [3], \quad \theta(1) = \theta(i)^4 = 4 \cdot [1] = [4] = [0]
\]

Theorem 10.1. Let \(G, H\) be groups and let \(\theta\) be an isomorphism \(\theta : G \to H\). Then given any \(a \in G\),

(i) \(\theta(e_G) = e_H\),
(ii) \(\theta(a^{-1}) = \theta(a)^{-1}\)
(iii) \(|G| = |H|\),
(iv) \(o(a) = o(\theta(a))\),
(v) if \(G\) is cyclic, then so is \(H\),
(vi) if \(G\) is abelian, then so is \(H\),
(vii) if \(S < G\) then \(\theta(S) < G\)

Proof. (i) Let \(a, b \in G\). Then 

\[
\theta(a) = \theta(ae_G) = \theta(a)\theta(e_G) = \theta(a)e_H,
\]
so by the cancellation law, \(\theta(e_G) = e_H\).

(ii) Let \(a, b \in G\) such that \(ab = e_G\). Then 

\[
e_H = \theta(e_G) = \theta(ab) = \theta(a)\theta(b).
\]

(vii) Let \(S < G\). Given any \(x, y \in \theta(S)\), there exist \(a, b \in S\) such that \(a, b \in S\). Then 

\[
\theta(a)\theta(b) = \theta(ab) \in \theta(S)
\]
as \(ab \in S\) for any \(a, b \in S\). Moreover, \(x^{-1} = \theta(a)^{-1} = \theta(a^{-1}) \in \theta(S)\), since \(a^{-1} \in S\) for any \(a \in S\).

We leave the remaining proofs as exercises.

Properties of a group that are preserved under group isomorphism are called the isomorphism invariants of a group.

Theorem 10.2. Group isomorphism is an equivalence relation on the set of all groups

Proof. The relation is clearly reflexive as every group is isomorphic to itself under the identity map. If \(\theta : G \to H\) is an isomorphism then so is \(\theta^{-1} : h \to G\), for if \(a, b \in H\) then \(\theta^{-1}(ab) = xy = \theta^{-1}(a)\theta^{-1}(b)\), where \(x, y \in G\) satisfy \(\theta(x) = a, \theta(y) = b\). Moreover \(\theta^{-1}\) is a bijection, being invertible. Composition of bijections results in a bijection. If \(\alpha : G \to H, \beta : H \to T\) are group isomorphisms then

\[
\beta \circ \alpha(ab) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(b)) = \beta(\alpha(a))\beta(\alpha(b)) = \beta \circ \alpha(a)\beta \circ \alpha(b),
\]
so \(\beta \circ \alpha : G \to T\) is a group isomorphism, and hence the relation is transitive.

We show that, up to isomorphism, any cyclic group is characterized by its order. In fact any cyclic group can be identified either with the additive group of the integers, or the additive group of the integers modulo \(n\) for some positive integer \(n\).

Theorem 10.3. If \(G\) is a cyclic group then either
1. G has finite order n and is isomorphic to (Zn, +), or
2. G has infinite order and is isomorphic to (Z, +).

Proof. Let G = (a) and let e be the identity element of G. If G is infinite then let θ : G → Z be defined by θ(a^k) = k · 1 for each integer k. Then θ is well defined on G since a^k is well-defined on G. Any pair of elements x, y ∈ G have the form x = a^u, y = a^v for some integers u, v. Then

θ(xy) = θ(a^u a^v) = θ(a^{u+v}) = (u + v) · 1 = u · 1 + v · 1 = θ(a^u)θ(a^v) = θ(x)θ(y),

so θ is a group homomorphism. If θ(x) = θ(y) then

θ(a^u) = θ(a^v) ⇒ (u · 1) = (v · 1) ⇒ (u - v) · 1 = 0 ⇒ u = v ⇒ a^u = a^v ⇒ x = y,

so G has finite order.

If G has finite order n, then define a map θ : G → Z_n by θ(a^k) = k · [1] = [k]. As before, it is straightforward to show that θ is a well-defined group isomorphism.

10.3 Cosets and Lagrange’s Theorem

The main result of this section is that if H is a subgroup of a finite group G then the order of H divides the order of G. This is known as Lagrange’s theorem. Before we prove this result, we need the notion of a coset.

Definition 10.3. Let G be a group and let H be a subgroup of G. A right coset of H in G is a set of the form

Hg = \{hg : h ∈ H\}.

A left coset is defined similarly.

Let H = 3Z_{12} = \{[0], [3], [6], [9]\}. Then H < Z_{12}. We list the cosets of H in Z_{12}.

\begin{align*}
H + [0] &= \{[0], [3], [6], [9]\} = H \\
H + [1] &= \{[1], [4], [7], [10]\} \\
H + [2] &= \{[2], [5], [8], [11]\} \\
H + [3] &= \{[3], [6], [9], [0]\}
\end{align*}

Note that H = H + [3], since [a] + [b] ∈ H for any [a], [b] ∈ H, so there are exactly 3 distinct cosets of H in G.

If H < G and Hx = Hy for some pair x, y ∈ G then ax = by for some a, b ∈ H. Then xy^{-1} = a^{-1}b ∈ H.

On the other hand, if xy^{-1} = h ∈ H then x = hy ∈ Hy, and hence Hx ⊂ Hy. Similarly, Hx ⊂ Hy, so both cosets are equal.

We’ve just shown that:

Lemma 10.3. Let H < G and let x, y ∈ G. Then Hx = Hy iff xy^{-1} ∈ H


Note that distinct cosets of H in Z_{12} are disjoint and their union is Z_{12}. In fact this holds in general.

Theorem 10.4. Let G be a group and let H < G. Let R be the relation on G defined by (x, y) ∈ R if xy^{-1} ∈ H. Then R is an equivalence relation on G and each equivalence class [x] is the coset Hx, for each x ∈ G. Moreover, the set of distinct cosets of H forms a partition of G.

Proof. Observe that (x, y) ∈ R iff Hx = Hy. Let P be the collection of distinct cosets of H in G. If z ∈ Hx ∩ Hy then z = ax = by for some a, b ∈ H, which means that xy^{-1} ∈ H, and so Hx = Hy. It follows that two cosets Hx, Hy are either equal or disjoint. Moreover, x = ex ∈ Hx, so every element of G is contained in some coset of H in G, namely Hx. It follows that P = \{Hx : x ∈ G\} is a partition of G. Since every partition determines an equivalence relation where (x, y) ∈ R iff x, y belong to the same set in the partition, R as defined is an equivalence relation on G with [x] = Hx for each x ∈ G.
Lemma 10.4. Let $G$ be a group and let $H < G$. Then $|H| = |Hx|$ for any $x \in G$.

Proof. Let $x \in G$. We define a bijection from $H$ onto $Hx$. Define

$$\theta : H \to Hx : h \mapsto hx.$$ 

Then $\theta$ is a well-defined map on $H$ since the operation in $H$ is well defined. It is also onto by construction, since every element of $Hx$ has the form $hx$ for some $h \in H$, given any $y = hx \in Hx$, $h$ is the required element satisfying $\theta(h) = y$. The equation $y = hx$ has a unique solution in $G$, for any given pair $x, y \in G$, so $\theta$ is $1 - 1$. It follows that there exists a bijection from $H$ onto $Hx$, so both sets must have the same cardinality.

We can now prove Lagrange’s theorem.

Theorem 10.5. Let $G$ be a finite group and let $H < G$. Then $|H|$ is a divisor of $|G|$.

Proof. List the distinct cosets of $H$ in $G$ as

$$H, Hg_2, Hg_3, ..., Hg_t$$

for some positive integer $t$. From Theorem 10.4, these form a partition of $G$, so as $G$ is the disjoint union of $H, Hg_2, Hg_3, ..., Hg_t$, it follows that

$$|G| = |H| + |Hg_2| + |Hg_3| + \cdots + |Hg_t|,$$

and from Lemma 10.4, $|H| = |Hg_i|$ for each $i$, so that $|G| = t|H|$, and $|H|$ divides $|G|$ in $\mathbb{Z}$.

If $H < G$ where $G$ is a group, we denote by $[G : H]$ the quotient $|G|/|H|$. The number $[G : H]$ is called the index of $H$ in $G$. It counts the number of distinct cosets of $H$ in $G$.

Lagrange’s theorem can be very useful for proving results about finite groups.

Corollary 10.1. Every group of prime order is cyclic.

Proof. Let $G$ be a group of order $p$ for some prime $p$ and let $a \in G$. Now $a$ generates the subgroup $H = \langle a \rangle$ of $G$ and from Lagrange’s thereom $|H|$ divides $p$. Since $p$ is prime, either $a$ is the identity element of $G$, or $H = G$.

A similar argument can be used to prove the following.

Corollary 10.2. If $G$ is a group of prime order then $G$ has no subgroups other than itself and the identity subgroup.

Corollary 10.3. Let $G$ be a group of finite order $n$. If $a \in G$ then $o(a)$ divides $n$.

For example, if $G$ is a group of order 33, from Lagrange’s theorem, if $G$ does have any subgroups, they must have order 3 or 11. Moreover, if $G$ does have any nontrivial subgroups, they must have prime order and hence be cyclic.

Remark: Note that the converse of Lagrange’s theorem does not hold in general, that is, if $d$ divides $|G|$ we cannot deduce that $G$ has a subgroup of order $d$. However, in the case of cyclic groups, we do have a partial converse. In fact if $G$ is cyclic and has finite order $n$, then $G$ has exactly one subgroup of order $d$ for every $d$ that divides $n$.

Theorem 10.6. Let $G$ be a cyclic group of order $n$ generated by $a \in G$. Then

(i) $o(a) = n$,

(ii) $a^s = a^t$ iff $s \equiv t \mod n$,

(iii) for each positive divisor $d$ of $n$, $\langle a^d \rangle$ is a subgroup of $G$ of order $n/d$,
(iv) there is exactly one subgroup of $G$ of order $d$ for each positive divisor $d$ of $n$.

Proof. Let $e$ be the identity element of $G$. (i) This follows immediately since $G = \langle a \rangle = \{a, a^2, a^3, ..., a^{n-1}, a^n = e\}$. 
(ii) If $a^s = a^t$ for some integers $s, t$ then 
$$e = (a^s)^{-1}a^t = a^{-s}a^t = a^{t-s} = a^n.$$ 
We claim that $n$ divides $t - s$. From the division algorithm there exist integers $m, r$ such that $t - s = mn + r$ and $0 \leq r < n$. Then 
$$e = a^{t-s} = a^{mn+r} = (a^n)^m a^r = ea^r = a^r,$$
so it follows that $a^r = e$. Since $n$ is the least positive integer satisfying $a^n = e$, we deduce that $r = 0$.
(iii) Let $d$ be a divisor of $n$, say $n = kd$ for some positive integer $k$. Then $a^n = a^{kd} = (a^d)^k = e$, so as in the proof of (ii), $t = o(a^d)$ divides $k$. If $t < k$ then $td < kd = n$, so $a^{td} \neq e$, giving a contradiction. It follows that $o(a) = k$.
(iv) Let $H_1, H_2 < G$ both have order $d$ for some divisor $d$ of $n$. Since any subgroup of a cyclic group is also cyclic, $H_1 = \langle a^{k_1} \rangle$ and $H_2 = \langle a^{k_2} \rangle$ for some positive integers $k_1, k_2$. From (i), $o(a^{k_1}) = o(a^{k_2}) = d$, so $n = k_1d = k_2d$. Then $(k_1 - k_2)d = 0$, so $k_1 = k_2$ and $H_1 = H_2$. \hfill \Box

From Lagrange’s theorem, every subgroup of a finite cyclic group $G$ has order that is a divisor of $|G|$, and from Theorem 10.6, every divisor of $|G|$ corresponds to exactly one subgroup of that order. It follows that the subgroup lattice of a cyclic group is completely determined by its order.

### 10.4 Some Final Remarks

The notion of a coset is not only useful as a tool in the proof of Lagrange’s theorem. If a subgroup $H$ of $G$ satisfies a further property, namely that $Hg = gH$ for each $g \in G$, we call it a normal subgroup. Note that the property of being normal is equivalent to the condition that $ghg^{-1} \in H$ for each $g \in G$. Note also that if $G$ is abelian, then every subgroup of $G$ is normal.

If $H$ is a normal subgroup of $G$, then the set of distinct cosets of $H$ in $G$ itself takes on the structure of a group. We denote this set of cosets by 
$$G/H = \{Hg : g \in G\},$$
and define an operation on $G/H$ by $(Hx)(Hy) = H(xy)$. If $Hx = Ha, Hy = Hb$ for some $a, b, x, y \in G$ then $xa^{-1}, yb^{-1} \in H$, and since $H$ is normal, $Hg = gH \Rightarrow H = ghg^{-1}$ for each $g \in G$. Then 
$$(xy)(ab)^{-1} = (xy)(b^{-1}a^{-1}) = x(a^{-1}a)(y(b^{-1}a^{-1})) = (xa^{-1})(a(yb^{-1})a^{-1}) \in H,$$
as $xa^{-1} \in H, yb^{-1} \in H$, and $g(yb^{-1})g^{-1} \in H$ for each $g \in G$. This shows that if $Hx = Ha, Hy = Hb$ then $H(xy) = H(ab)$, so the operation is well-defined on $G/H$.

Also, 
$$(H(a)(Hb))(Hc) = (H(ab))(Hc) = H(ab)c = H(a(bc)) = H(a(H(b)c)) = H(a(H(b))(Hc)),$$
since the operation in $G$ is associative, so the operation as defined on $G/H$ is associative. The identity of $G/H$ wrt this operation is $H$, and the inverse of $Hg$ in $G/H$ is $Hg^{-1}$.

So the set of cosets of a normal subgroup in a group $G$ forms a group wrt the operation as defined above.

**Example 10.5.** Let $H = 5\mathbb{Z} = \{5z : z \in \mathbb{Z}\}$. We’ve observed before that $H < (\mathbb{Z}, +)$. Moreover since $\mathbb{Z}$ is abelian wrt $+$, $H$ is a normal subgroup of $\mathbb{Z}$. Then $\mathbb{Z}/5\mathbb{Z}$ is a group. We list the distinct cosets of $H$ in $\mathbb{Z}$ as 

* $H = 5\mathbb{Z} = \{5k : k \in \mathbb{Z}\} = [0]$
* $H + 1 = 5\mathbb{Z} + 1 = \{5k + 1 : k \in \mathbb{Z}\} = [1]$
* $H + 2 = 5\mathbb{Z} + 2 = \{5k + 2 : k \in \mathbb{Z}\} = [2]$
* $H + 3 = 5\mathbb{Z} + 3 = \{5k + 3 : k \in \mathbb{Z}\} = [3]$
* $H + 4 = 5\mathbb{Z} + 4 = \{5k + 4 : k \in \mathbb{Z}\} = [4]$

35
Observe that these cosets are in fact the congruence classes of the integers modulo 5. This is easy to see also
from the fact that by definition, \([x] = [y]\) in \(\mathbb{Z}_5\) iff 5 divides \(x - y\), which is equivalent to the condition that
\([x] - [y] = [x - y] = [0]\) in \(\mathbb{Z}_5\). For this reason, the integers modulo 5 can be represented by the symbol \(\mathbb{Z}_5\)
or \(\mathbb{Z}/5\mathbb{Z}\).