Groups, Rings and Fields

Thobias Høivik

Spring 2026

Contents

1 Groups

Definition 1.1 (Group). *A group is a set S together with a binary operation $\circ$ such that the following properties hold:*

1. *Identity: There exists an element $e \in S$, satisfying*

$$e \circ a = a \circ e = a$$

   for every $a \in S$.

2. *Inverses: For every $a \in S$ there exists $b \in S$ such that*

$$a \circ b = b \circ a = e, \text{ the identity element}$$

   We usually denote this element as a^{-1} or $-a$, depending on context.

3. *Associativity: For any $a, b, c \in S$, we require*

$$a \circ (b \circ c) = (a \circ b) \circ c$$

A group is then the tupple $(S, \circ)$. We will often just write the set to refer to the group, e.g. refering to the group $(\mathbb{Z}, +)$ as just $\mathbb{Z}$.

1.1 Basic Examples

Example 1.1 (Integers under addition). *The set of integers $\mathbb{Z}$ with the operation $+$ forms a group:*

- *Identity: 0 since $0 + n = n + 0 = n$ for all $n \in \mathbb{Z}$.*
- *Inverses: For $n \in \mathbb{Z}$, the inverse is $-n$.*
- *Associativity: Addition is associative.*

Hence $(\mathbb{Z}, +)$ is a group.

Example 1.2 (Non-example: Natural numbers under addition). *The set $\mathbb{N}$ under $+$ is* not *a group since there is no inverse for $n > 0$.*

1.2 Basic Properties

Theorem 1.1 (Uniqueness of identity). *The identity element in a group is unique.*

Proof. Suppose e and e' are both identities. Then

$$e = e \circ e' = e',$$

so the identity is unique. □

Theorem 1.2 (Uniqueness of inverses). *Each element in a group has a unique inverse.*

Proof. Suppose b and c are inverses of a. Then

$$b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c.$$

□

1.3 Example Problem

Problem 1.1. *Determine whether the set*

$$G = \{1, -1, i, -i\} \subset \mathbb{C}$$

with multiplication is a group.

Solution. We check the group axioms:

1. **Closure:** Multiplying any two elements of G yields another element in G. True.
2. **Identity:** The element 1 acts as identity. True.
3. **Inverses:** Each element has an inverse in G: $1^{-1} = 1$, $(-1)^{-1} = -1$, $i^{-1} = -i$, $(-i)^{-1} = i$. True.
4. **Associativity:** Multiplication of complex numbers is associative. True.

Hence $(G, \cdot)$ is a group, in fact it is an abelian group which we shall describe below in definition 1.2. □

1.4 Abelian Groups

Definition 1.2 (Abelian Group). *A group $(G, \circ)$ is* abelian *(or commutative) if*

$$a \circ b = b \circ a \quad \forall a, b \in G.$$

Example 1.3. *The group $(\mathbb{Z}, +)$ is abelian because $m + n = n + m$.*

2 Important Groups

First let's define some often used notation.

For $g \in G$, define:

- $g^n = gg \dots g (n > 0)$
- $g^0 = e$
- $g^{-n} = (g^{-1})^n$

and recognize the following identities (which are provable by induction):

$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}$$

Definition 2.1 (Roots of Unity).

$$U_n = \{e^{2\pi ik/n} : 0 \leq k < n\}$$

are called the n-th roots of unity.

Definition 2.2. *An subset $\{g_1, \dots, g_k\} \subseteq G$ is a generating set if every $g \in G$ can be expressed as*

$$g_1^{n_1} \cdots g_k^{n_k}$$

If a singleton g' alone generates a group then it is called a generator of G and G is said to be cyclic.

The n-th roots of unity are finite, with exactly n elements. They are cyclic, with generator $e^{2i\pi/n}$.

Definition 2.3 (Symmetric Group). *The symmetric group S_n is the set of all permutations of n elements under composition. In other words it is the set of all $\sigma : [n] \to [n]$ with composition as its operation.*

The symmetric group is non-abelian for $n \geq 3$. The identity corresponds to the identity permutation (doing nothing) and inverses are undoing a permutation. We have the following notation for permutations in the symmetric Group (assume $n = 3$ for this example):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

corresponds to $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$.

Another way to write the same permutation is:

$$(1\,2\,3)$$

3 Subgroups

Definition 3.1 (Subgroup). *Let G be a group under $\star$. A subgroup $H \leq G$ is a subset $H \subseteq G$ that is itself a group under $\star$.*

Having to mechanically check if $H \subseteq G$ satisfies all the required axioms can be a bit tedious so next we introduce a powerful theorem which let's us easily determine whether some subset is a subgroup or not.

Theorem 3.1 (Subgroup Test). *A nonempty subset $H \subseteq G$ is a subgroup if and only if*

$$\forall x, y \in H,\ xy^{-1} \in H.$$

Proof Idea. If H is a subgroup the required conditions follows.

Conversely:

- Nonempty so some $h \in H$.
- $hh^{-1} = e \in H$.
- Closure under xy^{-1} will give inverses and closure.

□

We get some nice corollaries from this, as well as a nice and tidy way to prove whether or not a subset is a subgroup.

Corollary 3.1. *The intersection of any collection of subgroups is a subgroup.*
Given any subset $S \subseteq G$, there is a smallest subgroup containing it.

Definition 3.2 (Cyclic Subgroups). *Let G be a group.*
For any $g \in G$, define:

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

$\langle g \rangle$ is called the cyclic subgroup generated by g.

It is very straightforward to show that the cyclic subgroup generated by some $g \in G$ is indeed a subgroup with the use of theorem 3.1.

On page 6 we say that a group is cyclic if it has a signle element which generates it, but now we can simply say that a group G is cyclic if $G = \langle g \rangle$ for some $g \in G$.

Theorem 3.2. *Suppose a group G is cyclic, i.e. $G = \langle g \rangle$ for some $g \in G$.*
Then it is isomorphic to one of the following:

- $(\mathbb{Z}, +)$, *or*
- $(\mathbb{Z}/n\mathbb{Z}, +)$ *for some $n \geq 1$.*

3.1 Structure of Cyclic Subgroups

Definition 3.3 (Order). *The order of an element $g \in G$ is*

$$\mathrm{ord}(g) = |\langle g \rangle|$$

Furthermore, if $\mathrm{ord}(g) = n < \infty$, then $g^n = e$ and n is minimal, otherwise we say g has infinite order.

If $\mathrm{ord}(g) = n$, then:

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

Moreover:

- $g^k = e \Leftrightarrow n \mid k$
- $\langle g^k \rangle = \langle g \rangle \Leftrightarrow \gcd(k, n) = 1$

Theorem 3.3. *Every subgroup of a cyclic group is cyclic.*
More precisely:

- *Subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$.*
- *Subgroups of $\mathbb{Z}/n\mathbb{Z}$ correspond to the divisors of n.*

With all of this machinery we can approach group theory with geometric and algebraic intuition. Cyclic groups are like repeated motion, finite cyclic groups corresponding to rotations by rational angles and infinite ones corresponding to translations.

4 Cosets and Lagrange's Theorem

Definition 4.1 (Left and Right Cosets). *Let $H \leq G$, and let $g \in G$. The left- and right cosets are:*

$$gH = \{gh : h \in H\} \quad Hg = \{hg : h \in H\}$$

respectively.

A key intuition is that a coset is like a copy of H shifted by g. We may also recognize that the cosets are the same size as H by identifying $h \mapsto gh$ to be a bijection and so forth.

The next natural question is when are two cosets equal? Like with showing when a subset is a subgroup we have a little trick for this problem.

Theorem 4.1. *Let G be a group.*
For $g_1, g_2 \in G$, the following are equivalent:

$$\begin{gathered} g_1 H = g_2 H \\ \Updownarrow \\ g_2^{-1} g_1 \in H \\ \Updownarrow \\ g_1 \in g_2 H \end{gathered}$$

Theorem 4.2. *The set of all left cosets of $H \leq G$ forms a partition of G.*
That is,

- *Every element of G is in exactly on coset.*
- *Two cosets are either the same or disjoint.*

Definition 4.2. *Let G be a group with $H \leq G$.*
The index of H in G, written $[G : H]$, is the number of left cosets of H.

If G is finite we get $|G| = [G : H] \cdot |H|$.

Theorem 4.3 (Lagrange's Theorem). *Let G be a group with $H \leq G$. Then:*

$$|H| \,\big|\, |G|$$

Proof. Let G be a group with $H \leq G$.

Recall that by theorem 4.2 we have that the set of left cosets of H, $g_1H, g_2H, \ldots, g_kH$ (this set is finite since G is finite) are pairwise disjoint, satisfying

$$G = \bigcup_{i=1}^{k} g_iH$$

meaning

$$|G| = \sum_{i=1}^{k} |g_iH|$$

Recall also that $|H| = |g_iH|, \forall i \in [k]$. Thus

$$|G| = \sum_{i=1}^{k} |H| = k|H|$$

In other words $|G|$ is $|H|$ times some integer k, therefore $|H|$ divides $|G|$. □

Theorem 4.3 has the following immediate consequences:

- The order of any element divides $|G|$.
- $g^{|G|} = e$ for every $g \in G$.

Beware that it does not follow from Lagrange's Theorem that there exists a subgroup with the order of a divisor of $|G|$ for every divisor of G. The alternating group of order 12, A_4, has no subgroup of order 6 for example.

Proposition 4.1. *A group of order p where p is prime, is cyclic.*

Proof Sketch. Let G be a group with $|G| = p$ (prime).

Let $g \in G \setminus \{1\}$. Consider it's generated subgroup $\langle g \rangle$. By Lagrange's Theorem the order of this subgroup divides p so $|\langle g \rangle|$ is 1 or p, but it can't be 1 as $g \neq 1$ so it's order is p, i.e. g generates the entirety of G. □

4.1 Problems relating to subgroups

Problem 4.1. *Let G be a group and $g \in G$ with ord$(g) = 12$.*

- *List all distinct subgroups of $\langle g \rangle$.*
- *For which integers k does g^k generate $\langle g \rangle$?*

Solution. Recalling that $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$, we want to find all the distinct subgroups of $\langle g \rangle$. In other words, which subsets of $\langle g \rangle$ are also groups with respect to the operation of G?

ord$(g) = |\langle g \rangle| = 12$ hence $\langle g \rangle = \{g^0, g^1, \dots, g^{11}\}$. We know that there are two trivial subgroups of $\langle g \rangle$, namely $\{g^0\}$ and $\langle g \rangle$. Otherwise, we know that every cyclic subgroub of a cyclic group (which $\langle g \rangle$ is) is itself cyclic, so we can find the subgroups by looking at the generated groups of each element of $\langle g \rangle$. Otherwise, we could use the fact that $\langle g \rangle$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ together with realizing that the number of subgroups is then the same as the number of positive divisors of 12.

Using the first approach we get:

$$\begin{aligned}
\langle g^2 \rangle &= \{g^n : n = 2k,\ k \in \mathbb{Z}\} \\
&= \{e, g^2, \dots, g^10\} = \langle g^10 \rangle \\
\langle g^3 \rangle &= \{e, g^3, g^6, g^9\} = \langle g^9 \rangle \\
\langle g^4 \rangle &= \{e, g^4, g^8\} = \langle g^8 \rangle \\
\langle g^6 \rangle &= \{e, g^6\}
\end{aligned}$$

Those integers which are coprime to 12, like $1, 5, 7, 11$, will generate $\langle g \rangle$. Thus we have 6 distinct subgroups, exactly the same as the number of positive divisors of 12, as expected. □

Problem 4.2. *Let G be any group $H = \langle g \rangle$ where ord$(g) < \infty$. Prove that if $g^m \in H$, then $\langle g^m \rangle \leq H$.*

Proof. Assume, for contradiction, that $g^m \in H$, but $\langle g^m \rangle$ is not a subgroup of H.

Let $s = m \mod \text{ord}(g)$. Then $\langle g^m \rangle = \{g^{sk} : k \in \mathbb{Z}\} \neq \emptyset$. It is clear that this is a subset of $\langle g \rangle = H$, since $\langle g \rangle$ is closed under the group operation and $g^m \in H$. Then the only way our assumption is true is if there exists some $x, y \in \langle g^m \rangle$ such that $xy^{-1} \notin \langle g^m \rangle$.

Every element $x, y \in \langle g^m \rangle$ is of the form $x = g^{sn}, y = g^{st}$ for some $n, l \in \mathbb{N}$. By assumption, $xy^{-1} = g^{s(n-t)} \notin \langle g^m \rangle$ which would necessarily mean that $n - t \notin \mathbb{Z}$, impossible. □

The above argument can be made more rigorous by considering the isomorphism between $\langle g^m \rangle$ and $\mathbb{Z}/s\mathbb{Z}$, or by proving the claim directly (I am an idiot, and this was a bad approach).

5 Normal subgroups

Definition 5.1 (Normal subgroup). *A subgroup $H \leq G$ is normal, written $H \trianglelefteq G$, if:*

$$gH = Hg, \forall g \in G$$

with the equivalent characterization:

$$H \trianglelefteq G \Leftrightarrow gHg^{-1} = H, \forall g \in G$$

A few things to tick off immediately;

1. Every subgroup of an abelian group is normal.
2. {e} and G are always normal.
3. The alternating group $A_n \trianglelefteq S_n$.
4. Subgroups of index 2 are always normal.

If you consider the map (conjugation)

$$x \mapsto gxg^{-1},$$

which constitutes an automorphism of G we can say the following.

Normal subgroups are precisely those subgroups which are fixed under every conjugation.

Definition 5.2 (Quotient Group). *If $H \trianglelefteq G$, define:*

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

with an operation we'll call multiplication by:

$$(gH)(kH) = (gk)H$$

Theorem 5.1. *The quotient group with multiplication, as defined above, is a well-defined group.*

Definition 5.3. *We define the* ***canonical projection*** *as*

$$\pi : G \to G/H,\ \pi(g) = gH.$$

Notably, the projection π constitutes a homomorphism with kernel $\ker \pi = H$. Notice that this claim of the kernel being H itself should be immediately obvious as hH for some $h \in H$ is itself H as it's closed.

6 Exercises for Week 1

Problem 6.1 (29, p.48). *Show that if G is a finite group with identity e and an even number of elements, then there is $a \neq e$ in the group such that $a * a = e$.*

Proof. We are being asked to show that in a finite group with even order, there exists some element other than the identity which is it's own inverse.

Recall uniqueness of inverses and that for $g \in G$, $(g^{-1})^{-1} = g$. Thus for every element there exists one and only one element which is it's inverse. $e^{-1} = e$ is covered. In $G \setminus \{e\}$ there are an odd number of elements. Each of these have exactly one unique inverse meaning that there is one element "left" over which then necessarily has itself as it's inverse. □

Problem 6.2 (33, p.49). *Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a proof by mathematical induction that $(a * b)^n = a^n * b^n$ for all $a, b \in G$.*

Proof. Let $a, b \in G$. The base case where $n = 1$ is trivial so we proceed to our assumption that for any $k \in \mathbb{Z}^+$ we have $(a * b)^k = a^k * b^k$.

Let $n = k + 1$.

$$\begin{aligned}
(a * b)^n &= (a * b)^{k+1} \\
&= (a * b)^k * (a * b) \\
&= a^k * b^k * (a * b) && \text{by hypothesis} \\
&= a^k * (b^k * a) * b && \text{by associativity} \\
&= a^k * (a * b^k) * b && \text{by commutativity} \\
&= (a^k * a) * (b^k * b) \\
&= (a^{k+1}) * (b^{k+1}) \\
&= a^n * b^n
\end{aligned}$$

By the principle of mathematical induction we have that

$$(a * b)^n = a^n * b^n, \ \forall n \in \mathbb{Z}^+$$

□

Problem 6.3 (35, p. 49). *Show that if* $(a*b)^2 = a^2 * b^2$ *for* a, b *in a group, then* $a*b = b*a$.

Proof.

$$\begin{aligned}(a*b)^2 &= (a*b)*(a*b)\\ a^2*b^2 &= (a*a)*(b*b)\\ \Rightarrow (a*b)*(a*b) &= (a*a)*(b*b)\\ a*(b*a)*b &= a*(a*b)*b\end{aligned}$$

By one application each of left- and right cancellation we have

$$a*b = b*a$$

□

Problem 6.4 (41, p. 49). *Let* G *be a group and fix* $g \in G$. *Show that the map* i_g, *s.t.* $i_g(x) = gxg^{-1}$ *for* $x \in G$. *Show that* i_g *is an automorphism on* G.

Proof. Let $i_g : G \to G$ be defined as above. We need to show that it satisfies all the properties of an isomorphism.

It is clear, through left- and right cancellation, that i_g is injective.

Notice also that for any $x \in G$ we have the pre-image $g^{-1}xg$ since $i_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$, hence i_g is surjective.

Lastly we verify the homomorphism property:

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

completing the proof. □