Group Theory

Amit Rajaraman

December 2019

Contents

§1 Introduction to Groups

1.1 Definitions and Basics

Definition 1.1. A group G is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation such that

1. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$, that is, G is associative.
2. There exists an element e in G, which we call an *identity* of G, such that for all $g \in G$, $a * e = e * a = a$.
3. For each $g \in G$, there exists an element $g^{-1} \in G$ called an *inverse* of g such that $g * g^{-1} = g^{-1}g = e$.

We say that G is a group under $*$ if $(G, *)$ is a group. If $*$ is clear from context, we sometimes just say that G is a group.
We further say that G is a *finite group* if G is a finite set. Note that any group is nonempty.

Definition 1.2. We say that a group $(G, *)$ is *abelian* if $a * b = b * a$ for all $a, b \in G$.

Exercise 1.1. Show that $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Q}$ are abelian groups under the addition operation.

Exercise 1.2. Show that $\mathbb{Z} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ and $\mathbb{Q} \setminus \{0\}$ are abelian groups under the multiplication operation.

We define the set $\mathbb{Z}/n\mathbb{Z}$ for some integer n as follows. Let $\sim$ be an equivalence class given by

$$a \sim b \text{ if and only if } n \mid (b - a).$$

Each equivalence class is given by $\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$. There are precisely n equivalence classes, namely $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. These n equivalence classes are the elements of the set $\mathbb{Z}/n\mathbb{Z}$.
For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, we further define addition and multiplication as

$$\overline{a} + \overline{b} = \overline{a + b} \text{ and } \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

We see that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the addition operation with $e = \overline{0}$ and the inverse of $\overline{a}$ as $\overline{-a}$. We denote this group as $\mathbb{Z}/n\mathbb{Z}$.
Further, recall from number theory that a number a has a multiplicative inverse modulo n if and only if $(a, n) = 1$. We also see that the set of equivalence classes $\overline{a}$ which have multiplicative inverses modulo n is also an abelian group under multiplication. We denote this group as $(\mathbb{Z}/n\mathbb{Z})^\times$.

Definition 1.3. Let $(A, \star)$ and $(B, \diamond)$ be two groups. We can form a new group $A \times B$, called the *direct product* of A and B, whose elements are those in the cartesian product, and whose operation $\cdot$ is as follows.

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) \text{ for all } a_1, a_2 \in A, b_1, b_2 \in B$$

Theorem 1.1. Let G be a group under an operation $\star$. Then

1. The identity of G is unique.
2. For each $g \in G$, g^{-1} is unique.
3. For each $g \in G$, $(g^{-1})^{-1} = g$.
4. For any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how we bracket it. This is called the *generalized associative law.*
5. For $a, b \in G$, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Proof. We prove each of the parts of the theorem.

1. Let f and g be two identities of G. We have $f \star g = f$ and $f \star g = g$, which implies that $f = g$. Thus the identity of a group is unique.

2. Let $a, b \in G$ be two inverses of some $g \in G$. We have

$$\begin{aligned} a \star g &= b \star g \text{ where } e \text{ is the identity of } G \\ a \star g \star a &= b \star g \star a \\ a \star e &= b \star e \\ a &= b \end{aligned}$$

3. We have $g^{-1}g = gg^{-1} = e$ which implies that $(g^{-1})^{-1} = g$.

4. We leave this as an exercise to the reader. The idea is induction on n. First show the basis, then that any bracketing of k elements $g_1, \ldots, g_k$ can be reduced to $g_1 \star (g_2 \star (\cdots g_k)) \cdots)$. Next, argue that $a_1 \star a_2 \star \cdots \star a_n$ can be reduced to $(a_1 \star \cdots \star a_k) \star (a_{k+1} \star \cdots \star a_n)$ for some k. Apply the induction condition on each subproduct to complete the result.

5. Using the fourth result in this theorem on $(a \star b) \star (b^{-1} \star a^{-1})$ and $(b^{-1} \star a^{-1}) \star (a \star b)$ gives the required result.

■

Notation. Henceforth, for any group G under operation $\star$, we shall write $a \star b$ as ab unless it is needed that we mention it explicitly.
For some group G, $g \in G$ and $n \in \mathbb{Z}^+$, we write $xxx \cdots x$ (n times) as x^n.
We usually write the identity element of any group as 1.

Theorem 1.2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, $ax = bx$ if and only if $a = b$ and $ya = yb$ if and only if $a = b$.

Proof. Premultiplying and postmultiplying the two equations respectively and using the fact that inverses are unique gives the unique solution for x and y. ■

Definition 1.4. Let G be a group and $x \in G$. Let n be the smallest positive integer such that $x^n = 1$. This number is called the *order* of x and is denoted by $|x|$. If no positive power of x is the identity, x has order defined to be infinity and is said to be of infinite order.

Theorem 1.3. Any element of a finite group is of finite order.

Proof. Let $x \in G$. There are only finitely many distinct elements among $x, x^2, x^3, \ldots$. If $x^a = x^b$ for some integers a, b such that $b > a$, we have $x^{b-a} = 1$, that is, x is of finite order. ■

Example. In any group, the only element of order 1 is the identity. In the (additive) groups $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{C}$, any non-identity element is of order infinity. In $(\mathbb{Z}/7\mathbb{Z})^\times$, $\overline{2}$ is of order 3.

Definition 1.5. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* of G is an $n \times n$ matrix whose i, j element is $g_i g_j$.

This is a helpful way to understand the structure of any group.

Definition 1.6. Let G be a group under an operation $\star$. A subset H of G is called a *subgroup* of G if H also forms a group under the operation $\star$.

Example. $\mathbb{Q}$ is a subgroup of $\mathbb{R}$ under addition.

Exercise 1.3. If $x, g \in G$. Prove that $|x| = |gxg^{-1}|$. Deduce that $|ab| = |ba|$ for any $a, b \in G$.

Exercise 1.4. Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$, G is abelian.

Exercise 1.5. If x is an element of a group G, prove that $\{x^n \mid n \in \mathbb{N}\}$ is a subgroup of G. This subgroup is called the *cyclic subgroup* generated by x.

Exercise 1.6. If x is an element of infinite order in G, prove that $x^n, n \in \mathbb{Z}$ are all distinct. Deduce that if $x^i = x^j$ for some $i, j \in \mathbb{Z}, i \neq j$, x is of finite order.

Exercise 1.7. Let A, B be two groups and let $a \in A, b \in B$. Show that $(a, 1)$ and $(1, b)$ commute in $A \times B$. Further show that the order of (a, b) in $A \times B$ is the least common multiple of $|a|$ and $|b|$.

Exercise 1.8. Let $G = \{1, a, b, c\}$ be a group of order 4. If G has no elements of order 4, prove that there is a unique group table for G. Deduce that G is abelian. This group is called the *Klein four-group*.

1.2 Dihedral Groups

For each $n \in \mathbb{Z}^+$, $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon. A symmetry is any rigid motion of the n-gon which can be done by taking a copy of the polygon, moving it around in 3-dimensional space and superimposing it on the original polygon.
We can think of this as first labeling the n vertices as $1, 2, \ldots, n$ and describing each symmetry of the permutation σ of $\{1, 2, \ldots, n\}$ corresponding to this symmetry.
We make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s. That is, if s, t have corresponding permutations σ and τ, the permutation corresponding to st is $\sigma \circ \tau$.

To find the order of D_{2n}, we first observe, vertex 1 can go to any vertex $i, 1 \leq i \leq n$. Next, as 2 must remain adjacent to 1 even after applying the symmetry, it can go to either $i + 1$ or $i - 1$. As we have fixed the position of two of the vertices and the polygon is rigid, we have fixed the entire permutation. We have $n \times 2 = 2n$ possible permutations and so, the order of D_{2n} is $2n$.

This group is called the *dihedral group of order* $2n$.
These $2n$ symmetries are the n rotations by $2\pi i/n$ radians about the center for $i = 1, 2, \ldots, n$ and the n reflections about the n lines of symmetry.

Let r be the rotation symmetry that rotates the n-gon by $2\pi i/n$ radians and let s be the reflection symmetry that reflects the n-gon about the axis passing through vertex 1 and the origin.

Exercise 1.9. Prove the following.

1. $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
2. $|s| = 2$.
3. $s \neq r^i$ for any i.
4. $sr^i \neq sr^j$ for all $0 \leq i, j \leq n - 1, i \neq j$ so
$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}.$$
5. $rs = sr^{-1}$.
6. $r^i s = sr^{-i}$.

After doing the above exercise, we observe that all the elements of D_{2n} have a unique representation of the form $s^k r^i$ where $k = 0$ or 1 and $0 \leq i \leq n - 1$.

With the above expression of D_{2n} purely in terms of r and s as motivation, we introduce a new concept which can help in the expression of groups in a compact way.

Definition 1.7. We say that a subset S of a group G is a *set of generators* of G if every element in G can be written as a product of elements in S and their inverses. We indicate this by $G = \langle S \rangle$.

For example, $\mathbb{Z} = \langle \{1\} \rangle$.
Any equations in G that the generators satisfy are called *relations* in G. So in D_{2n}, we have the relations $r^n = 1, s^2 = 1$ and $rs = sr^{-1}$. It turns out that any relation in G can be deduced from these three relations. In general, if some group G is generated by a set S and there exist relations $R_1, R_2, \ldots, R_m$ such that any relation in G can be deduced from these relations, we shall call the generators and the relations together a *presentation* of G. We write
$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle.$$

For example,

$$D_{2n} = \langle \{r, s\} \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle.$$

Very often, given a presentation there is some non-obvious relation that can be deduced from the given relations.
There is in fact an (as of the time of writing, unsolved) problem called the *word problem* in groups, which asks for a way to determine whether two "words" (products of elements of the group and their inverses) are equal given a set of relations.

Exercise 1.10. Let

$$X_{2n} = \langle \{x, y\} \mid x^n = y^2 = 1, xy = yx^2 \rangle.$$

Show that if $n = 3k$, X_{2n} has order 6. (Note the similarity between X_{2n} and D_6 in this case.
Also show that if $(3, n) = 1$, then $x = 1$.

1.3 Symmetric groups

Let Ω be any nonempty set and S_Ω the set of all bijections from Ω to Ω (that is, all permutations). Make S_Ω a group under function composition. (Function composition is associative, the identity is the identity mapping on Ω and any bijection has an inverse)
In the case where $\Omega = \{1, 2, \ldots, n\}$, we denote S_Ω by S_n and call it the *symmetric group of order n*.
It is a simple combinatorial exercise to show that S_n has exactly $n!$ elements. We now describe a notation to write the elements of S_n, called the *cycle decomposition* of any permutation. A *cycle* is a string of integers that cyclically permutes the elements of this string (leaving all other integers fixed). So the cycle $(a_1\, a_2\, a_3\, \cdots\, a_k)$ sends a_1 to a_2, a_2 to a_3, …, a_{k-1} to a_k and a_k to a_1. In general, for any element of S_n can be rearranged and written as k (disjoint) cycles as

$$\sigma = (a_1\ a_2\ \cdots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \cdots\ a_{m_2}) \cdots (a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \cdots\ a_{m_k})$$

This notation is very easy to read as to determine what an element i is sent to, we just need to find the element written after i in the cycle decomposition.
Any permutation σ can also be easily written as its cycle decomposition using the following algorithm.

1. To start a new cycle, pick the smallest number in $\{1, 2, \ldots, n\}$ that has not appeared in a previous cycle. Call it a. Begin the new cycle $(a$.
2. Let $\sigma(a) = b$. If $b = a$, close with a parenthesis and return to step 1. If $b \neq a$, write b next to a so the cycle becomes $(ab$.
3. Let $\sigma(b) = c$. If $c = a$, close with a parenthesis and return to step 1. If $c \neq a$, write c next to b and repeat this step using c as b until the cycle closes.

Naturally this process gives the correct cycle decomposition. The *length* of a cycle is the number of integers which appear in it. A cycle of length l is called an l-cycle. We further adopt the convention that 1-cycles are not written. (So if some i does not appear in the cycle decomposition, it is understood that the permutation fixes i) The identity permutation is written as 1.
So the final step in the algorithm is to remove all 1-cycles.

Note that

$$(1\,3) \circ (1\,2) = (1\,2\,3) \text{ and } (1\,2) \circ (1\,3) = (1\,3\,2).$$

This shows that S_n is a non-abelian group for all $n \geq 3$.
Further, since disjoint cycles permute elements in disjoint sets, disjoint cycles commute.

Exercise 1.11. Let $\sigma = (1\,2\, \cdots\, m)$. Show that σ^i is also an m-cycle if and only if $(m, i) = 1$.

Exercise 1.12. Show that the order of an l-cycle in S_n is l. Deduce that the order of any element in S_n is the least common multiple of the lengths of the cycles in its cycle decomposition.

Exercise 1.13. Let p be a prime. Show that an element of S_n is of order p if and only if its cycle decomposition is a product of commuting p-cycles.

1.4 Matrix Groups

For the sake of understanding matrix groups, we define a field as follows.
A field is a set F together with two binary operations $+$ and $\cdot$ such that $(F, +)$ is an abelian group (call its identity 0) and $(F - \{0\}, \cdot)$ is an abelian group. Further,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ for all } a, b, c \in F.$$

For each $n \in \mathbb{Z}^+$, we define $GL_n(F)$ to be the set of all $n \times n$ matrices whose elements are elements of F and whose determinant is nonzero. $GL_n(F)$ is a group under matrix multiplication, and is called the *general linear group of order* n.
We have the following results (which we shall not prove in these notes).

1. if F is a finite field, then $|F| = p^m$ for some prime p and integer m.
2. if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.

Exercise 1.14. Let F be a field. Define

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in F \right\}$$

Prove that $H(F)$ is a group under matrix multiplication. This group is called the *Heisenberg group* over F.

1.5 Homomorphisms and Isomorphisms

We define homomorphisms and isomorphisms here, but shall discuss them much more in detail later on.

Definition 1.8. Let $(G, \star)$ and $(H, \diamond)$ be two groups. A map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \text{ for all } x, y \in G$$

is called a *homomorphism*.

The above condition is often compactly written as

$$\varphi(xy) = \varphi(x)\varphi(y).$$

Definition 1.9. Let G, H be two groups and $\varphi : G \to H$ be a homomorphism. The *kernel* of φ is defined as follows.

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$$

where 1_H is the identity element of H.

Definition 1.10. Let G, H be two groups. A map $\varphi : G \to H$ is called an *isomorphism* and we say G and H are isomorphic if φ is a homomorphism and φ is a bijection. If G and H are isomorphic, we write $G \cong H$.

Intuitively, two groups being isomorphic mean that they have the same structure.

Exercise 1.15. Show that the relation $\cong$ is an equivalence relation.

Example. The map $f : \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = e^x$ for all $x \in \mathbb{R}$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

Exercise 1.16. Let Ω and Δ be two finite sets. Show that $S_\Omega \cong S_\Delta$ if and only if $|\Omega| = |\Delta|$.

Isomorphisms are extremely useful in the study of abstract structures such as groups because if we want to study some group, it will do equally well to study a group that is isomorphic to this one.

Exercise 1.17. Let G and H be two groups and $\varphi : G \to H$ be an isomorphism. Then prove that

1. if G and H are finite, $|G| = |H|$.

2. G is abelian if and only if H is abelian.

3. for all $x \in G$, $|x| = |\varphi(x)|$.

We can deduce from the third part of the above exercise that $(\mathbb{R}, +)$ is not isomorphic to $(\mathbb{R}, \times)$ as -1 is of order 2 in $(\mathbb{R}, \times)$ but there is no element of order 2 in $(\mathbb{R}, +)$.

Exercise 1.18. Prove that $(\mathbb{R} - \{0\}, \times)$ is not isomorphic to $(\mathbb{C} - \{0\}, \times)$.

Exercise 1.19. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Exercise 1.20. Let G, H be groups and $\varphi : G \to H$ be a homomorphism. Prove that the image of G under φ is a subgroup of H.

1.6 Group Actions

We define group actions here, but shall discuss them much more in detail later on.

Definition 1.11. A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$ for all $g \in G, a \in A$) such that

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$.

2. $1 \cdot a = a$ for all $a \in A$.

We say that G is a group acting on the set A in the above definition.
More precisely, this is called a *left* group action. We have a similar notion of a *right* group action.

Theorem 1.4. For some fixed $g \in G$, consider the map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$. Then σ_g is a permutation of A. Further, the map $G \to S_A$ given by $g \mapsto \sigma_g$ is a homomorphism.

Proof. Consider $\sigma_{g^{-1}} : A \to A$. We shall show that $\sigma_{g^{-1}}$ is an inverse of σ_g. To see this, note that

$$\sigma_{g^{-1}} \circ \sigma_g(a) = g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = 1 \cdot a = a \text{ for all } g \in G$$

so $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map on A. Similarly, $\sigma_g \circ \sigma_g^{-1}$ is also the identity map on A. As σ_g has a two-sided inverse, it is a bijection and thus a permutation of A.
To see that the given map is a homomorphism, note that

$$\sigma_{g_1} \circ \sigma_{g_2}(a) = g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a = \sigma_{g_1 g_2}(a) \text{ for all } g_1, g_2 \in G, a \in A.$$

and $1 \cdot a = a$ for all $a \in A$. ∎

Definition 1.12. Let a group G act on a set A. We define the kernel of the group action as

$$\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$$

Note that any group acts on itself by the group operation itself. This action is called the *left regular action* of G on itself.
If a group G acts on a set A and distinct elements of G induce distinct permutations, the action is said to be *faithful*.

§2 Subgroups

2.1 Definitions and Basics

Although we have defined subgroups in section 1, we repeat the definition here.

Definition 2.1. Let G be a group. A subset H of G is a subgroup of G if H is nonempty and it is closed under products and inverses. That is, $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$. If H is a subgroup of G, we write $H \leq G$.

If $H \leq G$ and $H \neq G$, we write $H < G$.

Example. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ under the operation of addition.
If $G = D_{2n}$, $H = \{1, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of G.

Note that the relation $\leq$ is transitive. That is, if $K \leq H$ and $H \leq G$, then $K \leq G$.

Theorem 2.1 (Subgroup Criterion)**.** A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$.
2. for all $x, y \in H$, $xy^{-1} \in H$.

Further, if H is finite, then it suffices to check that H is nonempty and is closed under multiplication.

Proof. If $H \leq G$, the two given statements clearly hold as H contains the identity of G and is closed under inverses and multiplication.
To prove the converse, let x be any element of H (which exists as $H \neq \emptyset$). We have $xx^{-1} \in H \implies 1 \in H$. As H contains 1, for any element h of H, H contains $1h^{-1} = h^{-1}$, that is, it is closed under inverses. For any x and y in H, as $y^{-1} \in H$, we have that $x(y^{-1})^{-1} = xy \in H$, that is, H is closed under multiplication.
To prove the second part, we see that $x, x^2, x^3, \ldots \in H$ for any $x \in H$. Using 1.3, we see that x is of finite order n. Then $x^{-1} = x^{n-1} \in H$ so H is closed under inverses. ■

Exercise 2.1. Let G be a group and H, K be subgroups of G. Show that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

Exercise 2.2. Let G be a group and H, K be subgroups of G. Show that $H \cap K$ is also a subgroup of G.

Exercise 2.3. Let G be a group. Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G.

Exercise 2.4. Let G be a group of order $n > 2$. Show that G cannot have a subgroup H of order $n - 1$.

Exercise 2.5. Let G be a group. Let $H = \{g \in G \mid |g| < \infty\}$. Show that $H \leq G$ if G is abelian. In this case, H is called the *torsion subgroup* of G. Give an example where G is non-abelian and H is not a subgroup of G.

Exercise 2.6. Let H be a subgroup of $\mathbb{Q}$ under addition with the property that $\frac{1}{x} \in H$ for every nonzero $x \in H$. Show that $H = \{0\}$ or $\mathbb{Q}$.

2.2 Centralizers, Normalizers, Stabilizers and Kernels

We now introduce some important subgroups.

Definition 2.2. Let G be a group and A be any nonempty subset of A. Define

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

This subset is called the *centralizer* of A in G.

Since $gag^{-1} = g$ if and only if $ga = ag$, $C_G(A)$ is the set of all elements that commute with every element of A.
Now observe that $C_G(A)$ is a subgroup of G as first of all, $1 \in C_G(A)$ so $C_G(A) \neq \emptyset$, and second of all, if $x, y \in C_G(A)$, we have $xax^{-1} = a$ and $yay^{-1} = a$, that is, $y^{-1}ay = a$ for all $a \in A$. We then have $a = xax^{-1} = x(y^{-1}ay)x^{-1} = (xy^{-1})a(xy^{-1})^{-1}$ so $xy^{-1} \in C_G(A)$. Thus, $C_G(A) \leq G$.

Definition 2.3. Let G be a group. Define

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

This subset is called the *center* of G.

$Z(G)$ is the set of all elements that commute with every element of G.
As $Z(G) = C_G(G)$, we have $Z(G) \leq G$.

Definition 2.4. Let G be a group and A be a subset of G. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

This set is called the *normalizer* of A in G.

The proof that $N_G(A) \leq G$ is similar to that we used to prove that $C_G(A) \leq G$.
Note that $C_G(A) \leq N_G(A)$.

If G is an abelian group, $Z(G) = G$. Further, for any subset A of G, $N_G(A) = C_G(A) = G$ as $gag^{-1} = gg^{-1}a = a$ for all $a \in A, g \in G$.

Exercise 2.7. Show that the center of D_8 is $\{1, r^2\}$.

The fact that centralizers and normalizers are subgroups is in fact a special case of a results in group actions. We now introduce stablizers and kernels of group actions.

Definition 2.5. Let G be a group that acts on a set S. Let $s \in S$ be some fixed elements. Define

$$G_s = \{g \in G \mid g \cdot s = s\}$$

We shall now show that $G_s \leq G$. First of all, $1 \in G_s$ by the definition of a group action. If $x, y \in G_s$, we have

$$\begin{aligned} s &= 1 \cdot s \\ &= (x^{-1}x) \cdot s \\ &= x^{-1} \cdot (x \cdot s) \\ &= x^{-1} \cdot s \end{aligned}$$

so $x^{-1} \in G_s$ and

$$\begin{aligned} (xy) \cdot s &= x \cdot (y \cdot s) \\ &= x \cdot s \\ &= s \end{aligned}$$

We see that G_s is nonempty and is closed under inverses and multiplication. It is thus a subgroup of G.
Recall the definition of a *kernel* of an action, 1.12. Using 2.3 and the fact that $G_s \leq G$ for all $s \in S$ yields the result that the kernel of any group action is a subgroup of the group.

We now see that $C_G(A)$ is merely the kernel of the group action of G acting on A as $g \cdot a = gag^{-1}$ (so it is a subgroup of G) and $N_G(A)$ is the stabilizer of the group action of G acting on $\mathcal{P}(A)$ (the power set of A) as $g \cdot A = gAg^{-1}$ (so it is a subgroup of G).

Exercise 2.8. Prove that $C_G(Z(G)) = N_G(Z(G)) = G$.

Exercise 2.9. Prove that $H \leq N_G(H)$ for a subgroup H of a group G.

Exercise 2.10. For any subgroup H of group G and subset A of G, define $N_H(A) = \{h \in H \mid hAh^{-1} = A\}$. Prove that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A) \leq N_G(A)$.

Exercise 2.11. Let F be a field and the Heisenberg group $H(F)$ be defined as in 1.14. Determine $Z(H(F))$ and prove that $Z(H(F)) \cong (F, +)$.

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.6. A group H is *cyclic* if there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$.

In this case we write $H = \langle x \rangle$ and say that H is *generated* by x and x is a generator of H. The generator of a cyclic group need not be unique (as if x is a generator, so is $-x$).
Note that any cyclic group is abelian.

Example. The group $(\mathbb{Z}, +)$ is generated by 1 (here 1 is the integer 1 and not the identity).

Theorem 2.2. Let $H = \langle x \rangle$. Then $|H| = |x|$ (where if one side of the inequality is infinite, so is the other).

Proof. This proof is trivial and is left as an exercise to the reader. ■

It is observed that there is a great deal of similarity between $H = \langle x \rangle$, where $|x| = n$, and $\mathbb{Z}/n\mathbb{Z}$. Both of them appear to have very similar structure. It turns out that these two groups are isomorphic, which we shall prove shortly. First, let us prove the following.

Theorem 2.3. Let G be an arbitrary group, $x \in G$, and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x| \mid m$.

Proof. By the Euclidean algorithm, there exist integers r and s such that $d = mr + ns$. We have

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1.$$

This proves our first claim.
Next, let $n = |x|$ and $x^m = 1$. We have x^d=1, where $d = (|x|, m)$. Note that $0 < d \leq |x|$ and $|x|$ is the smallest positive integer k such that $x^k = 1$. This implies that $d = |x|$ and $|x| = (|x|, m)$. Thus, $|x| \mid m$. ■

Theorem 2.4. Any two cyclic groups of the same order are isomorphic. More specifically,

1. if $n \in \mathbb{Z}^+$ and $H = \langle x \rangle$ and $K = \langle y \rangle$ are both of order n, $H \cong K$.
2. if $\langle x \rangle$ is an infinite cyclic group, $(\mathbb{Z}, +) \cong \langle x \rangle$.

Proof. Let $\langle x \rangle$ and $\langle y \rangle$ be two cyclic groups of finite order n. Let $\varphi : \langle x \rangle \to \langle y \rangle$ be defined by $\phi(x^k) = y^k$. Let us first prove that φ is well defined, that is, if $x^a = x^b$, then $\varphi(x^a) = \varphi(x^b)$. If $x^a = x^b$, $x^{b-a} = 1$ and 2.3 implies that $n \mid b - a$. Let $b = a + tn$ so $\varphi(x^b) = \varphi(x^{a+tn}) = y^{a+tn} = (y^n)^t y^a = y^a = \varphi(x^a)$. Thus φ is well-defined. φ is a homomorphism as $\varphi(x^a)\varphi(x^b) = y^a y^b = y^{a+b} = \varphi(x^a x^b)$. φ is injective as any element y^a of $\langle y \rangle$ is the image of x^a. As φ is a surjection between two sets of equal finite order, it is a bijection and φ is an isomorphism.

Let $\langle x \rangle$ be an infinite cyclic group. Consider the map $\varphi : (\mathbb{Z}, +) \to \langle x \rangle$ given by $\varphi(k) = x^k$ for $k \in \mathbb{Z}$. This function is a homomorphism as $\varphi(a)\varphi(b) = x^a x^b = x^{a+b} = \varphi(a + b)$. Since $x^a \neq x^b$ for $a \neq b$, φ is an injection. As any element $x^a \in \langle x \rangle$ is the image of $a \in \mathbb{Z}$, φ is a surjection. Thus φ is a bijection and an isomorphism. ■

For each $n \in \mathbb{Z}^+$, let $\mathbb{Z}_n$ be the cyclic group of order n. $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Theorem 2.5. Let G be a group, $x \in G$ and $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, $|x^a| = \infty$.

2. If $|x| = n < \infty$, $|x^a| = \frac{n}{(n,a)}$.

Proof.

1. On the contrary, let $|x^a| = k < \infty$. Then $(x^a)^k = x^{ak} = 1$. Also $x^{-ak} = 1$. Since one of ak and $-ak$ must be positive, some positive power of x is 1, which contradicts the fact that $|x| = \infty$. Thus, $|x^a| = \infty$.

2. Let $y = x^a, d = (n,a), a = bd$ and $n = cd$ for some $b, c \in \mathbb{Z}$. We must show that $|y| = c$. We have $y^c = (x^a)^c = (x^{bd})^c = (x^{cd})^b = (x^n)^b = 1$. 2.3 implies that $|y| \mid c$. We also have $x^{a|y|} = 1$ which implies that $|x| \mid a|y|$. This gives $cd \mid bd|y|$, that is, $c \mid b|y|$. However, since $(b,c) = 1$, we have $c \mid |y|$. As $|y| \mid c$ and $c \mid |y|$, $|y| = c$.

■

Corollary 2.6. A corollary of the second part of the above theorem is that if $a \mid n$, $|x^a| = \frac{n}{a}$.

Exercise 2.12. Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a,n) = 1$.

Proof. We have that x^a generates a group of order $|x^a|$. This subgroup equals H if and only if $|x^a| = |x|$, that is, $\frac{n}{(a,n)} = n$. This is equivalent to $(a,n) = 1$. ■

This implies that the total number of generators of a cyclic group of order n is $\varphi(n)$, where φ is Euler's totient function.

Theorem 2.7. Let $H = \langle x \rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

2. If $|H| = \infty$, then for distinct nonnegative integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$. Also, $\langle x^m \rangle = \langle x^{|m|} \rangle$ so the nontrivial subgroups of H are in bijection with $\mathbb{N}$.

3. If $|H| = n < \infty$, then for each positive integer a dividing n, there is a unique subgroup of H of order a, namely $\langle x^{n/a} \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$. (So the subgroups of H are in bijection with the positive integers of n)

Proof.

1. Let d be the smallest positive integer such that $x^d \in K$. As K is a group, $x^k d \in K$ for any $k \in \mathbb{Z}$. Let $x^a \in K$ for some $a \in \mathbb{Z}$. Write $a = qd + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Then $x^r = x^a x^{-qd} \in K$ as K is a group. However, by the minimality of d and the fact that $0 \leq r < d$, we get $r = 0$. As d divides any a such that $x^a \in K$ and $\langle x^d \rangle \leq K$, we have $K = \langle x^d \rangle$.

2. This proof is similar to that of the third part so we leave it as an exercise to the reader.

3. Use 2.6 to get that $|x^{n/a}| = a$, which gives that $\langle x^{n/a} \rangle$ is of order a. We must now prove that this is the unique subgroup of order a. Let $b \in \mathbb{Z}$ such that $\langle x^b \rangle$ is of order a. We have that the order of $\langle x^b \rangle$ is equal to $|x^b|$ from 2.2. Using 2.5 gives $a = \frac{n}{(n,b)}$ so $\frac{n}{a} = (n,b)$. In particular, $\frac{n}{a} \mid b$. This implies that $\langle x^b \rangle \leq \langle x^{\frac{n}{a}} \rangle$. However, since they are of equal finite order, $\langle x^b \rangle = \langle x^{\frac{n}{a}} \rangle$ and $\langle x^{\frac{n}{a}} \rangle$ is the unique subgroup of order a.

■

Exercise 2.13. Let p be a prime and $n \in \mathbb{Z}^+$. Show that if x is an element of a group G such that $x^{p^n} = 1$, then $|x| = p^m$ for some $m \leq n$.

Exercise 2.14. Prove that $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are not cyclic.

Exercise 2.15. Let G be a group and $x \in G$. Prove that $g \in N_G(\langle x \rangle)$ if and only if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

Exercise 2.16. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.