Algebra I

Dhyan Laad
2024ADPS0875G

Contents

1 Preliminaries

1.1 The Natural Numbers

We start by covering a few basic and useful properties of the natural numbers, which in this text does not include 0. Stated below is an axiom reffered to as the *well ordering principle* (WOP).

Every nonempty subset of the natural numbers has a least element.

Note that the WOP holds trivially for any finite extension to $\mathbb{N}$. Now from it, it is possible to prove the *principle of mathematical induction* (PMI).

Theorem 1.1 (Principle of Mathematical Induction). *For a set $S \subseteq \mathbb{N}$, if*

(a) $1 \in S$, *and*

(b) *for every $k \in \mathbb{N}$, $k \in S \Rightarrow k+1 \in S$,*

then $S = \mathbb{N}$.

Proof. Assume for contradiction that $S \neq \mathbb{N}$. This implies that there must exist natural numbers not in S. Define

$$C = \mathbb{N} \setminus S.$$

By construction, C is nonempty, which means by the WOP, C must have a least element m.

Since $1 \in S$ and $m \in C$, $m \neq 1$, which means that $m > 1$. This means that $m-1$ is a natural number, and since m is the smallest element of C, $m-1$ must be in S. By (b), since $m-1 \in S$, it must be the case that $m \in S$ ($\Rightarrow\Leftarrow$). Since m cannot be in both S and C, the assumption that $S \neq \mathbb{N}$ must be false. □

This theorem is sometimes referred to as *weak induction*. Ironically, *strong induction* follows from the standard PMI.

Theorem 1.2 (Principle of Strong Induction). *For a set $S \subseteq \mathbb{N}$, if*

(a) $1 \in S$, *and*

(b) *for every $k \in \mathbb{N}$, $\{1, 2, \ldots, k\} \subseteq S \Rightarrow k+1 \in S$,*

then $S = \mathbb{N}$.

It is also possible to axiomatize the PMI and derive the WOP from it. The proof is done by proving the contrapositive statement: if a set S has no least element, then S is empty.

Definition 1.3. Let $a, b \in \mathbb{Z}$. We say that *a divides b* if there exists $c \in \mathbb{Z}$ such that

$$b = ac$$

and symbolically write $a \mid b$.

Now for another fundamental result in elementary number theory.

Theorem 1.4 (Division Lemma). *For any $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

Proof. Define the set

$$S = \{a - xb : x \in \mathbb{Z} \text{ and } a - xb \geq 0\}.$$

Set $x = -|a|$. Then,

$$a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

Therefore, S is nonempty. Since S is also a subset of $\mathbb{N}$, by an extension of the WOP to admit 0, S has a least element $r \geq 0$. Thus,

$$r = a - qb$$

for some $q \in \mathbb{Z}$. We now assert that $r < b$.

Assume for contradiction that $r \geq b$. Then,

$$r - b = (a - qb) - b = a - (q + 1)b \geq 0.$$

This means that $r - b$ is an element of S ($\Rightarrow\!\!\!\!\!\!\not\leq$), which contradicts the fact that r is the least element of S. Therefore, $r < b$.

We also prove the uniqueness of q and r by contradiction. Assume that there exist integers q' and r' different from q and r respectively such that

$$a = qb + r = q'b + r'$$

with $0 \leq r, r' < b$. Rearranging the above expression, we have

$$(q - q')b = r' - r \Rightarrow |q - q'||b| = |r' - r|.$$

Now,

$$q \neq q' \Rightarrow |q - q'| \geq 1 \Rightarrow |r' - r| \geq |b| \qquad (\Rightarrow\!\!\!\!\!\!\not\leq)$$

which contradicts our assumed bounds on r and r'. As such, q and r must be unique. □

Definition 1.5. The *greatest common divisor* (gcd) of two nonzero integers a and b is the unique positive integer d such that

(a) $d \mid a$ and $d \mid b$, and

(b) if $c \mid a$ and $c \mid b$ for some $c \in \mathbb{Z}$, then $c \mid d$.

Symbolically, $d = (a, b)$.

Equivalently, the gcd of two integers a and b is the largest integer that divides them. The *Euclidean algorithm* (described below) employs the division lemma to find the gcd of two arbitrary integers, along with a proof of termination.

Theorem 1.6 (Euclidean Algorithm). *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exist integers q_i and r_i for $i \in 1:k$ such that*

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < b, \\ b &= r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ &\vdots & \vdots \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 \leq r_k < r_{k-1}, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

Then $(a, b) = r_k$.

Step 1. Divide a by b to obtain

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

Step 2. If $r_1 = 0$, then $(a, b) = b$. Otherwise, divide b by r_1 to get

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

Step 3. Continue dividing the previous divisor by the remainder until a remainder of 0 is obtained.

Conclusion. The last nonzero remainder r_k is (a, b).

Proof. All of the remainders are nonnegative integers:

$$b > r_1 > r_2 > \cdots > r_{k-1} > r_k > 0.$$

By the WOP, $\mathbb{N}$ cannot contain an infinite strictly decreasing sequence, which means the algorithm must terminate after a finite number of steps, with the last remainder being 0. □

Now for a final result on the properties of natural numbers

Theorem 1.7 (Bézout's Lemma). *Let a and b be nonzero integers. Then, there exist integers x and y such that*

$$ax + by = (a, b).$$

Furthermore, (a, b) is the smallest positive integer that can be written in this form.

Proof. Define the set

$$S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

If $a > 0$, then $a \cdot 1 + b \cdot 0 = a \in S$ and if $a < 0$, then $a \cdot (-1) + b \cdot 0 = -a \in S$. If $a = 0$, then b can be similarly picked to match the sign of y for the linear combination to be positive, which means the set is nonempty.

Since the set is nonempty, by the WOP let d be the least element in S. As such, there exist integers x_0 and y_0 such that

$$d = ax_0 + by_0. \tag{$*$}$$

Now, by the division lemma, we know that there exist integers q and r such that

$$a = dq + r \tag{$**$}$$

where $0 \leq r < d$. From $(*)$ and $(**)$, we have

$$r = a - dq = a - (ax_0 + by_0)q \Rightarrow r = a(1 - x_0q) + b(-y_0q).$$

Now note that r must be 0, since if it were not, then it would be an element of S, which is not possible since $r < d$, which contradicts the fact that d is the least element of S. Since $r = 0$, it follows that $a = dq \Rightarrow d \mid a$, and by the same flow of thought, $d \mid b$.

Let c be an arbitrary divisor of a and b, i.e. there exist integers k and ℓ such that $a = ck$ and $b = c\ell$. To show that $d = (a, b)$, c must also divide d.

$$d = ax_0 + by_0 = (ck)x_0 + (c\ell)y_0 = c(kx_0 + \ell y_0) \Rightarrow c \mid d.$$

□

1.2 Relations

Definition 1.8. Let X be a set. A relation R on X is a subset of the Cartesian product

$$X \times X = \{(x, y) : x, y \in X\}.$$

If $(x, y) \in R$, we say that x *is related to* y *by* R. Symbolically

$$xRy,$$

and if there is no ambiguity in the relation, then it is common to write $x \sim y$.

We now discuss a few proprties that a relation may possess.

Definition 1.9. Let X be a set and $\sim$ be a relation on X. The relation is

(a) *reflexive* if $x \sim x$ for all $x \in X$,

(b) *symmetric* if $x \sim y \Rightarrow y \sim x$ for all $x, y \in X$, and

(c) *transitive* if $x \sim y$ and $y \sim z$ imply that $x \sim z$ for all $x, y, z \in X$.

Definition 1.10. A relation that is reflexive, symmetric, and transitive is said to be an *equivalence relation.*

Example 1.11. Let $n \in \mathbb{N}$ with $n \geq 2$. Define a relation $\sim$ on $\mathbb{Z}$ by

$$x \sim y \Leftrightarrow x \text{ and } y \text{ give the same remainder when divided by } n,$$

or symbolically

$$x \sim y \Leftrightarrow n \mid (x - y).$$

Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

Solution. We need only show that the three properties hold.

Reflexivity. For any $x \in \mathbb{Z}$, we have that $x - x = 0$, and since $n \mid 0$, it follows that $x \sim x$.

Symmetry. If $x \sim y$, then $n \mid (x-y) \Rightarrow x-y = nk$ for some $k \in \mathbb{Z}$. Now, $y-x = n(-k) \Rightarrow n \mid (y-x)$, and as such $y \sim x$.

Transitivity. If $x \sim y$ and $y \sim z$, then there exist integers k and ℓ such that $x - y = nk$ and $y - z = n\ell$. Therefore $x - z = (x - y) + (y - z) = n(k + \ell) \Rightarrow n \mid (x - z)$.

■

Definition 1.12. Let $\sim$ be an equivalence relation on a set X. For $x \in X$, the *equivalence class of* x is defined by

$$[x] = \{y \in X : x \sim y\}.$$

The set of all equivalence classes is denoted by

$$X/\sim = \{[x] : x \in X\}.$$

Note that the set of all equivalence classes of the relation in Example 1.11 is denoted by $\mathbb{Z}_n$ for a fixed $n \in \mathbb{N}$.

Definition 1.13. A *partition* of a set X is a collection of nonempty disjoint subsets of X whose union is X.

Theorem 1.14. *The equivalence classes of an equivalence relation on a set X form a partition of X. Conversely, given a partition of X, there exists an equivalence relation whose equivalence classes are exactly the elements of the partition.*

Proof. ($\Rightarrow$) Suppose $\sim$ is an equivalence relation on X. Since $\sim$ is reflexive, $x \in [x]$ for every $x \in X$, which means that all equivalence classes are nonempty. Furthermore, for any $x \in X$, it holds that $x \in [x]$, which means that

$$\bigcup_{x \in X} [x] = X.$$

To show that the equivalence classes are disjoint, assume for contradiction that there exist unique $[x]$ and $[y]$ such that $[x] \cap [y] \neq \varnothing$. Therefore, there exists an element z of X common to both $[x]$ and $[y]$, i.e. $z \sim x$ and $z \sim y$. By symmetry and transitivity, $x \sim y \Rightarrow [x] = [y]$ ($\Rightarrow\!\Leftarrow$) which contradicts the assumption that $[x] \neq [y]$. As such, equivalence classes are disjoint.

($\Leftarrow$) Given a partition of S, define $a \sim b$ iff a and b are in the same subset. Reflexivity, symmetry, and transitivity trivially hold. □

2 Introduction to Groups

A group is a fundamental algebraic structure that generalizes concepts such as symmetry, permutations, and transformations by abstracting their properties into a set with an operation defined on that set. The formal definition follows.

Definition 2.1. A *group* is an ordered pair $(G, *)$ where G is a set and $*$ is an operation

$$\cdot * \cdot : G \times G \to G$$

such that the following properties hold.

Associativity. For all $a, b, c \in G$,

$$(a * b) * c = a * (b * c).$$

Identity. There exists an element $e \in G$ such that for all $a \in G$,

$$a * e = e * a = a.$$

Inverse. For every $a \in G$, there exists an element $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

It is common to refer to the group by the name of the set, and when the operation may be inferred, to notate it by simple juxtaposition: $a * b \equiv ab$.

Definition 2.2. An *Abelian group* is a group on which the operation is commutative. That is, for a group G

$$ab = ba$$

for all $a, b \in G$.

Example 2.3. Verify that the set $\{1, -1, i, -i\} \subset \mathbb{C}$ under multiplication forms an Abelian group.

Solution. Before proving the three properties, it is of importance to note that the operation maps into the set, i.e. the group is *closed* under the operation, which in our case, it is.

Associativity & Commutativity. Since the complex numbers are associative and commutative, this property carries forward to a subset.

Identity. Clearly, 1 is the identity element since $1 \cdot z = z$ for all $z \in \mathbb{C}$.

Inverse. Since $1 \cdot 1 = i \cdot (-i) = -1 \cdot (-1) = 1$, all elements have an inverse element.

■

Example 2.4. Show that the set $S = \{1\} \cup (\mathbb{R} \setminus \mathbb{Q})$ under mutliplication *does not* form a group.

Solution. Note that $\sqrt{2} \cdot \sqrt{2} = 2 \notin S$. Since the group operation is not closed, S does not form a group under multiplication. ■

2.1 Arithmetic Modulo n

It is possible to define arithmetic operations on $\mathbb{Z}_n$ as follows for $[a], [b] \in \mathbb{Z}_n$:

$$[a] +_n [b] = [a + b],$$
$$[a] \times_n [b] = [ab].$$

These operations are called *addition modulo n* and *multiplication modulo n* respectively. For brevity, we may write $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ while working with arithmetic operations modulo n. It is now possible to define groups surrounding the set, as follows.

Theorem 2.5. *The set $\mathbb{Z}_n$ is a group under addition modulo n.*

The proof for the theorem is trivial and has been omitted.

Theorem 2.6. *The set $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n iff n is a prime number.*

Proof. ($\Rightarrow$) We prove the forward direction by contraposition. Let n be a composite number. By definition, there exist natural numbers $a, b < n$ such that

$$n = ab \Rightarrow a \times_n b = 0,$$

which means the operation is not closed, and therefore n must be a prime number.

($\Leftarrow$) We must now prove that if $n = p$ is a prime number, then the set is a group. Firstly, the identity element is 1 since $1 \times_p a = a$ for all $a \in \mathbb{Z}_p^*$. The operation is also closed since for any nonidentity elements a and b, their product cannot be a multiple of a prime number. Therefore, $a \times_p b \neq 0$. Since the multiplication of integers is associative, the property is also inherited by modular arithmetic.

To prove the existence of the inverse, apply Bézout's lemma on $a \in \mathbb{Z}_p^*$ and p. There exist integers x and y such that

$$ax + py = 1 \Rightarrow [ax + py] = [1] \Rightarrow a \times_p [x] = 1.$$

Therefore, there always exists an inverse for an arbitrary element of $\mathbb{Z}_p^*$. □

It is possible to generalize this theorem.

Theorem 2.7. *Let $U(n)$ be the set of integers less than n that are relatively prime to n. Then, $U(n)$ is a group with respect to multiplication modulo n.*

The proof for the theorem proceeds identically to that of Theorem 2.6.

2.2 Elementary Properties of Groups

We first define some useful notation.

Definition 2.8. Let G be a group, then we define

$$a^n = \underbrace{aa\cdots a}_{n \text{ times}}$$

for $n \in \mathbb{N}$ and $a^0 = e$ for all $a \in G$ with identity element e. Similarly,

$$a^{-n} = (a^{-1})^n = \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}}.$$

From this, our regular laws of exponents with integer powers follow.

Theorem 2.9. *The identity element of a group is unique.*

Proof. Assume for contradiction that there are two distinct identity elements e and e'. Then, for all $a \in G$,

$$ae = ea = a \quad \text{and} \quad ae' = e'a = a.$$

Let $a = e'$ in the first equation and $a = e$ in the second equation. Then,

$$e'e = ee' = e' \quad \text{and} \quad ee' = e'e = e.$$

This implies that $e = e'$ $(\Rightarrow\Leftarrow)$ which contradicts the assumption that the elements were distinct. Therefore, the identity element is unique. □

Theorem 2.10 (Cancellation Laws). *Let G be a group. Then,*

$$ba = ca \Rightarrow b = c \quad \textit{and} \quad ab = ac \Rightarrow b = c$$

for all $a, b, c \in G$.

These are referred to as right and left cancellation respectively. The proof for the theorem is trivial and has been omitted.

Theorem 2.11. *The inverse of each element in a group is unique.*

Proof. Let G be a group and $a \in G$. Assume for contradiction that there exist two distinct inverse elements b and c for a. Then,

$$ab = ba = e \quad \text{and} \quad ac = ca = e,$$

where e is the identity element. Now,

$$ab = e \Rightarrow cab = ce \Rightarrow b = c. \qquad (\Rightarrow\Leftarrow)$$

This contradicts the assumption that b and c are distinct. As such, the inverse is unique. □

Theorem 2.12. *Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof.

$$(ab)^{-1}ab = e \Rightarrow (ab)^{-1}abb^{-1}a^{-1} = eb^{-1}a^{-1} \Rightarrow (ab)^{-1} = b^{-1}a^{-1}.$$

□

Definition 2.13. The cardinality of the set of a group, i.e. the number of elements in it, is called its *order*. It is denoted by $|G|$ or $\mathrm{ord}(G)$.

Definition 2.14. Let G be a group and $a \in G$. The smallest natural number n for which a^n equals the identity element is called the *order of* a, and is denoted by $\mathrm{ord}(a)$. If no such n exists, a is said to have *infinite order*.

Now for a few preliminary results related to orders of groups and their elements.

Theorem 2.15. *Let G be a group and $a \in G$. Then,* $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$.

Proof. First, consider the case of a having a finite order n, i.e. $a^n = e$, where e is the identity. Now,

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$$

Since raising the inverse of a to the power of n also results in the identity, the order of a^{-1} cannot exceed n:

$$\mathrm{ord}(a^{-1}) \leq n.$$

Now, let $\mathrm{ord}(a^{-1}) = m$. By definition, $(a^{-1})^m = e$, and

$$(a^{-1})^m = a^{-m} = (a^m)^{-1} = e \Rightarrow a^m = e.$$

Therefore, the order of a must be less than or equal to m.

Since $n \leq m$ and $m \leq n$, it must be the case that $m = n$:

$$\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$$

for all $a \in G$.

In the case that the order is infinite, we proceed with contradiction. Suppose a has infinite order, but a^{-1} has a finite order n. Then,

$$(a^{-1})^k = e \Rightarrow a^{-k} = e \Rightarrow a^k = e \qquad (\Rightarrow\Leftarrow)$$

which implies that a has an order not exceeding k. Therefore, if one is infinite, the other one must be too. □

Theorem 2.16. *Let G be a group, $a \in G$,* $\mathrm{ord}(a) = d$, *and $k \in \mathbb{N}$. Then,*

$$\mathrm{ord}(a^k) = \frac{d}{(k, d)}$$

Proof. The order of a^k would be the smallest positive integer m such that $(a^k)^m = e$, where e is the identity. For any $n \in \mathbb{N}$, $a^n = e$ only if n is a multiple of $\text{ord}(a)$. Therefore,

$$(a^k)^m = a^{km} = e \Leftrightarrow d \mid km.$$

To find the smallest positive integer m such that km is a multiple of d, we require km to be the least common multiple of k and d:

$$km = \text{lcm}(k, d).$$

We also know that $kd = (k, d) \cdot \text{lcm}(k, d)$. Therefore,

$$m = \frac{d}{(k, d)}.$$

□

We also state one final theorem without proof (for now).

Theorem 2.17. *Let G be a group. Then,*

$$\text{ord}(a) \mid \text{ord}(G)$$

for all $a \in G$.

2.3 Subgroups

Definition 2.18. A nonempty subset H of a group G is said to be a *subgroup* of G if is a group under the same binary operation. Symbolically,

$$H \leq G.$$

If H is a proper subset of G, then we say that it is a *proper subgroup* and is notated by $H < G$. The identity element by itself forms the *trivial subgroup*.

We now present some tests to ascertain whether a given subset of the group forms a subgroup.

Theorem 2.19 (Two-Step Subgroup Test). *Let H be a nonempty subset of a group G and $a, b \in G$. If*

(a) *$a, b \in H \Rightarrow ab \in H$, and*

(b) *$a \in H \Rightarrow a^{-1} \in H$,*

then $H \leq G$.

This test may also be condensed into a single condition.

Theorem 2.20 (One-Step Subgroup Test). *Let H be a nonempty subset of a group G, and $a, b \in G$. If $a, b \in H \Rightarrow ab^{-1} \in H$, then $H \leq G$.*

We now look at specific subgroups.

Definition 2.21. Let G be a group and $a \in G$, define

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

Here, a is called a *generator* of $\langle a \rangle$.

Theorem 2.22. *Let G be a group and $a \in G$. Then, $\langle a \rangle \leq G$.*

In particular, $\langle a \rangle$ is called a cyclic group, and a more detailed discussion on the topic will follow later.

Definition 2.23. Let G be a group. The *center* of the group is the subset of elements in G that commute with every element in G. Symbolically

$$Z(G) = \{a \in G : ax = xa,\ \forall x \in G\}.$$

Theorem 2.24. *Let G be a group. Then, $Z(G) \leq G$.*

Definition 2.25. Let G be a group and $a \in G$. The *centralizer of a* is the subset of all elements in G that commute with a. Symbolically,

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

Theorem 2.26. *Let G be a group and $a \in G$. Then $C(a) \leq G$.*

3 Cyclic Groups

Definition 3.1. The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a.*

Example 3.2. Consider the following cyclic subgroups.

1. In $\mathbb{Z}_{10}$, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$.
2. In $U(10)$, $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$.

Note that in the second example, the group is entirely generated by a single element.

Definition 3.3. Let G be a group and $a \in G$. In the case that $G = \langle a \rangle$, we say that G is *cyclic* an a is a *generator* of G. Generators need not be unique.

Theorem 3.4. *Let G be a group and $a \in G$.*

(i) *If a has infinite order, then $a^i = a^j$ iff $i = j$, and*

(ii) *If a has finite order n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ iff $n \mid i - j$.*

Proof. We prove both parts seperately, first for the case of infinite order.

($\Rightarrow$) Let $a^i = a^j$. WLOG, assume $i \geq j$ and let $k = i - j \geq 0$.

$$a^i = a^j \Rightarrow a^i \cdot a^{-j} = e \Rightarrow a^{i-j} = e \Rightarrow a^k = e.$$

Since a has infinite order, there exists no $k > 0$ such that $a^k = e$. Therefore, $k = 0 \Rightarrow i = j$.

($\Leftarrow$) If $i = j$, then clearly $a^i = a^j$.

Now for the case of finite order, we must first show that any power a^k reduces to an element of $\{e, a, a^2, \ldots, a^{n-1}\}$. By the division lemma, we know that for every $k \in \mathbb{N}$, there exist integers q and r such that $k = qn + r$ where $r \in [0, n)$.

$$a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r.$$

Since $0 \leq r < n$, $a^k = a^r \in \{e, a, a^2, \ldots, a^{n-1}\} = \langle a \rangle$.

We must now show that $a^i = a^j \Leftrightarrow n \mid i - j$. Let $m = i - j$, which reduces the theorem to proving $a^m = e \Leftrightarrow n \mid m$.

($\Rightarrow$) Let $a^m = e$. Once again, using the division lemma, $m = qn + r$ where $0 \leq r < n$.

$$a^m = a^{qn+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r.$$

Since $a^m = e = a^r$, $r = 0$. As such, $m = qn \Rightarrow n \mid m$.

($\Leftarrow$) If $n \mid m$, then there exists $k \in \mathbb{Z}$ such that $m = nk$.

$$a^m = a^{nk} = (a^n)^k = e^k = e.$$

□

By corollary, note that $\text{ord}(a) = |\langle a \rangle|$ for all $a \in G$.

Theorem 3.5. *Let a be an element of order n in a group, $k \in \mathbb{N}$, and $d = (n, k)$. Then*

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

(b) $\langle a^k \rangle = \langle a^d \rangle$.

Part (a) is a corollary of Theorem 2.16, and the proof of part (b) follows.

Proof. We proceed by double inclusion.

By definition of the gcd, $d \mid k$, and as a result, there exists $m \in \mathbb{Z}$ such that $k = dm$. Therefore,

$$a^k = a^{dm} = (a^d)^m \in \langle a^d \rangle.$$

As such, $\langle a^k \rangle \subseteq \langle a^d \rangle$.

We now proceed to show the reverse inclusion. By Bézout's lemma, there exist integers x and y such that

$$d = nx + ky.$$

Therefore,

$$a^d = a^{nx+ky} = (a^n)^x \cdot (a^k)^y = (a^k)^y \in \langle a^k \rangle.$$

It follows that $\langle a^d \rangle \subseteq \langle a^k \rangle$. □

We may now prove Theorem 2.17 for cyclic groups G.

Proof. Since G is cyclic, there $g \in G$ such that $\langle g \rangle = G$. Let the order of g be n, i.e. $\text{ord}(g) = \text{ord}(G) = n$, and a be an arbitrary element of G.

Since g is a generator, we know that there exists $k \in \mathbb{Z}$ such that $a = g^k$. By Theorem 2.16,

$$\text{ord}(a) = \text{ord}(g^k) = \frac{n}{(n,k)} \Rightarrow \text{ord}(a) \cdot (n,k) = n.$$

Since $(n,k) \in \mathbb{N}$, $\text{ord}(a) \mid \text{ord}(G)$. □

We now list several important corollaries of Theorem 3.5

Corollary 3.6. *Let G be a finite cyclic group of order n, $a \in G$, and $\text{ord}(a) = k$.*

(i) $k \mid n$.

(ii) $\langle a^i \rangle = \langle a^j \rangle \Leftrightarrow (k,i) = (k,j)$. *Moreover,* $\text{ord}(a^i) = \text{ord}(a^j) \Leftrightarrow (k,i) = (k,j)$.

(iii) $\langle a^j \rangle = \langle a \rangle \Leftrightarrow (k,j) = 1$.

(iv) *An integer $m \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $(n,m) = 1$.*

3.1 Fundamental Theorem of Cyclic Groups

Theorem 3.7 (Fundamental Theorem of Cyclic Groups). *Let $G = \langle a \rangle$ be a cyclic group of order n.*

(i) *If $H \leq G$, then H is cyclic.*

(ii) *The order of all subgroups H of G are divisors of n.*

(iii) *For each positive divisor k of n, G has exactly one subgroup of order k, that being $\langle a^{n/k} \rangle$.*

Proof. To prove (i), we must show that H may be generated with a single element. If $H = \{e\}$, then the group is trivially generated by e. Now suppose $H \neq \{e\}$. Since $H \leq G$, every element in H has the form a^k for some integer k, and since H contains nonidentity elements, the set of positive integers k such that $a^k \in H$ is nonempty. By the WOP, let m be the smallest natural number such that $a^m \in H$. We claim that $H = \langle a^m \rangle$, and will proceed to prove this with double inclusion.

Since $a^m \in H$ and H is closed under the group operation, every power of a^m must also be an element of H: $\langle a^m \rangle \subseteq H$. To show the reverse inclusion, let $b \in H$. Since $b \in G$, there exists $k \in \mathbb{N}$ such that $b = a^k$. By the division lemma,

$$k = qm + r$$

where q and r are integers with $0 \leq r < m$. It follows that

$$r = k - qm \Rightarrow a^r = a^{k-qm} = a^k \cdot (a^m)^{-q}.$$

Both a^k and $(a^m)^{-q}$ are elements of H, and as such the product must also be in H. Therefore $a^r \in H$. Recall that $0 \leq r < m$, but since m is the smallest natural number such that $a^m \in H$, we require $r = 0$. As such,

$$b = a^k = a^{qm} = (a^m)^q \in \langle a^m \rangle \Rightarrow H \subseteq \langle a^m \rangle.$$

To prove (ii), we invoke Theorem 2.16. Since $H \leq G$ is cyclic, there exists $g \in G$ such that $H = \langle g^d \rangle$ for some $d \in \mathbb{N}$. Then,

$$\text{ord}(H) = \text{ord}(g^d) = \frac{n}{(n,d)} \Rightarrow n = \text{ord}(H) \cdot (n,d) \Rightarrow \text{ord}(H) \mid \text{ord}(G).$$

To prove (iii), we must individually show the existence of the subgroup of order k and its uniqueness. By Theorem 2.16,

$$\text{ord}(\langle a^{n/k} \rangle) = \text{ord}(a^{n/k}) = \frac{n}{(n, n/k)} = \frac{n}{n/k} = k.$$

This proves the existence of the subgroup and that its order is k. We now proceed to prove its uniqueness. Let $H \leq G$ such that $\text{ord}(H) = k$. By part (i), H must be cyclic, and generated by some element a^m:

$$H = \langle a^m \rangle.$$

Since $\text{ord}(H) = k$, the order of the generator must also be k:

$$\text{ord}(a^m) = \frac{n}{(n,m)} = k \Rightarrow (n,m) = \frac{n}{k}.$$

By Theorem 3.5 (a),

$$H = \langle a^m \rangle = \langle a^{(n,m)} \rangle = \langle a^{n/k} \rangle.$$

Since all subgroups of order k are equal to $\langle a^{n/k} \rangle$, the subgroup of order k is unique. □

3.2 Symmetric and Dihedral Groups

Definition 3.8. A *permutation* of a set A is a bijection $f : A \to A$.

Let S_A denote the set of permutations of A. It is easy to verify that S_A forms a group under the function composition operation $\circ$. This group is referred to as the *symmetric group* or *permutation group* on A.

We typically focus our study on finite order groups where the set A is of the form $\{1, 2, \ldots, n\}$, and we denote the group by S_n. We denote permuations using matrices. For example, consider the group S_3, and the permutation f such that $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$. Then, we write

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Example 3.9. List all elements of the symmetric group S_3.

Solution.

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad ba = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

■

The order of S_n is trivially $n!$, and when $n \geq 3$, it is Nonabelian.

Now, consider a square whose vertices are labelled $\{1, 2, 3, 4\}$ clockwise, and define the following transformations:

- r: rotation by 90° clockwise.
- s: reflect across a vertical axis.

The symmetries of a square under these operations form a group

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

called the dihedral group of order 4.

Definition 3.10. A *dihedral group* of order $2n$ is the group of symmetrised of a regular n-gon. Symbolically,

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