Fall 2025 Introduction to Algebra (I)

Preview Note

Department : Atmospheric Sciences Name : Guan-Hao, Chen Student ID : B11209022

Contents

0 Preliminaries

0.1 Basics

The subset of a given set A is

$$B = \{a \in A \mid \ldots \text{(conditions on a)} \ldots\}$$

The *order* (or *cardinality*) of a set A will be denoted by $|A|$. If A is a finite set, the order of A is simply the number of elements of A.
The *Cartesian product* of two sets A and B is the collation $A \times B = \{(a, b) \mid a \in A, b \in B\}$, of ordered pairs of elements from A and B.
The following notation for some common sets of numbers

1. **Integers**: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.
2. **Rational numbers**: $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$.
3. **Real numbers**: $\mathbb{R} = \{\text{all decimal expansions} \pm d_1 d_2 \ldots d_n . a_1 a_2 a_3 \ldots\}$.
4. **Complex numbers**: $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$.
5. $\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ will denote the positive (nonzero) elements in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.

The notation $f : A \to B$ or $A \xrightarrow{f} B$ to denote a *function* (or *map*) f from A to B, and the value of f at a is denoted by $f(a)$. The set A is called the *domain* of f and B is called the *codomain* of f.
The notation $f : a \mapsto b$ or $a \mapsto b$ if f is understood indicates that $f(a) = b$, i.e., the function is being specified on *elements*. If the function f is not specified on elements, it is important in general to check that f is *well defined*, i.e., is unambiguously determined.
The set

$$f(A) = \{b \in B \mid b = f(a), \text{ for some } a \in A\}$$

is a subset of B, called the *range* or *image* of f (or the *image* of A under f).
For each subset C of B, the set

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

consisting of the elements of A mapping into C under f is called the *preimage* or *inverse image* of C under f. For each $b \in B$, the preimage of $\{b\}$ under f is called the *fiber* of f over b. Note that f^{-1} is not in general a function and that the fibers of f generally contain many elements since there may be many elements of A mapping to the element b.
If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by

$$(g \circ f)(a) = g(f(a))$$

Definition 0.1-1 Let $f : A \to B$

1. f is *injective* or is an *injection* if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.
2. f is *surjective* or is a *surjection* if for all $b \in B$, there is some $a \in A$ such that $f(a) = b$.
3. f is *bijective* or is a *bijection* if it is both injective and surjective. If such a bijection f exists from A to B, we say A and B are in *bijective correspondence*.
4. f has a *left inverse* if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A, i.e., $(g \circ f)(a) = a$ for all $a \in A$.
5. f has a *right inverse* if there is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B, i.e., $(f \circ h)(b) = b$ for all $b \in B$.

Proposition 0.1-1 Let $f : A \to B$

1. The map f is injective if and only if f has a left inverse.
2. The map f is surjective if and only if f has a right inverse.
3. The map f is a bijection if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.
4. If A and B are finite sets with the same number of elements (i.e., $|A| = |B|$), then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.

Proof.

1. ($\Rightarrow$) Suppose f is injective. Notice that if $b \in f(A)$ then there is a unique $a \in A$ such that $f(a) = b$. Choose any $a_0 \in A$, and define $g : B \to A$ by

$$g(b) = \begin{cases} a & \text{if } b \in f(A) \\ a_0 & \text{if } b \notin f(A) \end{cases}$$

   Then $(g \circ f)(a) = a$ for all $a \in A$, so g is a left inverse of f.

   ($\Leftarrow$) Suppose f has a left inverse g, and that $f(a) = f(b)$. Then $g(f(a)) = g(f(b))$, and since $g \circ f : A \to A$, we have $a = b$, which shows f is injective.

2. ($\Rightarrow$) Suppose f is surjective. Then every $b \in B$ is in the image of f, so for each $b \in B$ pick an element $g(b) \in A$ such that $f(g(b)) = b$. Then g is a right inverse of f.

   ($\Leftarrow$) Suppose f has a right inverse g and let $b \in B$. Then $f(g(b)) = b$ as $f \circ g : B \to B$. This shows $b \in f(A)$, so $f(A) = B$ and f is surjective.

3. ($\Rightarrow$) Suppose f is a bijection, then f is injective and surjective by definition. By part 1. there exists a left inverse $g : B \to A$ such that $g \circ f : A \to A$, and by part 2. there exists a right inverse $g : B \to A$ such that $f \circ g : B \to B$.

   ($\Leftarrow$) Suppose there exists $g : B \to A$ such that $f \circ g : B \to B$ and $g \circ f : A \to A$. Then by part 1., f is surjective, and by part 2., f is injective. Then f is a bijection.

4. **Claim**:

   (1) If $f : A \to B$ is injective, then $|A| \le |B|$.

   (2) If $f : A \to B$ is surjective, then $|A| \ge |B|$.

   (3) If $f : A \to B$ is a bijection, then $|A| = |B|$.

   proof. Let $A = \{a_1, a_2, \ldots, a_m\}$ has m elements.

   (1) $\{f(a_1), f(a_2), \ldots, f(a_m)\}$ is a subset of B, because f is injective, $|A| = m \le |B|$.

   (2) $\{f(a_1), f(a_2), \ldots, f(a_m)\} = B$ has at most m different elements because f is surjective, $|A| = m \ge |B|$.

   (3) This follows from (1) and (2), since $|A| \le |B|$ and $|A| \ge |B|$, we have $|A| = |B|$.

The situation of part 3. of **Proposition 0.1-1**, the map g is necessarily unique and we shall say g is the *2-sided inverse* (or *inverse*) of f.
A *permutation* of a set A is simply a bijection from A to itself.
If $A \subseteq B$ and $f : B \to C$, we denote the *restriction* of f to A by $f|_A$.
If $A \subseteq B$ and $g : A \to C$ and there is a function $f : B \to C$ such that $f|_A = g$, we shall say f is an *extension* of g to B.

Definition 0.1-2 Let A be a nonempty set.

1. A *binary relation* on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.
2. The relation $\sim$ on A is said to be:

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

   (b) *symmetric* if $a \sim b$ implies $b \sim a$ for all $a, b \in A$

   (c) *transitive* if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$

   A relation is an *equivalence relation* if it is reflexive, symmetric and transitive.
3. If $\sim$ defines an equivalence relation on A, then the *equivalence class* of $a \in A$ is defined to be $\{x \in A \mid x \sim a\}$. Elements of the equivalence class of a are said to be *equivalent* to a. If C is an equivalence class, any element of C is called a *representative* of the class C.
4. A *partition* of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A (I some indexing set) such that

   (a) $A = \cup_{i \in I} A_i$

   (b) $A_i \cap A_j = \varnothing$ for all $i, j \in I$ with $i \neq j$, i.e., A is the disjoint union of the sets in the partition.

Proposition 0.1-2 Let A be a nonempty set.

1. If $\sim$ defines an equivalence relation on A, then the set of equivalence classes of $\sim$ form a partition of A.
2. If $\{A_i \mid i \in I\}$ is a partition of A, then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i, $i \in I$.

Proof. Link

0.2 Properties of the integers

0.2.1 Well Ordering of $\mathbb{Z}$

If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ (m is call a *minimal element* of A).

0.2.2 Divides

If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case, we write $a \mid b$; if a does not divide b, we write $a \nmid b$.

0.2.3 Greatest Common Divisor (g.c.d.)

If $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer d, called the *greatest common divisor* of a and b (or g.c.d. of a and b), satisfying:

(1) $d \mid a$ and $d \mid b$ (d is a common divisor of a and b)

(2) If $e \mid a$ and $e \mid b$, then $e \leq d$ (d is the greatest such divisor)

The g.c.d. of a and b will be denoted by (a, b) (or $\gcd(a, b)$). If $(a, b) = 1$, we say that a and b are *relatively prime*.

0.2.4 Least Common Multiple (l.c.m.)

If $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer l, called the *least common multiple* of a and b (or l.c.m. of a and b), satisfying:

(1) $a \mid l$ and $b \mid l$ (l is a common multiple of a and b)

(2) If $a \mid m$ and $b \mid m$, then $l \leq m$ (l is the least such multiple)

The l.c.m. of a and b will be denoted by $[a, b]$ (or $\operatorname{lcm}(a, b)$). The connection between the g.c.d. d and the l.c.m. l of two integers a and b is given by $dl = ab$.

0.2.5 The Division Algorithm

If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \qquad \text{and} \qquad 0 \leq r < |b|$$

where q is the *quotient* and r is the *remainder*.

0.2.6 The Euclidean Algorithm

If $a, b \in \mathbb{Z} \setminus \{0\}$, then we obtain a sequence of quotients and remainders

$$
\begin{aligned}
a &= q_0 b + r_0 && (0)\\
b &= q_1 r_0 + r_1 && (1)\\
r_0 &= q_2 r_1 + r_2 && (2)\\
r_1 &= q_3 r_2 + r_3 && (3)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n && (\mathrm{n})\\
r_{n-1} &= q_{n+1} r_n && (n+1)
\end{aligned}
$$

where r_n is the last nonzero reminder. Such an r_n exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a decreasing sequence of strictly positive integers if the reminders are nonzero and such a sequence cannot continue indefinitely. Then r_n is the g.c.d. (a, b) of a and b.

Example 0.2.6-1 Find the g.c.d. of $a = 57970$ and $b = 10353$.

Sol. Applying the Euclidean algorithm, we have

$$
\begin{aligned}
57970 &= (5)10353 + 6205\\
10353 &= (1)6205 + 4148\\
6205 &= (1)4148 + 2057\\
4148 &= (2)2057 + 34\\
2057 &= (60)34 + 17\\
34 &= (2)17
\end{aligned}
$$

Thus, the g.c.d. of 57970 and 10353 is $(57970, 10353) = 17$.

0.2.7 $\mathbb{Z}$-linear Combinations

One consequence of the Euclidean Algorithm which we shall use regularly is the following: if $a, b \in \mathbb{Z} \setminus \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

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

that is, *the g.c.d. of a and b is a $\mathbb{Z}$-linear combination of a and b.* This follows by recursively writting the element r_n in the Euclidean Algorithm in terms of the previous remainders (namely, use equation (n) above to solve for $r_n = r_{n-2} - q_n r_{n-1}$ in terms of the remainders r_{n-1} and r_{n-2}, then use equation $(n-1)$ to write r_n in terms of the remainders r_{n-2} and r_{n-3}, etc., eventually writing r_n in terms of a and b).

Example 0.2.7-1 Use the Euclidean Algorithm to find integers x, y such that

$$(57970, 10353) = 57970x + 10353y$$

Sol. Based on **Example 0.2.6-1** we know that $(57970, 10353) = 17$. Start from the fifth equation in the Euclidean Algorithm,

$$\begin{aligned}
17 &= 2057 - 60 \cdot 34 \\
&= 2057 - 60 \cdot (4148 - (2)2057) = 121 \cdot 2057 - 60 \cdot 4148 \\
&= 121 \cdot (6205 - (1)4148) - 60 \cdot 4148 = 121 \cdot 6205 - 181 \cdot 4148 \\
&= 121 \cdot 6205 - 181 \cdot (10353 - (1)6205) = 302 \cdot 6205 - 181 \cdot 10353 \\
&= 302 \cdot (57970 - (5)10353) - 181 \cdot 10353 \\
&= 302 \cdot 57970 + (-1691) \cdot 10353
\end{aligned}$$

Thus, $x = 302$ and $y = -1691$ is a solution of $(57970, 10353) = 57970x + 10353y$.

0.2.8 Prime and Composite Numbers

An element p of $\mathbb{Z}^+$ is called a *prime* if $p > 1$ and the only positive divisors of p are 1 and p. An integer $n > 1$ which is not prime is called *composite*.

0.2.9 The Fundamental Theorem of Arithmetic

If $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$$

This factorization is unique in the sense that if $q_1, q_2, \ldots, q_t$ are any distinct primes and positive integers $\beta_1, \beta_2, \ldots, \beta_t$ such that

$$n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$$

then $s = t$ and if we arrange the two sets of primes in increasing order, then $q_i = p_i$ and $\alpha_i = \beta_i$ $1 \leq i \leq s$.

Suppose the positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$$

where $p_1, p_2, \ldots, p_s$ are distinct and the exponents are ≥ 0 (we allow the exponents to be 0 here, so that the products are taken over the same set of primes – the exponent will be 0 if that prime is not actually a divisor). Then the g.c.d. of a and b is

$$(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \ldots p_s^{\min\{\alpha_s,\beta_s\}}$$

and the l.c.m. of a and b is

$$[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \ldots p_s^{\max\{\alpha_s,\beta_s\}}$$

0.2.10 Euler φ-function

For $n \in \mathbb{Z}^+$, let $\varphi(n)$ be the number of positive integers $a \le n$ with a relatively prime to n, i.e., $(a, n) = 1$. For example, $\varphi(12) = 4$ since the positive integers $1, 5, 7, 11$ are the only positive integers less than or equal to 12 which have no factors in common with 12. For prime p, $\varphi(p) = p - 1$, and more generally, for all $a \ge 1$ we have the formula

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$$

The function φ is *multiplicative* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{if } (a, b) = 1$$

(note that it is important here that a and b be relatively prime). Together with the formula above this gives a general formula for the values of φ : if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, then

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_s^{\alpha_s - 1}(p_s - 1) \end{aligned}$$

Example 0.2.10-1 Find the value of $\varphi(36)$.

Sol. The prime factorization of 36 is $36 = 2^2 \cdot 3^2$, therefore

$$\begin{aligned} \varphi(36) &= \varphi(2^2)\varphi(3^2) \\ &= 2^{2-1}(2-1)3^{2-1}(3-1) \\ &= 2 \cdot 1 \cdot 3 \cdot 2 = 12 \end{aligned}$$

0.3 $\mathbb{Z}/n\mathbb{Z}$: The integers modulo n

Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by

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

Clearly $a \sim a$, and $a \sim b$ implies $b \sim a$ for any integers a and b, so this relation is trivially reflexive and symmetric. If $a \sim b$ and $b \sim c$, then n divides $a - b$ and n divides $b - c$, so n also divides the sum of these two integers, i.e., n divides $(a - b) + (b - c) = a - c$, so $a \sim c$ and the relation is transitive. Hence, this is an equivalence relation. Write $a \equiv b \pmod n$ (read: a is *congruent* to b mod n) if $a \sim b$. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of a by $\overline{a}$ – this is called the *congruent class* or *residue class* of a mod n and consists of the integers which differ from a by an integral multiple of n, i.e.,

$$\begin{aligned} \overline{a} &= \{a + kn \mid k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\} \end{aligned}$$

There are precisely n distinct equivalence classes mod n, namely

$$\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}$$

determined by the possible remainders after division by n, and this residue classes partition the integers $\mathbb{Z}$. the set of equivalence classes under this equivalence relation will be denoted by $\mathbb{Z}/n\mathbb{Z}$, and called the *integers modulo* n (or the *integers mod* n).
The process of finding the equivalence class mod n of some integer a is often referred to as *reducing* a *mod* n. This terminology also frequently refers to finding the smallest nonnegative integer congruent to a mod n (the *least residue* of a mod n).

Definition 0.3-1 We can define an addition and a multiplication for the elements of $\mathbb{Z}/n\mathbb{Z}$, defining *modular arithmetic* as follows: for $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, define their sum and product by

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

Given any two elements $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$, to compute their sum (respectively, their product) take *any representative* integer a in the *class* $\overline{a}$ and *any representative* integer b in the *class* $\overline{b}$, and add (respectively, multiply) the integers a and b as usual in $\mathbb{Z}$, and then take the equivalence class containing the result.

Theorem 0.3-1 The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined in **Definition 0.3-1** are both well defined, that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., if

$$a_1 \equiv b_1 \pmod{n} \qquad \text{and} \qquad a_2 \equiv b_2 \pmod{n}$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \qquad \text{and} \qquad a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

Proof. Suppose $a_1 \equiv b_1 \pmod{n}$, i.e., $a_1 - b_1$ is divisible by n. Then $a_1 = b_1 + sn$ for some integer s. Similarly, $a_2 \equiv b_2 \pmod{n}$ means $a_2 = b_2 + tn$ for some integer t. Then $a_1 + a_2 = (b_1 + b_2) + (s+t)n$, so $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, which shows that the sum of the residue classes is independent of the representatives chosen.
Similarly, $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + stn)n$, so $a_1 a_2 \equiv b_1 b_2 \pmod{n}$, and so the product of the residue classes is also independent of the representatives chosen.

Example 0.3-1 Find the last two digits in the number 2^{1000}.

Sol. First observe that the last two digits give the remainder of 2^{1000} after we divided by 100, so we are interested in the residue class mod 100 containing 2^{1000}. We compute $2^{10} = 1024 \equiv 24 \pmod{100}$, so then $2^{20} = (2^{10})^2 \equiv 24^2 = 576 \equiv 76 \pmod{100}$. Then $2^{40} = (2^{20})^2 \equiv 76^2 = 5776 \equiv 76 \pmod{100}$. Similarly, $2^{80} \equiv 2^{160} \equiv 2^{320} \equiv 2^{640} \equiv 76 \pmod{100}$. Finally, $2^{1000} = 2^{640} \cdot 2^{320} \cdot 2^{40} \equiv 76 \cdot 76 \cdot 76 \equiv 76 \pmod{100}$. Thus, the last two digits of 2^{1000} are 76.

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{a} \cdot \overline{c} = \overline{1}\}$$

Proposition 0.3-1

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

Proof. It is easy to see that if any representative of $\overline{a}$ is relatively prime to n, then all representatives are relatively prime to n, so that the set on the right in the proposition is well defined.

If a is an integer relatively prime to n, then the Euclidean Algorithm produces integers x and y satisfying $ax + ny = 1$, hence $ax \equiv 1 \pmod{n}$, so that $\overline{x}$ is the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$. This gives an efficient method for computing multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

Example 0.3-2 Find the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$.

Sol. Suppose $n = 60$ and $a = 17$. Applying the Euclidean Algorithm, we obtain

$$\begin{aligned} 60 &= (3)17 + 9 \\ 17 &= (1)9 + 8 \\ 9 &= (1)8 + 1 \\ 8 &= (8)1 \end{aligned}$$

so that a and n are relatively prime, and $(-7)17 + 2 \cdot 60 = 1$. Hence, $\overline{-7} = \overline{53}$ is the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$.

Part I

Group Theory

1 Introduction to Groups

1.1 Basic Axioms and Examples

Definition 1.1-1

1. A *binary operation* $\star$ on a set G is a function $\star : G \times G \to G$. For any $a, b \in G$, we shall write $a \star b$ for $\star(a, b)$.
2. A binary operation $\star$ on a set G is *associative* if for all $a, b, c \in G$, we have $a\star(b\star c) = (a\star b)\star c$.
3. If $\star$ is a binary operation on a set G, we say elements a and b of G *commute* if $a \star b = b \star a$. We say $\star$ (or G) is *commutative* if for all $a, b \in G$, we have $a \star b = b \star a$.

Example 1.1-1

1. $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively).
2. $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively).
3. $-$ (usual subtraction) is noncommutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$. It is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+$, $\mathbb{R}^+$) (e.g. $-(1, 2) = 1 - 2 = -1 \notin \mathbb{Z}^+$).
4. Taking the vector cross-product of two vectors in $\mathbb{R}^3$ is a binary operation which is not associative and not commutative. For example,
   (1) $\mathbf{u} = (1, 2, 3)$, $\mathbf{v} = (4, 5, 6) \in \mathbb{R}^3$, $\mathbf{u} \times \mathbf{v} = (-3, 6, -3)$
   $\Rightarrow \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$
   (2) $\mathbf{u} = (1, 2, 3)$, $\mathbf{v} = (4, 5, 6) \in \mathbb{R}^3$, $\mathbf{u} \times \mathbf{v} = (-3, 6, -3)$, $\mathbf{v} \times \mathbf{u} = (3, -6, 3)$
   $\Rightarrow$ it is not commutative.
   (3) $\mathbf{u} = (1, 2, 3)$, $\mathbf{v} = (4, 5, 6)$, $\mathbf{w} = (7, 8, 9) \in \mathbb{R}^3$,
   $(\mathbf{u} \times \mathbf{v}) \times \mathbf{w} = (-3, 6, -3) \times (7, 8, 9) = (78, 6, -66)$
   $\mathbf{u} \times (\mathbf{v} \times \mathbf{w}) = (1, 2, 3) \times (-3, 6, -3) = (-24, -6, 12)$

Suppose that $\star$ is a binary operation on a set G, and H is a subset of G. If the restriction of $\star$ to H is a binary operation on H ($\forall\ a, b \in H, a \star b \in H$), we say that H is *closed* under $\star$.
Observe that if $\star$ is an associative (respectively, commutative) binary operation on a set G, and $\star$ restricted to some subset H of G is a binary operation on H, then $\star$ is automatically associative (respectively, commutative) on H as well.

Definition 1.1-2

1. A *group* is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   (i) **Associative**: $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$.
   (ii) **Identity**: There exists an element $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.
   (iii) **Inverses**: For each $a \in G$, there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
2. The group $(G, \star)$ is called *abelian* (or *commutative*) if $a \star b = b \star a$ for all $a, b \in G$.

We say G is a *finite group* if in addition G is a finite set.
Note that the axiom (ii) ensures that a group is always nonempty.

Example 1.1-2

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$ for all a.
2. $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are groups under $\times$ with $e = 1$ and $a^{-1} = \dfrac{1}{a}$.
3. The axioms for a vector space V which specify that $(V, +)$ is an abelian group.
4. For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ with the identity element $\overline{0}$ and the inverse of $\overline{a}$ is $\overline{-a}$.
5. For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\overline{a}$ which have multiplicative inverses mod n is an abelian group under multiplication with the identity element $\overline{1}$.

If $(A, \star)$ and $(B, \diamond)$ are groups, we can find a new group $A \times B$, called the *direct product*, whose elements are those in the Cartesian product

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

and whose operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

Proposition 1.1-1 If G is a group under the operation $\star$, then

1. The identity of G is unique.
2. For each $a \in G$, a^{-1} is uniquely determined.
3. $(a^{-1})^{-1} = a$ for all $a \in G$.
4. $(a \star b)^{-1} = (b)^{-1} \star (a)^{-1}$
5. **Generalized Associative Law**: 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 the expression is bracketed.

Proof.

1. If f and g are both identities, then by axiom (ii) of the **Definition 1.1-2**, we have $f \star g = f$ and $g \star f = g$. Thus $f = g$, and the identity is unique.

2. Assume b and c are both inverses of a, and let e be the identity of G. By axiom (iii) of the **Definition 1.1-2**, $a \star b = e$ and $c \star a = e$. Thus

$$\begin{aligned} c &= c \star e && \text{(Axiom (ii))} \\ &= c \star (a \star b) && \text{(Since } e = a \star b\text{)} \\ &= (c \star a) \star b && \text{(Axiom (i))} \\ &= e \star b && \text{(Since } e = c \star a\text{)} \\ &= b && \text{(Axiom (ii))} \end{aligned}$$

3. The inverse of a is a^{-1}, and the inverse of a^{-1} is $(a^{-1})^{-1}$, by part 2., we know $a = (a^{-1})^{-1}$.
4. Let $c = (a \star b)^{-1}$, so by definition of c, $(a \star b) \star c = e$. By the associative law, we have

$$a \star (b \star c) = e$$

Multiply both sides on the left by a^{-1} to get

$$a^{-1} \star (a \star (b \star c)) = a^{-1} \star e$$

The associative law on the LHS and the definition of e on the RHS give

$$\begin{aligned} (a^{-1} \star a) \star (b \star c) &= a^{-1} \\ e \star (b \star c) &= a^{-1} \\ b \star c &= a^{-1} \end{aligned}$$

Now, multiply both sides on the left by b^{-1} to get

$$\begin{aligned} b^{-1} \star (b \star c) &= b^{-1} \star a^{-1} \\ (b^{-1} \star b) \star c &= b^{-1} \star a^{-1} \\ e \star c &= b^{-1} \star a^{-1} \\ c &= b^{-1} \star a^{-1} \end{aligned}$$

Thus $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

5. First show the result is true for $n = 1, 2$ and 3. Next, assume for any $k < n$ that any braketing of a product of k elements, $b_1 \star b_2 \star \cdots \star b_k$ can be reduced (without altering the value of the product) to an expression of the form

$$b_1 \star (b_2 \star (b_3 \star (\cdots \star b_k)) \dots)$$

Now argue that an bracketing of the product $a_1 \star a_2 \star \cdots \star a_n$ must break into 2 subproducts, say $(a_1 \star a_2 \star \cdots \star a_k) \star (a_{k+1} \star a_{k+2} \star \cdots \star a_n)$, where each subproduct is bracketed in some fashion. Apply the induction assumption to each of these two subproducts and finally reduce the result to the form $a_1 \star (a_2 \star (a_3 \star (\cdots \star a_n)) \dots)$ to complete the induction.

For any group G (operation $\cdot$ implied) and $x \in G$ and $n \in \mathbb{Z}^+$ since the product $xx\dots x$ (n terms) does not depend on how it is bracketed, we shall denote it by x^n. Denote $x^{-1}x^{-1}\dots x^{-1}$ (n terms) by x^{-n}. Let $x^0 = 1$, the identity of G.
When we are dealing with specific groups, we shall use the natural (given) operation. For example, when the operation is $+$, the identity will be denoted by 0 and for any element a, the inverse a^{-1} will be written $-a$, and $a + a + \cdots + a$ ($n > 0$ terms) will be written na; $-a - a - \cdots - a$ (n terms) will be written $-na$, and $0a = 0$.

Proposition 1.1-2 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, the left and right cancellation laws hold in G, i.e.,

1. If $au = av$, then $u = v$.
2. If $ub = vb$, then $u = v$.

Proof. We can solve $ax = b$ by multiplying both sides on the left by a^{-1} and simplifying to get $x = a^{-1}b$. The uniqueness of x follows because a^{-1} is unique. Similarly, we can solve $ya = b$ by multiplying both sides on the right by b^{-1} and simplifying to get $y = ba^{-1}$. The uniqueness of y follows because b^{-1} is unique.
If $au = av$, multiply both sides on the left by a^{-1}, and simplify to get $u = v$. Similarly, if $ub = vb$, multiply both sides on the right by b^{-1}, and simplify to get $u = v$.

Definition 1.1-3 For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of order n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

Example 1.1-3

1. An element of a group has order 1 if and only if it is the identity.
2. In the additive groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ every nonzero element has infinite order.
3. In the multiplicative groups $\mathbb{R} \setminus \{0\}$ or $\mathbb{Q} \setminus \{0\}$ the element -1 has order 2 and all other nonidentity elements have infinite order.
4. In the additive group $\mathbb{Z}/9\mathbb{Z}$, the element $\overline{6}$ has order 3 since $\overline{6} \neq \overline{0}$, $\overline{6} + \overline{6} = \overline{12} = \overline{3} \neq \overline{0}$, but $\overline{6} + \overline{6} + \overline{6} = \overline{18} = \overline{0}$, the identity in this group.
5. In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$, the element $\overline{2}$ has order 3 since $\overline{2} \neq \overline{1}$, $\overline{2} \times \overline{2} = \overline{4} \neq \overline{1}$, but $\overline{2} \times \overline{2} \times \overline{2} = \overline{8} = \overline{1}$, the identity in this group.

Definition 1.1-4 Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

More about the group table:

1. Group Multiplication Tables | Cayley Tables (Abstract Algebra)
2. Group Theory Step-by-Step: 1 - 7

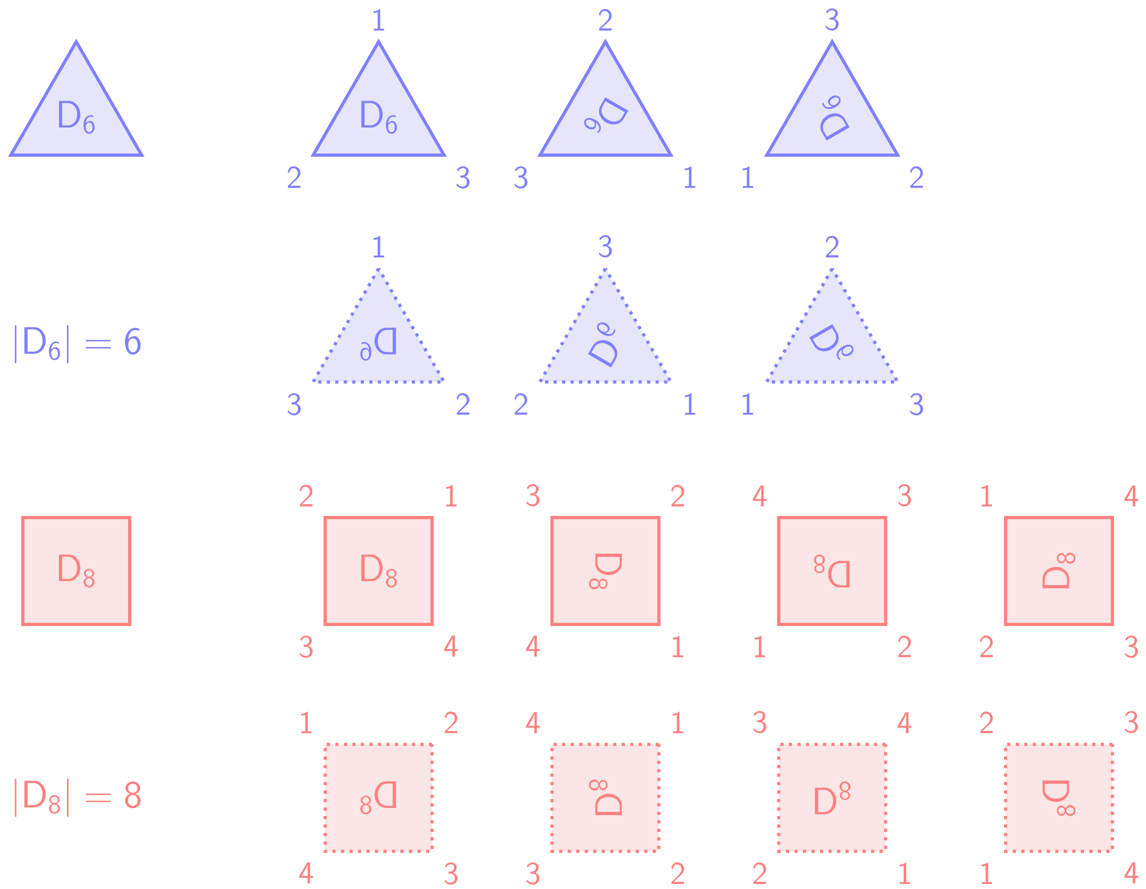
1.2 Dihedral Groups

For each $n \in \mathbb{Z}^+$, $n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space, then placing the copy back on the original n-gon so it exactly covers it.
Each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \ldots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j.
The identity og D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s (so if s effects permutation σ, then the inverse of s effects the permutation σ^{-1}).

Proposition 1.2-1 The order of the dihedral group

$$|D_{2n}| = 2n$$

Proof. To find the order $|D_{2n}|$ observe that given any vertex i, there is a symmetry which sends vertex 1 into position i. Since vertex 2 is adjacent to vertex 1, vertex 2 must end up in position $i+1$ or $i-1$ (when $n+1$ is 1 and $1-1$ is n, i.e., the integers labelling the vertices are read mod n). Moreover, by following the first symmetry by a reflection about the line through vertex i and the center of the n-gon one sees that vertex 2 can be sent to either position $i+1$ or $i-1$ by some symmetry. Thus there are $2n$ positions the ordered pair of 1, 2 may be sent to upon applying symmetries.



These symmetries are the n rotations about the center through $2\pi/n$ radian, $0 \leq i \leq n-1$, and the n reflections through the n lines of symmetry. Now, we only need to define two generators to describe the group D_{2n}.

1. **Rotation** r: Rotation clockwise about the origin through $2\pi/n$ radian.
2. **Reflection** s: Reflection about the line of symmetry through vertex 1 and the origin.

1.3 Symmetric Groups

SSSSS

1.4 Matrix Groups

1.5 The Quaternion Group

1.6 Homomorphisms and Isomorphisms

1.7 Group Actions

2 Subgroups