Chapters 1 and 2

<u>Defn</u>: • Let G be a set. A <u>binary operation</u> on G is a function that assigns to every ordered pair of elements of G another element of G. (More simply, a binary operation on G is a function from $G \times G$ to G).

• If ϕ is a binary operation on G and $S \subseteq G$, we say S is <u>closed with respect to ϕ</u> if $\forall a,b \in S$ $\phi(a,b) \in S$.

<u>Ex</u>: • Addition, subtraction, and multiplication are binary operations on $\mathbb{R}$. $\mathbb{Z}$ and $\mathbb{Q}$ are closed with respect to all three operations. The set of negative real numbers is closed with respect to addition, but not closed with respect to subtraction nor multiplication

<u>Defn</u>: Let G be a set equipped with a binary operation (typically called <u>multiplication</u>) that associates to each pair $(a,b) \in G \times G$ an element denoted $a \cdot b$, or more simply ab. We call G a <u>group</u> if the following properties hold:

① (Associativity) $\forall a,b,c \in G$ $(ab)c = a(bc)$

② (Identity) there is $e \in G$ (called the <u>identity</u>) such that $\forall g \in G$ $ge = eg = g$

③ (Inverses) for all $a \in G$ there is $b \in G$ satisfying $ab = ba = e$.

Defn: A group G is abelian if $\forall a,b \in G$ $ab = ba$.
Otherwise, G is non-abelian

	Examples	Non-examples
Abelian	• $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ~~and~~ $\mathbb{C}$, and $\mathbb{R}^n$ under (normal) addition	• $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$ under subtraction (not associative)
Abelian	• $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, and $\mathbb{C}\setminus\{0\}$ under multiplication	• $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, and $\mathbb{C}\setminus\{0\}$ under division (not associative)
Abelian	• $\{p \in \mathbb{Q} : p > 0\}$ and $\{r \in \mathbb{R} : r > 0\}$ under multiplication	• $\mathbb{Z}$ under multiplication (no inverses)
Abelian	• $\{-1, 1\}$, $\{1, -1, i, -i\}$, and the set of n^{th} roots of unity $\{e^{2\pi i t/n} : t \in \mathbb{Z}, 0 \le t < n\}$ under multiplication	• $\{r \in \mathbb{R} : r \text{ is irrational}\}$ under multiplication (not closed: $\sqrt{2}\cdot\sqrt{2} = 2$)
Abelian	• 2×2 matrices with coefficients in ~~$\mathbb{Z}$~~, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ under addition	• 2×2 matrices with coeff. in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ under matrix multiplication (matrices with determinant 0 have no inverse)
Non-abelian	• 2×2 matrices with coeff. in $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ that have non-zero determinant, under matrix multiplication	

Lem 2.A Let $n \in \mathbb{Z}$, $n \geq 2$. Then the set
$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$
is a group under addition mod n

~~Def.~~ Note: The "addition mod n" binary operation sends $a, b \in \mathbb{Z}_n$ to $(a+b) \bmod n$.

Pf: (Associative) Let $a, b, c \in \mathbb{Z}_n$. By Lem 0.B
$$[(a+b) \bmod n + c] \bmod n$$
$$= [a+b+c] \bmod n$$
$$= [a+((b+c) \bmod n)] \bmod n$$
(Identity) For all $j \in \mathbb{Z}_n$ $(j+0) \bmod n = j$.
So 0 is the identity
(Inverse) Let $j \in \mathbb{Z}_n$. If $j=0$ then the inverse of j is 0 since $(j+0) \bmod n = 0$.
If $j \neq 0$ then the inverse of j is $n-j$ since $n-j \in \mathbb{Z}_n$ and $(j+(n-j)) \bmod n = n \bmod n = 0$.
$\square$

So $\mathbb{Z}_n$ is an abelian group under addition mod n.

Lem 2.B: Let $n \in \mathbb{Z}$, $n \geq 2$. Then the set
$$U(n) = \{0 < j < n : j \in \mathbb{Z}, \gcd(j, n) = 1\}$$
is a group under multiplication mod n

Pf: Multiplication mod n is a binary operation on $\mathbb{Z}_n$. We first check $U(n)$ is closed with respect to multiplication mod n.
So let $a, b \in U(n)$. Pick $q, r \in \mathbb{Z}$ so that $ab = nq + r$ and $0 \le r < n$. In particular $ab \bmod n = r$.

Towards a contradiction, suppose $k = \gcd(r, n) > 1$. Let p be a prime factor of k. Then $p \mid k$ hence $p \mid n$ and $p \mid r$. Therefore p divides $nq + r = ab$. By Euclid's Lem, $p \mid a$ or $p \mid b$. But if $p \mid a$ then $\gcd(a, n) \ge p > 1$, contradicting $a \in U(n)$. And if $p \mid b$ then similarly $\gcd(b, n) \ge p > 1$, contradicting $b \in U(n)$. So we must have $\gcd(r, n) = 1$ and thus $ab \bmod n = r \in U(n)$. We conclude $U(n)$ is closed under multiplication mod n.

(Associativity) Follows from Lem 0.B (see proof of Lem 2.A)

(Identity) For all $j \in U(n)$ $j \cdot 1 \bmod n = j$, so 1 is the identity.

(Inverse) This follows from Homework 1 (Ch. 0 #11)

$\square$

So $U(n)$ is an abelian group under multiplication mod n

Note: $\mathbb{Z}_n$ is not a group under multiplication mod n since 0 has no inverse

Fix $n \in \mathbb{Z}$, $n \geq 2$

Lem 2.C: The following are equivalent.

① $\{1, 2, \cdots, n-1\}$ is a group under multiplication mod n

② n is prime

③ $U(n) = \{1, 2, \cdots, n-1\}$

Pf: (② ⇒ ③) Assume n prime. By definition $U(n) \subseteq \{1, \cdots, n-1\}$. On the other hand, for any $1 \leq j \leq n-1$ we have $\gcd(j, n) = 1$ since n prime and $j < n$. Thus $j \in U(n)$, so $U(n) \supseteq \{1, \cdots, n-1\}$.

(③ ⇒ ①) This follows from Lem 2.B

(① ⇒ ②) We'll prove contrapositive. So assume n not prime. Then there are $1 < a, b < n$ with $ab = n$. So $ab \bmod n = 0$ which means $\{1, \cdots, n-1\}$ is not closed under multiplication mod n, hence isn't a group. □

Note: If $a \mid n$ then a has no multiplicative inverse mod n. Indeed, say $ab = n$. Then $ab \bmod n = 0$. If k were a multiplicative inverse mod n for a, we would have

$$kab \bmod n = [(ka \bmod n) \cdot b] \bmod n = 1 \cdot b \bmod n = b \bmod n = b$$

But we know

$$kab \bmod n = [k(ab \bmod n)] \bmod n = [k \cdot 0] \bmod n = 0 \bmod n = 0.$$

Let p be prime.

Ex: The set $GL_2(\mathbb{Z}_p) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}_p, (ad-bc) \bmod p \neq$
is a group under matrix multiplication mod n

Associativity can be checked by direct computation
The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Inverses: Consider any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}_p)$
Let f be the multiplicative inverse mod p of $ad-bc$ (which exists by lem 2.C).
By direct computation can verify the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is:

$$\begin{bmatrix} df & -bf \\ -cf & af \end{bmatrix}$$

Note: $GL_2(\mathbb{Z}_p)$ is non-abelian

Ex: Symmetries of the square (Chapter 1)

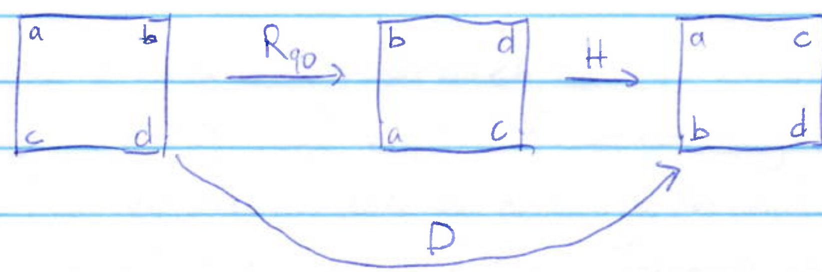
Consider a square S (for instance, $S = \{(x,y) \in \mathbb{R}^2 : 0 \leq x,y \leq 1\}$
A symmetry of S is a function $f: S \to S$
that preserves distances between pairs of points

The square has precisely 8 symmetries:

① R_0 (do nothing / rotate 0°)	⑤ H flip over horizontal line
② R_{90} (rotate 90° counter-clockwise)	⑥ V flip over vertical line
③ R_{180} (rotate 180° " ")	⑦ D flip over main diagonal
④ R_{270} (rotate 270° " ")	⑧ D' flip over 2nd diagonal

The set of symmetries of the square is a group under the binary operation of composition of functions

<u>Ex:</u> $HR_{90} = D$ because the combined effect of rotating the square $90°$ counter-clockwise and then flipping it over its horizontal midline is the same as flipping it over its main diagonal



<u>Associativity</u>: Composition of functions is always associative. If $f, g, h: S \to S$ are symmetries then for all $x \in S$

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x))$$
$$= f(g(h(x))) = f((g \circ h)(x)) = [f \circ (g \circ h)](x)$$

<u>Identity</u>: R_0 is the identity. Since $\forall x \in S$ $R_0(x) = x$, we have that $R_0 \circ f = f = f \circ R_0$ for every symmetry f.

<u>Inverses</u>: If $f: S \to S$ is a symmetry, then so is f^{-1} and

$$f \circ f^{-1} = R_0 = f^{-1} \circ f.$$

<u>Defn</u>: D_4 is the group of symmetries of a square. In general for $n \in \mathbb{Z}$, $n \geq 3$, the group of symmetries of a regular n-gon is denoted D_n and called the <u>dihedral group of order $2n$</u>.

Basic Properties of Groups

<u>Thm 2.1</u>: In a group G, there is only one identity element.

<u>Pf</u>: Suppose e and e' are identities for G, meaning $\forall g \in G$ $ge = g$ and $e'g = g$. Plugging in $g = e'$ in the first equation, and $g = e$ in the second equation, we get $e'e = e'$ and $e'e = e$. Therefore $e' = e$ $\square$

<u>Note</u>: We therefore refer to "the" identity of G and will denote it by e.

<u>Thm 2.2</u>: In a group G, right and left cancellation laws hold. Specifically, for all $a, b, c \in G$

① $ba = ca \Rightarrow b = c$

② $ab = ac \Rightarrow b = c$

<u>Pf</u>: ① Let a' be an inverse to a. ~~Then~~ And let e be the identity. Then

$$b = be = b(aa') = (ba)a' = (ca)a' = c(aa') = ce = c$$

② Similar, but multiply the equation $ab = ac$ on the left by a'. $\square$

<u>Thm 2.3</u>: In a group G inverses are unique, meaning for every $a \in G$ there is a unique $b \in G$ satisfying $ab = ba = e$.

Pf: Inverses must exist (by definition of being a group). Uniqueness holds because if $ab = e$ and $ac = e$ then $ab = ac$ and $b = c$ by left-cancellation. $\square$

Defn: For a group G and $a \in G$, we write a^{-1} for the (unique) inverse of a. Also, we define $a^0 = e$ and for integers $k > 0$:

$$a^k = \underbrace{a \cdot a \cdots a}_{k \text{ factors}}$$

$$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{k \text{ factors}}$$

Note: • Only integer exponents of a are defined. $a^{1/2}$ is not.
• For integers m, n we have

$$a^m \cdot a^n = a^{m+n} \text{ and } (a^m)^n = a^{mn}$$

Warning: $(ab)^n \neq a^n b^n$ (unless G is abelian)

Thm 2.4: Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$

Pf: $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$.
Also $(ab)(ab)^{-1} = e$, so $(ab)(b^{-1}a^{-1}) = (ab)(ab)^{-1}$.
Now use left-cancellation. $\square$