# Section 3.1 Notes

Scribe: Heidi Bronson
09/10/2025

## 1. Section 3.1

**Definition 1.** A <u>group</u> is a set S along with a binary operation $*$ that is
- <u>closed</u> $* : S \times S \to S$
- <u>associative</u> $(a * b) * c = a * (b * c)$
- Has an <u>identity</u> element e, $a * e = a = e * a$
- Every element a has an <u>inverse</u> $a^{-1}, a * a^{-1} = e = a^{-1} * a$.

**Theorem 1.** Groups have the cancellation property:
If $a * b = a * c$ then $b = c$ (left cancellation) and if $b * a = c * a$ then $b = c$ (right cancellation).

*Proof.* Since $a^{-1}$ is an element of the group then if $a * b = a * c$ then composing both sides on the left by $a^{-1}, a^{-1} * (a * b) = a^{-1} * (a * c)$. Now using associativity $(a^{-1} * a) * b = (a^{-1} * a) * c$ so $e * b = e * c$ since $e$ is the identity $b = c$. This proves left cancellation. Right cancellation is similar. □

In general, groups do not have the commutative property $a * b \neq b * a$ in general. (Example: permutations. $\sigma \circ \tau \neq \tau \circ \sigma$ if they aren't disjoint.)

**Definition 2.** If G is a group where $a * b = b * a$ for all $a, b \in G$. We call $G$ an <u>abelian group</u>.

**Theorem 2.** If $a * b = e$ in a group then $b * a = e$.

*Proof.* Suppose $a * b = e$. Then $a = e * a$ so $a = (a * b) * a$. By associativity $a = a * (b * a)$. Since $a = a * e, a * e = a * (b * a)$ by left cancellation we find that $e = b * a$. (Note: in loops (non-associative) this may not be true!) □

**Corollary 1.** If $a \in G$ and $G$ is a group, then $(a^{-1})^{-1} = a$.

*Proof.* Since $a^{-1} * a = e,\ a * a^{-1} = e$ so $a$ is the inverse of $a^{-1}$ □

**Theorem 3.** Inverses are unique. If $a * b = e$ and $a * c = e$, then $b = c$.

*Proof.* This follows immediately from left cancellation. □

If G is a group with finitely many elements we call $G$ a <u>finite</u> group otherwise its an <u>infinite group</u>. We can always define a finite group just by writing down its operation table.

**Example 1.** a. $(\mathbb{Z}, +)$ is an infinite abelian group.
b. Positive integers under multiplication? $(\mathbb{N}, \times)$
- <u>Closed</u>
- has an <u>identity</u> (1)
- <u>associative</u>
- Doesn't have inverses

This is a monoid
c. Positive rational numbers under multiplication? $(\mathbb{Q}, \times)$

- Closed
- has an identity (1)
- associative $(\frac{a}{b} \times \frac{c}{d}) \times (\frac{e}{f})$ where $a, b, c, d, e, f \in \mathbb{Z}_{\geq 0}$. $(\frac{a \times c}{b \times d}) \times (\frac{e}{f}) = \frac{(a \times c) \times e}{(b \times d) \times f} = \frac{a \times (c \times e)}{b \times (d \times f)} = \frac{a}{b} \times (\frac{c}{d} \times \frac{e}{f})$ because multiplication of $\mathbb{Z}$ is associative.
- Every element has an inverse. Let $\frac{a}{b} \in \mathbb{Q}_{>0}$. $\frac{b}{a} \times \frac{a}{b} = \frac{b \times a}{a \times b} = 1$. $\frac{b}{a} = (\frac{a}{b})^{-1}$. $\frac{b}{a} \in \mathbb{Q}_{>0}$ since $a, b > 0$.

Yes, $(\mathbb{Q}, \times)$ is an infinite abelian group.

**Example 2.** a. $(\mathbb{Q}, \times)$: 0 has no inverse but $\mathbb{Q}^{\times} = \{q \in \mathbb{Q}, q \neq 0\}$
b. $(\mathbb{Q}^{\times}, \times)$ is an infinite abelian group.

**Example 3.** a. $(\mathbb{Q}, +)$
b. $(\mathbb{C}, +)$ (complex numbers)
c. $(\mathbb{R}, +)$
d. $(\mathbb{R}^{\times}, \times)$ (every real number except 0)

Matrices:
- $M_n(\mathbb{R}) \to$ all $n \times n$ matrices with real entries
- $(M_n(\mathbb{R}), +)$ is a group for any $n > 0$.

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

does not have an inverse under multiplication.
- $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ is the set of matrices with nonzero determinant (invertible).
- $(GL_n(\mathbb{R}), \times)$ is a group. Not abelian if $n > 1$.

Finite Groups:
$S_n$ - symmetric group on $n$ elements.
$|S_n| = n!$ (not abelian)
$\mathbb{Z}_n$ represents the equivalence classes of the integers mod $n$.
$(\mathbb{Z}_n, +)$ is an abelian group.
Note: $S_n$ is associative since we can think of the elements as functions, function composition is always associative.

Additive/multiplicative notation for groups:
For a general group we use "multiplicative notation" $a^{-1}$ for inverses $a^n = a * a * ... * a$ $n$ times. Sometimes we use additive notation $(+)$, use $-a$ for inverses, and $na = a + a\ + ... +\ a$ (repeated composition). Additive notation is only used when the group is abelian.

**Theorem 4.** Let $G$ be a group and $a, b \in G$, then $a * b = b * a$ iff $a^2 * b^2 = (ab)^2$.

*Proof.* Suppose $a * b = b * a$ then $a^2 * b^2 = (a * a) * (b * b) = a * (a * b) * b = a * (b * a) * b = (a * b) * (a * b) = (a * b)^2$.
Suppose $a^2 * b^2 = (a * b)^2$ then $(a * a) * (b * b) = (a * b) * (a * b)$ so $a * (a * b) * b = a * (b * a) * b$ (by associativity).
By both left and right cancellation, $a * b = b * a$. $\square$