Algebra Winter Notes

by Camila Restrepo

Last updated January 12, 2024

Week 1

Introduction to Groups

Definition of a group:
A **group** G is a nonempty set together with a multiplication $G \times G \to G$ satisfying

1. $(ab)c = a(bc) \forall a, b, c, \in G$, (Associativity)
2. there exists $e \in G$ such that $ea = ae = a \forall a \in G$, (Identity)
3. and for every $a \in G$ there exists $b \in G$ such that $ab = ba = e$. (Inverse)

Example of a group:
Let $\mathbb{R}^* = \mathbb{R}^\dagger = \{a \in \mathbb{R} : a \neq 0\}$ together with multiplication on $\mathbb{R}$.
Associativity is immediate.
The identity is $1 \in \mathbb{R}^*$.
For every $a \in \mathbb{R}^*$, $\frac{1}{a} \in \mathbb{R}$ and $a(\frac{1}{a}) = \frac{1}{a}(a) = 1$.
So $\mathbb{R}^*$ is a group.

Remark: When we need to highlight the group multiplication we write a group as a pair of the set and the multiplication, e.g., $(\mathbb{R}, +), (\mathbb{R}, \cdot)$.
From now on, G is **always** a group.

Theorem 1.1
There is a unique identity element in G.

Theorem 1.2 Cancellation
Suppose $ba = ca$ for $a, b, c \in G$. Then $b = c$

Proof. Let $d \in G$ be an inverse for a, i.e. $da = ad = e$. Multiplying on the right by d, we obtain

$$\begin{aligned}(ba)d = (ca)d &\implies b(ad) = c(ad)\\ &\implies be = ce\\ &\implies b = c.\end{aligned}$$

□

Theorem 1.3 Uniqueness of Inverses
For every $a \in G$ there is a unique element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

Proof. Suppose $a \in G$ and $b, b' \in G$ are inverses of a, then

$$ba = e = b'a \implies b = b'$$

(by theorem 1.2) □

Example of inverses in different groups:

.

1. For $b \in \mathbb{R}^*$, $b^{-1} = \frac{1}{b}$.
2. For $b \in \mathbb{R}$ under addition $b^{-1} = -b$.
3. For $b \in \mathbb{Z}_n$, $b^{-1} = n - b$.

Example of groups using a field F:

.

1. $(F, +)$ is a group (Imitate $(\mathbb{R}, +)$).
2. $(F^*, \cdot)$ where $F^* = F^\dagger = \{a \in F : a \neq 0\}$ is a group. In particular, if p is a prime number, then $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ is a group.
3. The set of $m \times n$ matrices with entries in F, $M_{mn}(F)$ is a group under addition. When $n = 1$, $M_{m1}(F) = F^m$.
4. The set of invertible $m \times n$ matrices with entries in F, $GL(n, F) = \{A \in M_{mn}(F) : \det(A) \neq 0\}$ together with matrix multiplication is called (rank n) **general linear group** (over F). The identity matrix $I \in GL(n, F)$ is the identity. $\det(A) \neq 0 \implies \exists A^{-1} \in GL(n, F)$ such that $AA^{-1} = A^{-1}A = I$.

Example of the symmetries of the equilateral triangle:
Let $\sigma =$ flip through the vertical axis. Let $\rho =$ rotation by $\frac{2\pi}{3}$.
We can compose two symmetries, e.g., $\sigma\rho = \sigma \cdot \rho$.

We can show that the symmetries given by σ and ρ under composition are $\{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ where $e =$ doing nothing.
We call this set D_3. It forms a group under composition. Clearly $\rho^3 = \rho\rho\rho = e$, $\sigma^2 = \sigma\sigma = e$, and $\sigma\rho\sigma = \rho^2 = \rho^{-1}$.

Definition of a dihedral group:
The **dihedral group** of order $2n$ is defined by

$$D_n = \{e, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}$$

where $p^n = e$, $\sigma^2 = e$, and $\sigma\rho\sigma = \rho^{-1}$. This is a group with the multiplication given by $\sigma\rho\sigma = \rho^{-1}$.

Remark: D_n is the group of symmetries of a regular n-gon.

Definition of an Abelian Group:
A group G is **abelian (commutative)** if $ab = ba$ for all $a, b \in G$

Example of classifying groups:

.

1. $(F, +)$ where F is a field is Abelian.
2. $(F^*, \cdot)$ where F is a field is Abelian.
3. $(M_{mn}(F), +)$ is Abelian.
4. $(GL(n, F), \cdot)$ is not Abelian.
5. D_n is not Abelian.

Definition of the group of units:
Let $n \geq 2$ and $U(n) = \{1 \leq k \leq n-1 : \gcd(k, n) = 1\}$.
$U(n)$ is called the **group of units** of $\mathbb{Z}_n$

Recall Facts about $d = \gcd(a, b)$*: .*

1. $d \mid a$ and $d \mid b$, and d is the largest integer with this property
2. There exists $l, m \in \mathbb{Z}$ such that $\gcd(a, b) = la + mb$
3. $\gcd(a, b)$ is the smallest positive $\mathbb{Z}$-linear combination of a and b.
4. If $f \mid a$ and $f \mid b$ then f divides $\gcd(a, b) = la + mb \implies f \mid d$

Example of $U(n)$ together with multiplication $\mod n$ is a group:
Facts 2 and 3 tell us that $\gcd(k, n) = 1 \iff \exists l, m \in \mathbb{Z}$ such that $lk + mn = 1$.
So $U(2) = \{1\}, U(3) = \{1, 2\}, U(4) = \{1, 3\}, U(5) = \{1, 2, 3, 4\}$, etc.
So $U(p) = \{1, \ldots, p-1\} = \mathbb{Z}_p^*$ where p is prime.

Definition of exponentiation:
Suppose $g \in G$.

1. $g^0 = e$
2. $g^n = g \cdot \dots \cdot g$ (n times)
3. $g^{-n} = (g^{-1})^n$

Theorem 1.4 Socks and Shoes
Suppose $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$ (only relevant for non-abelian groups)

Proof.

$$(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e$$
$$(b^{-1}a^{-1})(ab) = b^{-1}eb = b^{-1}b = e$$

□

Definition of the order of a group and its elements:
The number of elements in G is called the **order** of G. Suppose $a \in G$. Then the **order of a** is the largest positive integer n such that $a^n = e$. If no such integer exists, we say a has **infinite order**. We denote the order of a by $|a|$.

Example of the order of $\{e\}$:
We know $|\{e\}| = 1$, and $e^1 = e \implies |e| = 1$

Example of the order of $\mathbb{R}^*$:
$\mathbb{R}^*$ is an infinite group so it has infinite order.
Obviously, $|1| = 1$.
$|-1| = 2$ since $(-1)^2 = 1$ and $(-1)^1 \neq 1$.
All other real numbers in $\mathbb{R}^*$ have infinite order.

Example of the order of D_3:
$|D_3| = 6$.
$|\sigma| = 2, |\rho| = 3, \left|\rho^2\right| = 3, |\sigma\rho| = 2, \left|\sigma\rho^2\right| = 2$.

Definition of a subgroup:
A **subgroup** of G is a subset $H \subseteq G$ which is a group under the same group multiplication as G.

Example of subgroups:

.

1. $\{\pm 1\} \subseteq \mathbb{R}^*$ is a subgroup
2. $\mathbb{Z}_5 \subseteq \mathbb{Z}$ is not a subgroup of $\mathbb{Z}$ since they have different group multiplications

Theorem 1.5 2-step subgroup test
Suppose H is a non-empty subset of G. Then H is a subgroup of G if and only if:

1. $a, b \in H \implies ab \in H$ (closure under multiplication)
2. $a \in H \implies a^{-1} \in H$ (closure under inverse)

Theorem 1.6 1-test subgroup test
$\emptyset \neq H \subseteq G$ is a subgroup $\iff a, b \in H \implies ab^{-1} \in H$

Proof. The forward direction is immediate.
" $\impliedby$ " Suppose 1 and 2 hold. 1 tells us that the group multiplication on G restricts to a multiplicationon H. The associativity of this multiplication on H is inherited from the associativity of the group multiplication on G.
By 1 and 2, for any $a \in H$, $a^{-1} in H$ and $e = aa^{-1} \in H$. Therefore $e \in H$.
Finally, 2 is the inverse axiom for H. $\square$

Example of showing subgroup-ness:
Let $\mu_4 = \left\{a \in \mathbb{C}^* : a^4 = 1\right\} = \{1, -1, i, -i\}$.
$\mu_4 \neq \emptyset$.
$a, b \in \mu_4 \implies (ab)^4 = a^4 b^4 = (1)(1) = 1 \implies ab \in \mu_4$
$a \in \mu_4 \implies (a^{-1})^4 = a^{-4} = (a^4)^{-1} = 1^{-1} = 1 \implies a^{-1} \in \mu_4$