Algebra Winter Notes

by Camila Restrepo

Last updated January 18, 2024

Note: Theorem numbers come from the order they are presented in lecture, and do not correspond to any textbook or written course material.

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 $\mathbb{R}^\times = \mathbb{R}^\dagger = \{a \in \mathbb{R} : a \neq 0\}$ together with multiplication on $\mathbb{R}$.
Associativity is immediate.
The identity is $1 \in \mathbb{R}^\times$.
For every $a \in \mathbb{R}^\times$, $\frac{1}{a} \in \mathbb{R}$ and $a(\frac{1}{a}) = \frac{1}{a}(a) = 1$.
So $\mathbb{R}^\times$ 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 $b \in \mathbb{R}^{\times}$, $b^{-1} = \frac{1}{b}$.
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. $(F^{\times}, \cdot)$ where $F^{\times} = F^{\dagger} = \{a \in F : a \neq 0\}$ is a group. In particular, if p is a prime number, then $\mathbb{Z}_p^{\times} = \{1, \ldots, p-1\}$ 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 σ = flip through the vertical axis. Let ρ = 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 $\left\{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\right\}$ 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

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

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. $(F^\times, \cdot)$ 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 $U(p) = \{1, \ldots, p-1\} = \mathbb{Z}_p^\times$ where p is prime.

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

1. $g^0 = e$
2. $g^n = g \cdot \cdots \cdot g$ (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.

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

$\square$

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 $\mathbb{R}^\times$:
$\mathbb{R}^\times$ 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 $\mathbb{R}^\times$ 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. $\{\pm 1\} \subseteq \mathbb{R}^{\times}$ 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.
" $\Longleftarrow$ " 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 $a \in H$, $a^{-1} inH$ and $e = aa^{-1} \in H$. Therefore $e \in H$.
Finally, 2 is the inverse axiom for H. □

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

Theorem 1.7 Finite subgroup test
Suppose $H \neq \emptyset$ is a finite subset $H \subseteq G$. Then H is a subgroup $\iff$ $a, b \in H \implies ab \in H$.

Proof. " $\implies$ " Follows from 2-step subgroup test.
" $\impliedby$ " By the 2-step subgroup test it is enough to show that if $a, b \in H \implies ab \in H$ then $b \in H \implies b^{-1} \in H$ also holds. Suppose $a, b \in H \implies ab \in H$ (*). Suppose $e \neq b \in H$. Let's prove $b^{-1} \in H$
By (*), $b^2 = bb \in H$, and by induction, $b^n \in H$ for all $n \geq 1$.
Since H is a finite set, $b^k = b^j$ for some $k > j \geq 1 \implies b^k b^{-j} = b^j b^{-k} = e \implies b^{k-j} = e$ for $k - j \geq 1$.
So $b^{-1} = b^{k-j-1}$. $k - j - 1$ cannot be zero, since then $b = e$. So $k - j - 1 \geq 1$ and so $b^{-1} = b^{k-j-1} \in H$. If $b = e \in H$, then its inverse (itself) is obviously also in H. $\square$

Example of a finite subgroup:
Consider $\{1, i, -1, -i\} \subseteq \mathbb{C}^{\times}$. By the finite subgroup test, it suffices to show that $\{1, i, -1, -i\}$ is closed under multiplication to prove that it is a subgroup. This can be done by brute force.

Week 2

Cyclic Subgroups

Definition of a cyclic group:
A group G is called **cyclic** if there is an element $a \in G$ such that $G = \{a^j : j \in \mathbb{Z}\}$. a is called a **generator** of G. We indicate that G is a cyclic group generated by a with the notation $G =< a >$.

Theorem 2.1
Suppose $a \in G$. Then $< a >$ is a subgroup of G.

Proof. Suppose $a^m, a^n \in < a >$ where $m, n \in \mathbb{Z}$. Then $a^m a^n = a^{m+n} \in < a >$ since $m + n \in \mathbb{Z}$. Also $a^{-m} \in < a >$ for all m since $-m \in \mathbb{Z}$, and $a^m a^{-m} = a^0 = e = a^0 = a^{-m} a^m$.
By the 2-step subgroup test $< a >$ is a subgroup. $\square$

Definition of a cyclic subgroup:
The subgroup $< a > \subseteq G$ is called the **cyclic subgroup** generated by $a \in G$.

Example of generators:
Take $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ together with addition mod 6.
$\mathbb{Z}_6 =< 1 >$ since $n(1) = n \mod 6$. Note that we also have $\mathbb{Z}_6 =< 5 >$.

Remark: In general, $\mathbb{Z}_n$ is cyclic and generated by $< -1 >$. All finite cyclic are isomorphic to Z_n for some n.
Remark: For $a \in G$, $< a >=< a^{-1} >$.

Example of the integers:
Take $G = \mathbb{Z}$.

$< 1 >= \{j1 : j \in \mathbb{Z}\} = \mathbb{Z}$.
$< 2 >= \{j2 : j \in \mathbb{Z}\} =$ even numbers $\subset \mathbb{Z}$.
$< m >= \{jm : j \in \mathbb{Z}\} =$ integers divisible by m for $m \neq 0$.
$< 0 >= \{0\}$.

Remark: Infinite cyclic groups are all isomorphic to $\mathbb{Z}$.

Definition of the centre of a group:
The **centre** of G is the subset

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

i.e., the elements that commute with everything in G.

Theorem 2.2
$Z(G)$ is a subgroup of G.

Proof. Suppose $x, y \in Z(G) and a \in G$. Then $(xy)a = x(ya) = xay = axy = a(xy)$. Therefore $xy \in Z(G)$.
Moreover, $xa = ax \implies x^{-1}xa = x^{-1}ax \implies a = x^{-1}ax \implies ax^{-1} = x^{-1}axx^{-1} \implies ax^{-1} = x^{-1}a \implies x^{-1} \in Z(G)$.
By the 2-step subgroup test, $Z(G)$ is a subgroup of G. $\square$

Remark:

1. G is abelian $\iff Z(G) = G$
2. $Z(G)$ is abelian (even when G is not)
3. $Z(D_3) = \{e\}$ (brute force)
4. $x \in Z(G) \iff xax^{-1} = a$ for all $a \in G \iff axa^{-1} = x$ for all $a \in G$

Example of a non-trivial center:
$Z(GL(2,\mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R}^\times \right\}$

Definition of the centralizer:
Fix $b \in G$. The **centralizer** of b in G is

$$\begin{aligned} C_G(b) = C(b) &= \{a \in G : ab = ba\} \\ &= \left\{a \in G : aba^{-1} = b\right\} \end{aligned}$$

Theorem 2.3
For any $b \in G$, $C_G(b)$ is a subgroup.

Proof. Subgroup test. ☐

Remark:

1. $C_G(e) = G$
2. $C_G(b) = G \iff b \in Z(G)$
3. $e \in C_G(b)$, $< b > \subseteq C_G(b)$

Example of a centralizer:
$C_{GL(2,\mathbb{R})}\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = \left\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R}^\times\right\}$

Recall: G is cyclic if $G =< a >= \left\{a^j : j \in \mathbb{Z}\right\}$ for some $a \in G$.

Theorem 2.4
Suppose $a \in G$. Then

1. If $|a| = \infty$, then $a^k = a^j \iff j = k$
2. If $|a| = n$, then $a^k = a^j \iff n$ divides $k - j$

Proof.

1. Suppose $|a| = \infty$. This means $a^n \neq e$ for any $n \geq 1$. Suppose now $a^k = a^j$ with $k \geq j$. Then $a^k a^{-j} = aja^{-j} = e \implies a^{k-j}$ for $k - j \geq 0$. Since $a^n \neq e \forall n \geq 1$, we have $k - j = 0 \implies k = j$.
2. Suppose $|a| = n$. This means $a^n = e$ and n is the least positive number satisfying this equation. Suppose $a^k = a^j$ with $k \geq j$. Then $a^{k-j} = e$ where $k - j \geq 0$. By definition of n, $n \leq k - j$. By the division algorithm, $k - j = qn + r$ where $q, r \in \mathbb{Z}$ are unique and $0 \leq r \leq n - 1$.
   $e = a^{k-j} = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r$, so $r = 0$ by the minimality of n, and so $k - j = qn \implies \frac{k-j}{n} = q \in Z \implies n$ divides $k - j$.
   Conversely if $qn = k - j$, then $a^{k-j} = (a^n)^q = e^q = e \implies a^k = a^j$.

☐

Remark: In part 2., n divides $k - j \iff (k - j) \mod n = 0 \iff k \mod n = j \mod n$

Corollary 2.5
Suppose $|a|\,n$. Then $a^k = e$ for some $k \in \mathbb{Z} \iff$ k is a multiple of $|a|$

Proof. Suppose $a^k = e$. Then $a^k = a^0$, so n divides $k - 0 = k$. ☐

Corollary 2.6
Suppose $a \in G$. Then

1. If $|a| = n$ then $< a >= \left\{e, a^1, a^2, \ldots, a^{n-1}\right\}$ and $|< a >| = |a|$.
2. If $|a| = \infty$, then $< a >$ is infinite and $|< a >| = |a| = \infty$

Proof. Didn't take notes for this one. ☐

Corollary 2.7
Suppose G is a finite group and $a, b \in G$. Then

1. $|a|\,, |b|$ are finite
2. If $ab = ba$ then $|ab|$ divides $|a|\,|b|$

Proof.

1. Suppose by way of contradiction that $|a|$ is infinite. Then $< a >\subseteq G$ is infinite. But G is finite so $|< a >| \leq |G|$ is a contradiction.
2. $(ab)^{|a||b|} = a^{|a||b|}b^{|a||b|} = (a^{|a|})^{|b|}(b^{|b|})^{|a|} = e^{|b|}e^{|a|} = e$

☐

2 examples omitted. Sorry, I'm prepping for my tutorial later!

Theorem 2.8
Suppose $a \in G$ and $|a| = n$. Then for any $k \geq 1$, $< a^k >=< a^{\gcd(n,k)} >$ and $\left|a^k\right| = \frac{n}{\gcd(n,k)}$

Theorem 2.9 Fundamental Theorem of Cyclic Groups
Suppose $G =< a >$ is cyclic and $|G| = n$. Then

1. Every subgroup of H is cyclic and $k = |H|$ divides $n = |G|$, i.e., k is a divisor of n
2. For every divisor k of n, there is a unique subgroup of G of order k and it is equal to $< a^{\frac{n}{k}} >$

Proof. Suppose H is a subgroup of G and $H \neq< e >$. Let $m \geq 1$ be the least power of a such that $a^m \in H$. Since H is closed under multiplication and inversion, $< a^m >\subseteq H$. Suppose $a^j \in H$. By the division algorithm, $j = qm + r$ with $0 \leq r \leq m \implies a^j = (a^m)^q a^r \implies a^j (a^m)^{-q} = a^r$, so since $a^j, (a^m)^{-q} \in H$, $a^r \in H \implies r = 0$ by the minimality of m. $\square$