MATH 343 · GROUP THEORY · CHAPTER 3

Finite Groups; Subgroups

Order · Subgroup Tests · Cyclic Subgroups, Centre, Centralizers

Fahd M. Alshammari

Part 1 — Order of a Group and of an Element

GOAL. Attach two numbers to a group: how many elements it has, and how long each element takes to return to the identity.

- Both are called *order* and both are written with vertical bars — but they are different things
- The order of an element is computed by a single, mechanical procedure
- Almost every structural theorem in the rest of the course is a statement about these two numbers

Order of a Group

DEFINITION. The number of elements of a group, finite or infinite, is its **order**, written $|G|$.

- $\mathbb{Z}$ under addition has **infinite** order
- $U(10) = \{1,3,7,9\}$ under multiplication modulo 10 has order 4
- $|D_n| = 2n$, and $|D_4| = 8$
- $|\mathbb{Z}_n| = n$

A group is **finite** if it has finitely many elements.

Order of an Element

DEFINITION. The order of g in a group G is the **smallest positive integer** n with

$$g^n = e.$$

In additive notation this reads $ng = 0$. If no such integer exists, g has **infinite order**. The order of g is written $|g|$.

- The identity is the only element of order 1
- $|g| = 2$ exactly when $g \neq e$ and g is its own inverse

How to Compute the Order of an Element

To find $|g|$, compute the sequence

$$g,\ g^2,\ g^3,\ \ldots$$

until the identity appears for the **first** time. The exponent at which it appears is $|g|$. If the identity never appears, $|g|$ is infinite.

CHECK. In additive notation the same procedure reads $g,\ 2g,\ 3g,\ \ldots$ until 0 appears, and the *coefficient* is the order.

Worked Example: Orders in U(15)

$U(15) = \{1,2,4,7,8,11,13,14\}$, a group of order 8 under multiplication modulo 15.

To find $|7|$: $7^1 = 7, 7^2 = 4$, $7^3 = 13, 7^4 = 1$, so $|7| = 4$.

To find $|11|$: $11^1 = 11$, $11^2 = 1$, so $|11| = 2$.

element	1	2	4	7	8	11	13	14
order	1		2	4	4	2	4	2

A Shortcut Worth Knowing

Computing $13^1, 13^2, 13^3, 13^4$ modulo 15 is unpleasant. Instead observe that

$$13 \equiv -2 \pmod{15},$$

and then

$$13^2 \equiv (-2)^2 = 4, \qquad 13^3 \equiv (-2)(4) = -8,$$

$$13^4 \equiv (-2)(-8) = 16 \equiv 1.$$

So $|13| = 4$.

Worked Example: Orders in Z_{10}

$\mathbb{Z}_{10}$ under addition modulo 10. Here g^n means ng.

To find $|2|$: $1 \cdot 2 = 2, 2 \cdot 2 = 4, 3 \cdot 2 = 6, 4 \cdot 2 = 8, 5 \cdot 2 = 0$, so $|2| = 5$.

element	0	1	2	3	4	5	6	7	8	9
order	1	10	5	10	5	2	5	10	5	10

Elements of Infinite Order

EXAMPLE. In $\mathbb{Z}$ under addition, every nonzero element has infinite order: the sequence $a, 2a, 3a, \dots$ never reaches 0 when $a \neq 0$.

EXAMPLE. In $\mathbb{R}^*$ under multiplication, the elements of finite order are exactly 1 and -1. For any other x, the powers $x, x^2, x^3, \dots$ either grow without bound or shrink towards 0, and never return to 1.

|G| and |g| Are Different Things

- $|G| = \text{how many elements the group has}$
- $|g| = \text{how many times you must multiply } g \text{ by itself to reach } e$
  - In $U(15)$: $|U(15)| = 8$ but $|7| = 4$
  - An infinite group can contain elements of finite order — in $\mathbb{R}^*$, $|-1| = 2$
  - A finite group has **every** element of finite order

Part 2 — Subgroups and the Subgroup Tests

GOAL. Recognise when a subset of a group is itself a group, without re-checking the axioms.

- The definition, and the notation $H \leq G$
- Three tests: **one-step**, **two-step**, and **finite**
- How to prove that a subset is **not** a subgroup
- Which test to reach for, and why

Subgroups

DEFINITION. If a subset H of a group G is itself a group under the operation of G, we say H is a **subgroup** of G, written $H \leq G$.

- $H < G$ means $H \leq G$ and $H \neq G$; such an H is a **proper** subgroup
- $\{e\}$ is the **trivial** subgroup; any other subgroup is **nontrivial**
- $SL(2, \mathbb{R}) \leq GL(2, \mathbb{R})$, and $\{1, -1, i, -i\} \leq \mathbb{C}^*$

A Warning About the Operation

WARNING. $\mathbb{Z}_n$ under addition modulo n is **not** a subgroup of $\mathbb{Z}$ under addition.

The set $\{0,1,\ldots,n-1\}$ is a subset of $\mathbb{Z}$, but addition modulo n is **not the operation of** $\mathbb{Z}$. A subgroup must use the operation it inherits.

- $\{0,1,2,3\}$ with addition mod 4: $3+3=2$
- The same set inside $\mathbb{Z}$: $3+3=6$

Theorem 3.1 — One-Step Subgroup Test

> **THEOREM 3.1.** Let G be a group and H a **nonempty** subset of G. If $ab^{-1} \in H$ whenever $a, b \in H$, then $H \leq G$.
>
> In additive notation: if $a - b \in H$ whenever $a, b \in H$, then $H \leq G$.

Proof of Theorem 3.1

PROOF. Associativity is inherited from G.

Identity. H is nonempty, so pick $x \in H$. Taking $a = x$ and $b = x$ gives $e = xx^{-1} \in H$.

Inverses. Taking $a = e$ and $b = x$ gives $x^{-1} = ex^{-1} \in H$ for every $x \in H$.

Closure. Let $x, y \in H$. We now know $y^{-1} \in H$, so taking $a = x$ and $b = y^{-1}$ gives $xy = x\left(y^{-1}\right)^{-1} \in H$.

Applying the One-Step Test — Four Steps

Although it is called the *one-step* test, applying it involves four:

- Identify the property P that defines the elements of H
- Prove that the identity has property P — this shows $H \neq \varnothing$
- Assume a and b have property P
- Show that ab^{-1} has property P

Example: The Elements Satisfying $x^2 = e$

EXAMPLE. Let G be an **Abelian** group with identity e. Then

$$H = \{ x \in G \mid x^2 = e \}$$

is a subgroup of G.

PROOF. The defining property is $x^2 = e$. Since $e^2 = e$, H is nonempty. Assume $a^2 = e$ and $b^2 = e$. Because G is Abelian,

$$\left(ab^{-1}\right)^2 = ab^{-1}ab^{-1} = a^2\left(b^{-1}\right)^2 = a^2\left(b^2\right)^{-1} = ee^{-1} = e.$$

Why “Abelian” Cannot Be Dropped

COUNTEREXAMPLE. In D_4 the set of elements satisfying $x^2 = R_0$ is

$$\{R_0,\ R_{180},\ H,\ V,\ D,\ D'\},$$

six elements out of eight. It is **not** a subgroup: it is not closed, since

$$HD = R_{90} \quad \text{and} \quad R_{90}^2 = R_{180} \neq R_0.$$

Example: The Set of Squares

EXAMPLE. Let G be an Abelian group under multiplication. Then

$$H = \{\, x^2 \mid x \in G \,\}$$

— the set of all squares — is a subgroup of G.

PROOF. Since $e^2 = e$, the identity has the right form. Write two elements of H as a^2 and b^2. Because G is Abelian,

$$a^2 (b^2)^{-1} = (ab^{-1})^2,$$

which is again a square.

Theorem 3.2 — Two-Step Subgroup Test

THEOREM 3.2. Let G be a group and H a **nonempty** subset of G. If

- $ab \in H$ whenever $a, b \in H$ (closed under the operation), and
- $a^{-1} \in H$ whenever $a \in H$ (closed under inverses),

then $H \leq G$.

PROOF. Associativity is inherited, H is closed, and inverses exist in H; only the identity remains. Take any $a \in H$. Then $a^{-1} \in H$, and hence $aa^{-1} = e \in H$.

Example: Elements of Finite Order

EXAMPLE. Let G be an Abelian group. Then

$$H = \{\, x \in G \mid |x| \text{ is finite} \,\}$$

is a subgroup of G.

PROOF. $e^1 = e$, so $H \neq \varnothing$. Let $|a| = m$ and $|b| = n$. Since G is Abelian,

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e,$$

so ab has finite order. Also $\left(a^{-1}\right)^m = (a^m)^{-1} = e^{-1} = e$, so a^{-1} has finite order.

Example: The Product of Two Subgroups

EXAMPLE. Let G be an Abelian group with subgroups H and K. Then

$$HK = \{\, hk \mid h \in H,\ k \in K \,\}$$

is a subgroup of G.

PROOF. $e = ee \in HK$. Let $a = h_1k_1$ and $b = h_2k_2$. Since G is Abelian,

$$ab = h_1k_1h_2k_2 = (h_1h_2)(k_1k_2) \in HK, \qquad a^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}k_1^{-1} \in HK.$$

How to Prove a Subset Is Not a Subgroup

Any **one** of these settles it:

- Show the identity is not in the set
- Exhibit an element of the set whose inverse is not in the set
- Exhibit two elements of the set whose product is not in the set

EXAMPLE. In $\mathbb{R}^*$ under multiplication, let $H = \{x \mid x = 1 \text{ or } x \text{ is irrational}\}$ and $K = \{x \mid x \geq 1\}$. Then H fails by (3), since $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$; and K fails by (2), since $2 \in K$ but $2^{-1} \notin K$.

Theorem 3.3 — Finite Subgroup Test

THEOREM 3.3. Let H be a **nonempty finite** subset of a group G. If H is closed under the operation of G, then $H \leq G$.

PROOF. By Theorem 3.2 we need only produce inverses. If $a = e$ then $a^{-1} = a \in H$. If $a \neq e$, consider $a, a^2, a^3, \ldots$; all lie in H by closure, and H is finite, so they are not all distinct. Say $a^i = a^j$ with $i > j$. Then $a^{i-j} = e$, and since $a \neq e$ we have $i - j > 1$. Hence

$$a\,a^{i-j-1} = a^{i-j} = e, \qquad \text{so} \qquad a^{-1} = a^{i-j-1} \in H.$$

Which Test to Use

Every test requires $H \neq \varnothing$, and in practice that is shown by checking $e \in H$.

Situation	Test
H defined by an equation the elements satisfy	one-step, Thm 3.1
H defined by a form the elements have	two-step, Thm 3.2
H finite	finite, Thm 3.3 — closure alone
H infinite, closure easy, inverses hard	one-step, Thm 3.1

Part 3 — Cyclic Subgroups, the Centre, and Centralizers

GOAL. Meet the three families of subgroups that every group has, whether or not anything else is known about it.

- $\langle a \rangle$, the cyclic subgroup generated by an element
- $Z(G)$, the centre — what commutes with everything
- $C(a)$, the centralizer — what commutes with a

Each is proved to be a subgroup using one of the three tests.

Cyclic Subgroups

NOTATION. For an element a of a group G, write

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \},$$

where the exponents include the negative integers and 0, with $a^0 = e$.

THEOREM 3.4. $\langle a \rangle$ is a subgroup of G.

PROOF. $a \in \langle a \rangle$, so it is nonempty. If $a^n, a^m \in \langle a \rangle$ then $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$. Apply Theorem 3.1.

Cyclic Groups and Generators

$\langle a \rangle$ is the **cyclic subgroup of G generated by a**. If $G = \langle a \rangle$ we call G **cyclic** and a a **generator** of G. A cyclic group may have several generators.

OBSERVATION. Every cyclic group is Abelian, since

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i.$$

FORWARD REFERENCE. In Chapter 4 we prove $|\langle a \rangle| = |a|$ — the order of the subgroup generated by a equals the order of a. Do not use it yet.

Examples of Cyclic Subgroups

EXAMPLE. In $U(10)$: $3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$, and the negative powers repeat these, so

$$\langle 3\rangle = \{3,9,7,1\} = U(10).$$

Thus $U(10)$ is cyclic with generator 3.

EXAMPLE. In $\mathbb{Z}_{10}$, where a^n means na: $\langle 2\rangle = \{2,4,6,8,0\}$.

EXAMPLE. In $\mathbb{Z}$ under addition, $\langle -1\rangle = \mathbb{Z}$; every entry of the list $\ldots, -2(-1), -1(-1), 0(-1), 1(-1), \ldots$ is a different integer.

The Rotation Subgroup of D_n

EXAMPLE. In D_n let $R = R_{360/n}$. Then

$$R^n = R_{360°} = R_0, \qquad R^{n+1} = R, \qquad R^{n+2} = R^2, \ \ldots$$

and $R^{-1} = R^{n-1}$, $R^{-2} = R^{n-2}$, and so on. Hence

$$\langle R \rangle = \{ R_0, R, R^2, \ldots, R^{n-1} \},$$

a subgroup of order n — exactly half of D_n.

Example: D_3 Inside D_6

EXAMPLE. Inscribe an equilateral triangle in a regular hexagon, sharing alternate vertices. Let F be a reflection whose axis passes through a vertex of the triangle. Then

$$K = \{ R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F \}$$

is a subgroup of D_6 of order 6 — a copy of D_3 sitting inside D_6.

The Subgroup Generated by a Set

DEFINITION. For a subset S of a group G, $\langle S \rangle$ is the **smallest** subgroup of G containing S: it contains S, and it is contained in every subgroup of G that contains S.

EXAMPLES.

- In $\mathbb{Z}_{20}$: $\langle 8,14 \rangle = \{0,2,4,\dots,18\} = \langle 2 \rangle$
- In $\mathbb{Z}$: $\langle 8,13 \rangle = \mathbb{Z}$
- In D_4: $\langle H, V \rangle = \{R_0, R_{180}, H, V\}$, while $\langle R_{90}, V \rangle = D_4$
- In $\mathbb{C}^*$: $\langle 1, i \rangle = \{1, -1, i, -i\} = \langle i \rangle$

The Centre of a Group

DEFINITION. The **centre** $Z(G)$ of a group G is the set of elements that commute with every element of G:

$$Z(G) = \{\, a \in G \mid ax = xa \ \text{ for all } x \in G \,\}.$$

THEOREM 3.5. $Z(G)$ is a subgroup of G.

- $Z(G) = G$ exactly when G is Abelian
- $Z(D_4) = \{R_0, R_{180}\}$

Proof of Theorem 3.5

PROOF. Clearly $e \in Z(G)$, so $Z(G) \neq \varnothing$. We use the two-step test.

Closure. Let $a, b \in Z(G)$. For every $x \in G$,

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Inverses. Let $a \in Z(G)$, so $ax = xa$ for all x. Multiplying on the left and right by a^{-1},

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \;\Rightarrow\; xa^{-1} = a^{-1}x.$$

The Centre of a Dihedral Group

EXAMPLE. For $n \geq 3$,

$$Z(D_n) = \begin{cases} \{R_0, R_{180}\} & n \text{ even}, \\ \{R_0\} & n \text{ odd}. \end{cases}$$

WHY. Every rotation is a power of $R_{360/n}$, so rotations commute with rotations. For a rotation R and a reflection F, RF is a reflection, so $RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$. Hence R and F commute exactly when $FR = FR^{-1}$, that is, $R = R^{-1}$ — which happens only for R_0 and R_{180}, and $R_{180} \in D_n$ only when n is even.

Centralizers

DEFINITION. For a fixed a in a group G, the **centralizer of a in G** is

$$C(a) = \{\, g \in G \mid ga = ag \,\}.$$

THEOREM 3.6. For each $a \in G$, $C(a)$ is a subgroup of G.

- The proof is close to that of Theorem 3.5 and is left as Exercise 47 — which is on your exercise list
- Every element commutes with all of its own powers, so $\langle a \rangle \subseteq C(a)$

The Centralizers in D_4

EXAMPLE. In D_4,

$$C(R_0) = D_4 = C(R_{180}),$$
$$C(R_{90}) = \{R_0, R_{90}, R_{180}, R_{270}\} = C(R_{270}),$$
$$C(H) = \{R_0, H, R_{180}, V\} = C(V),$$
$$C(D) = \{R_0, D, R_{180}, D'\} = C(D').$$

Each one is a subgroup — as Theorem 3.6 guarantees.

How the Three Fit Together

For every a in a group G:

$$Z(G) \;\subseteq\; C(a) \;\subseteq\; G.$$

- G is Abelian **if and only if** $C(a) = G$ for every a in G
- $Z(G)$ is the intersection of all the centralizers: $Z(G) = \bigcap_{a\in G} C(a)$
- $\langle a\rangle \subseteq C(a)$ always, since a commutes with its own powers

The Subgroups of D_4

D_4 has exactly **ten** subgroups, arranged by order:

- order 1: $\{R_0\}$
- order 2: $\langle R_{180}\rangle, \langle H\rangle, \langle V\rangle, \langle D\rangle, \langle D'\rangle$
- order 4: $\langle R_{90}\rangle, \{R_0, R_{180}, H, V\}, \{R_0, R_{180}, D, D'\}$
- order 8: D_4

What to Take Away

- $|G|$ counts elements; $|g|$ is the least $n > 0$ with $g^n = e$. Same notation, different objects
- $H \leq G$ is checked by a **test**, never by rechecking the axioms: one-step ($ab^{-1} \in H$), two-step (closed under product and inverse), finite (closure alone)
- Every test needs $H \neq \varnothing$ — show $e \in H$
- $\langle a \rangle, Z(G)$ and $C(a)$ are subgroups of every group, with $Z(G) \subseteq C(a)$
- $Z(D_n) = \{R_0, R_{180}\}$ for n even and $\{R_0\}$ for n odd