# Modern Algebra 1 — Homework 1 Solutions

Spring 2026 | Due: April 7

KIM Süngsoo · 2022-14643

## Problem 1

> **Claim.** *If $G$ is a finite group with identity $e$ and $|G|$ is even, then there exists $a \neq e$ in $G$ such that $a * a = e$.*

***Proof.***

Define the *inversion map* $\iota : G \to G$ by $\iota(a) = a^{-1}$. Since $(a^{-1})^{-1} = a$ for every $a \in G$, this map is an involution: $\iota^2 = \mathrm{id}_G$.

The involution $\iota$ partitions $G$ into orbits under the action of $\langle \iota \rangle \cong \mathbb{Z}_2$. Each orbit has size 1 or 2:

- **Fixed points** (size-1 orbits): elements $a \in G$ with $\iota(a) = a$, i.e. $a^{-1} = a$, equivalently $a^2 = e$. Let $F = \mathrm{Fix}(\iota) = \{a \in G : a^2 = e\}$.
- **Free orbits** (size-2 orbits): pairs $\{a, a^{-1}\}$ with $a \neq a^{-1}$.

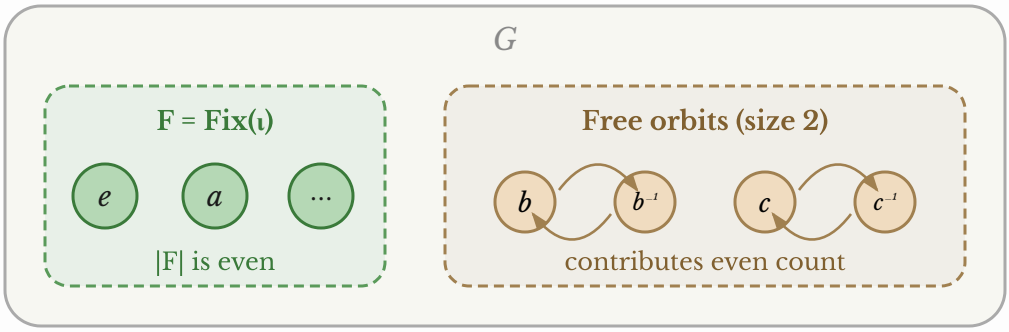



*Figure 1. Partition of $G$ under the inversion involution $\iota : a \mapsto a^{-1}$.*

Since every element lies in exactly one orbit, we have the orbit-counting equation:

$$|G| \;=\; |F| \;+\; 2k$$

for some non-negative integer $k$ (the number of free orbits). Because $|G|$ is even and $2k$ is even, $|F|$ must also be **even**.

Now $e \in F$ (since $e^2 = e$), so $|F| \geq 1$. But $|F|$ is even, which forces $|F| \geq 2$. Therefore there exists some $a \in F$ with $a \neq e$, meaning $a^2 = e$.

■

> **Remark (categorical perspective).** The existence of an element of order 2 is equivalent to the existence of a non-trivial group homomorphism $\mathbb{Z}_2 \to G$. In the category **Grp**, this is encoded by the following commutative diagram, where $\varphi(\bar{1}) = a$ with $a^2 = e$:
>
> $$\begin{array}{ccc} \mathbb{Z}_2 & \xrightarrow{\exists\, \varphi \neq 0} & G \\ {\scriptstyle \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \iota} \\ \mathbb{Z}_2 & \xrightarrow[\varphi]{} & G \end{array}$$
>
> The diagram commutes because $\iota(\varphi(\bar{1})) = a^{-1} = a = \varphi(\bar{1})$, i.e. $\varphi$ maps into the fixed-point set of $\iota$. This problem is essentially the $p = 2$ case of Cauchy's theorem.

---

## Problem 2

> **Claim.** *The number of cycles $\sigma$ in $S_5$ such that $\sigma^2$ is also a cycle (counting the identity as a cycle) is* **55**.

***Proof.***

**Definition.** A *$k$-cycle* in $S_n$ is a permutation $\sigma$ of the form $\sigma = (a_1\ a_2\ \cdots\ a_k)$, meaning $\sigma(a_i) = a_{i+1}$ for $1 \leq i \leq k-1$, $\sigma(a_k) = a_1$, and $\sigma$ fixes all elements outside $\{a_1, \ldots, a_k\}$. A 1-cycle is the identity, and a 2-cycle is a transposition.

> **Lemma.** *Let $\sigma = (a_1\ a_2\ \cdots\ a_k)$ be a $k$-cycle. Then $\sigma^2$ consists of exactly $d = \gcd(2,k)$ disjoint cycles, each of length $k/d$. In particular, $\sigma^2$ is a cycle if and only if $\gcd(2,k) = 1$ (i.e., $k$ is odd) or $k \leq 2$.*

***Proof of Lemma.***

By definition, $\sigma(a_i) = a_{i+1 \pmod k}$, so $\sigma^2(a_i) = a_{i+2 \pmod k}$. Thus $\sigma^2$ acts on the index set $\mathbb{Z}/k\mathbb{Z}$ by the map $i \mapsto i+2$. The orbit of index $i$ under this map is $\{i,\ i+2,\ i+4,\ \ldots\}$ taken modulo $k$.

The size of this orbit equals the order of $\bar{2}$ in $\mathbb{Z}/k\mathbb{Z}$, which is $k/\gcd(2,k)$. The number of distinct orbits is $\gcd(2,k)$, since $|\mathbb{Z}/k\mathbb{Z}|$ = (number of orbits) $\times$ (orbit size). Concretely:

- $k$ **odd** ($\gcd(2,k) = 1$): the single orbit $\{0, 2, 4, \ldots, k-1, 1, 3, \ldots\}$ visits every index, so $\sigma^2$ is a $k$-cycle.
- $k$ **even** ($\gcd(2,k) = 2$): there are two orbits — the even indices $\{0, 2, 4, \ldots, k-2\}$ and the odd indices $\{1, 3, 5, \ldots, k-1\}$ — each of size $k/2$. So $\sigma^2$ is a product of two disjoint $(k/2)$-cycles.

Hence $\sigma^2$ is a single cycle precisely when $k$ is odd (giving a $k$-cycle) or $k \leq 2$ (where $\sigma^2 = \mathrm{id}$, which we count as a cycle).

■

Applying the lemma, $\sigma^2$ is a cycle for $k \in \{1, 2, 3, 5\}$ and fails to be a cycle for $k = 4$ (where $\sigma^2$ splits into two transpositions).

We now enumerate each case in $S_5$. Recall that the number of $k$-cycles in $S_n$ is $\binom{n}{k} \cdot (k-1)!$.

| **Length $k$** | **$\sigma^2$ structure** | **$\sigma^2$ a cycle?** | **Count in $S_5$** |
|---|---|---|---|
| 1 (identity) | identity | Yes | 1 |
| 2 (transposition) | identity | Yes | $\binom{5}{2} \cdot 1! = 10$ |

| | | | |
|---|---|---|---|
| 3 | 3-cycle | Yes | $\binom{5}{3} \cdot 2! = 20$ |
| 4 | product of two 2-cycles | **No** | 0 (excluded) |
| 5 | 5-cycle | Yes | $\binom{5}{5} \cdot 4! = 24$ |

**Verification for $k = 3$:**

Let $\sigma = (1\ 2\ 3)$. Then $\sigma^2(1) = 3$, $\sigma^2(3) = 2$, $\sigma^2(2) = 1$, giving $\sigma^2 = (1\ 3\ 2)$, which is indeed a 3-cycle.

**Verification for $k = 4$:**

Let $\sigma = (1\ 2\ 3\ 4)$. Then $\sigma^2(1) = 3$, $\sigma^2(3) = 1$, $\sigma^2(2) = 4$, $\sigma^2(4) = 2$, giving $\sigma^2 = (1\ 3)(2\ 4)$, which is *not* a single cycle.

**Verification for $k = 5$:**

Let $\sigma = (1\ 2\ 3\ 4\ 5)$. Then:

$$\sigma^2(1) = 3, \quad \sigma^2(3) = 5, \quad \sigma^2(5) = 2, \quad \sigma^2(2) = 4, \quad \sigma^2(4) = 1,$$

giving $\sigma^2 = (1\ 3\ 5\ 2\ 4)$, which is indeed a 5-cycle.

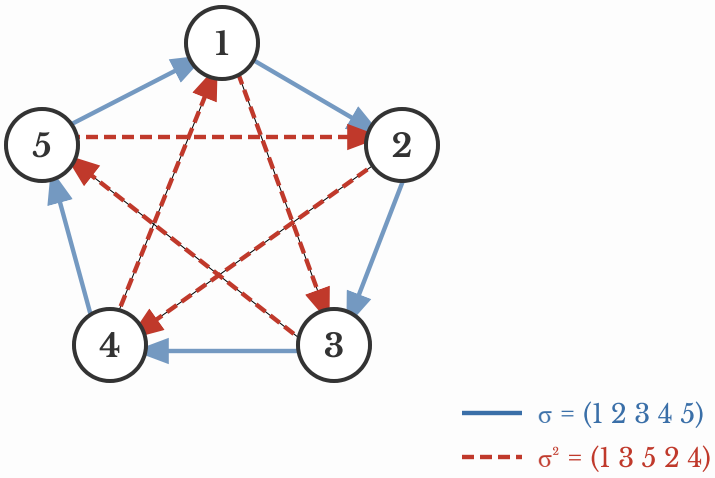



*Figure 2. Pentagon vs. pentagram: $\sigma$ traverses edges (blue, connected), $\sigma^2$ traverses the star (red, still connected — a single cycle).*

**Total:**

$$1 + 10 + 20 + 0 + 24 \;=\; \boxed{55}$$

■

**Remark (generalization).** The lemma generalizes: for a $k$-cycle $\sigma$ and any positive integer $m$, the permutation $\sigma^m$ consists of $\gcd(m,k)$ disjoint cycles each of length $k/\gcd(m,k)$. In particular, $\sigma^m$ is again a cycle if and only if $\gcd(m,k) = 1$ or $k \mid m$ (where $\sigma^m = \mathrm{id}$). The proof is identical — $\sigma^m$ acts on indices by $i \mapsto i + m \pmod{k}$, and the orbit size of this map is $k/\gcd(m,k)$.

For the present problem ($m = 2$), this reduces to: $\sigma^2$ is a cycle iff $k$ is odd (or $k \le 2$ trivially). One could therefore bypass the case analysis entirely and write: the qualifying cycles are precisely those of odd length, plus the transpositions. This gives

$$\underbrace{1}_{\mathrm{id}} + \underbrace{\binom{5}{2}\cdot 1!}_{k=2} + \underbrace{\binom{5}{3}\cdot 2!}_{k=3} + \underbrace{\binom{5}{5}\cdot 4!}_{k=5} \;=\; 1 + 10 + 20 + 24 = 55.$$

---

## Problem 3

**Theorem (Fundamental Theorem of Finitely Generated Abelian Groups).** *Every finitely generated abelian group $G$ is isomorphic to*

$$G \;\cong\; \mathbb{Z}^{\,r} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

*where $r \ge 0$ and $n_1 \mid n_2 \mid \cdots \mid n_s$ with each $n_i > 1$. The integer $r$ (the free rank) and the integers $n_1, \ldots, n_s$ (the invariant factors) are uniquely determined by $G$.*

*Equivalently, $G$ can be decomposed into elementary divisors (prime-power cyclic factors), and the two decompositions determine each other.*

**Claim.** *The invariant factor decomposition of $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20}$ is $\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{60}$, i.e., $m_1 = 2$, $m_2 = 12$, $m_3 = 60$.*

*Proof.*

**Step 1: Primary (elementary divisor) decomposition via the Chinese Remainder Theorem.**

We use the following form of the CRT for cyclic groups:

> **Chinese Remainder Theorem.** *If $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is the prime factorization of $n$, then*
>
> $$\mathbb{Z}_n \;\cong\; \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_s^{a_s}}.$$
>
> *The isomorphism is given by the map $[x]_n \mapsto \left([x]_{p_1^{a_1}}, [x]_{p_2^{a_2}}, \ldots, [x]_{p_s^{a_s}}\right)$, which is well-defined because $p_i^{a_i} \mid n$ for each $i$. This is an isomorphism precisely because $\gcd(p_i^{a_i}, p_j^{a_j}) = 1$ for $i \neq j$.*

We apply this to each factor. First, the prime factorizations:

$$6 = 2 \cdot 3, \qquad 12 = 2^2 \cdot 3, \qquad 20 = 2^2 \cdot 5.$$

Applying the CRT to each:

- $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \quad (\text{since } \gcd(2,3) = 1)$
- $\mathbb{Z}_{12} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_3 \quad (\text{since } \gcd(4,3) = 1)$
- $\mathbb{Z}_{20} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_5 = \mathbb{Z}_4 \times \mathbb{Z}_5 \quad (\text{since } \gcd(4,5) = 1)$

Now substitute into the original product and rearrange by prime:

$$\begin{aligned} \mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} &\cong (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_5) \\ &= \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4}_{\text{2-primary component } G_2} \times \underbrace{\mathbb{Z}_3 \times \mathbb{Z}_3}_{\text{3-primary component } G_3} \times \underbrace{\mathbb{Z}_5}_{\text{5-primary component } G_5}. \end{aligned}$$

This uses associativity and commutativity of the direct product (valid in the category of abelian groups). The *elementary divisors* of the group are exactly these prime-power factors: $2, 4, 4, 3, 3, 5$.

The overall decomposition pipeline is:

$$\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \xrightarrow{\text{CRT per factor}} G_2 \times G_3 \times G_5 \xrightarrow{\text{recombine columns}} \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3}$$

**Step 2: From elementary divisors to invariant factors.**

The passage from elementary divisors to invariant factors works as follows. For each prime $p$, list the $p$-power elementary divisors in non-decreasing order. Since different primes may contribute different numbers of factors, pad the shorter lists on the *left* with 1's so all lists reach the same length $r$ (the maximum). Then the $j$-th invariant factor $m_j$ is the product of the $j$-th entries across all primes. Because we padded on the left and each column's entries are coprime (one entry per prime), the CRT guarantees $\mathbb{Z}_{m_j} \cong \prod_p \mathbb{Z}_{p\text{-entry in column } j}$, and the divisibility $m_j \mid m_{j+1}$ follows from the non-decreasing arrangement within each row.

In our case, $r = 3$ (the 2-primary component has 3 factors, the most of any prime):

| **Prime $p$** | **Column 1 (smallest)** | **Column 2** | **Column 3 (largest)** |
|---|---|---|---|
| $p = 2$: $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ | $2^1 = 2$ | $2^2 = 4$ | $2^2 = 4$ |
| $p = 3$: $\mathbb{Z}_3 \times \mathbb{Z}_3$ | $3^0 = 1$ (pad) | $3^1 = 3$ | $3^1 = 3$ |
| $p = 5$: $\mathbb{Z}_5$ | $5^0 = 1$ (pad) | $5^0 = 1$ (pad) | $5^1 = 5$ |
| **Invariant factor $m_j = \prod_p$** | $m_1 = 2 \cdot 1 \cdot 1 = 2$ | $m_2 = 4 \cdot 3 \cdot 1 = 12$ | $m_3 = 4 \cdot 3 \cdot 5 = 60$ |

Each invariant factor recombines via CRT:

$$m_1 = 2, \qquad m_2 = 4 \cdot 3 = 12, \qquad m_3 = 4 \cdot 3 \cdot 5 = 60.$$

Equivalently: $\mathbb{Z}_2 \cong \mathbb{Z}_2,\ \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3,\ \mathbb{Z}_{60} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

**Step 3: Verification.**

We verify the divisibility chain: $m_1 \mid m_2$ since $2 \mid 12$, and $m_2 \mid m_3$ since $12 \mid 60$, as required. The product $m_1 \cdot m_2 \cdot m_3 = 2 \cdot 12 \cdot 60 = 1440 = 6 \cdot 12 \cdot 20 = |G|$ confirms the order is preserved.

As a consistency check, we reverse the process and recover the elementary divisors:

$$\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{60} \overset{\text{CRT}}{\cong} \mathbb{Z}_2 \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \;=\; \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

which agrees with the primary decomposition obtained in Step 1. By uniqueness of the invariant factor decomposition (guaranteed by the Fundamental Theorem), this is the only valid decomposition with $m_i > 1$ and $m_i \mid m_{i+1}$.

Therefore: $\boxed{m_1 = 2, \quad m_2 = 12, \quad m_3 = 60.}$

■

---

## Problem 4

> **Claim.** *Let $H, K$ be subgroups of a group $G$ satisfying:*
> *(a) every element of $G$ is of the form $hk$ for some $h \in H$, $k \in K$;*
> *(b) $hk = kh$ for all $h \in H$, $k \in K$;*
> *(c) $H \cap K = \{e\}$.*
> *Then $G \cong H \times K$.*

***Proof.***

Define the map

$$\varphi : H \times K \longrightarrow G, \qquad \varphi(h, k) = hk.$$

The key structures are captured by the following commutative diagram, where $\iota_H : H \hookrightarrow G$ and $\iota_K : K \hookrightarrow G$ are the inclusion homomorphisms and $j_H(h) = (h, e)$, $j_K(k) = (e, k)$ are the canonical embeddings:

$$\begin{array}{ccccc} H & \xrightarrow{j_H} & H \times K & \xleftarrow{j_K} & K \\ \| & & \downarrow{\scriptstyle \varphi} & & \| \\ H & \xrightarrow[\iota_H]{} & G & \xleftarrow[\iota_K]{} & K \end{array}$$

We show that $\varphi$ is an isomorphism by verifying the three required properties.

**Step 1: $\varphi$ is a homomorphism.**

Let $(h_1, k_1)$, $(h_2, k_2) \in H \times K$. On one hand:

$$\varphi\big((h_1,k_1)(h_2,k_2)\big) = \varphi(h_1h_2,\ k_1k_2) = h_1h_2 \cdot k_1k_2.$$

On the other hand:

$$\varphi(h_1,k_1)\cdot\varphi(h_2,k_2) = h_1k_1 \cdot h_2k_2 = h_1\underbrace{(k_1h_2)}_{\overset{(b)}{=}\, h_2k_1}k_2 = h_1h_2 \cdot k_1k_2.$$

The two expressions agree, so $\varphi$ is a homomorphism.

**Step 2: $\varphi$ is surjective.**

By condition (a), every $g \in G$ can be written as $g = hk$ for some $h \in H$, $k \in K$. Thus $g = \varphi(h,k)$, so $\varphi$ is surjective.

**Step 3: $\varphi$ is injective.**

Suppose $\varphi(h,k) = e_G$, i.e., $hk = e$. Then:

$$h = k^{-1}.$$

Now $h \in H$ and $k^{-1} \in K$ (since $K$ is a subgroup, closed under inverses). Therefore:

$$h = k^{-1} \in H \cap K \overset{(c)}{=} \{e\}.$$

This forces $h = e$ and $k = e$, so $\ker\varphi = \{(e,e)\}$, meaning $\varphi$ is injective.

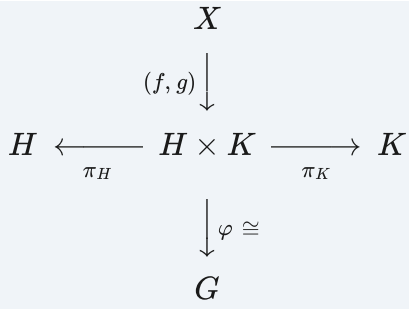
**Conclusion.**

Since $\varphi$ is a bijective homomorphism, it is an isomorphism:

$$\boxed{G \ \cong\ H \times K.}$$

■

> **Remark (universal property of the direct product in Grp).** In the category **Grp**, the direct product $H \times K$ satisfies the following universal property: for any group $X$ with homomorphisms $f : X \to H$ and $g : X \to K$, there exists a unique homomorphism $(f,g) : X \to H \times K$ making the diagram commute.




Conditions (a)–(c) assert precisely that $G$ realizes this universal property *internally*: the multiplication map $\varphi(h,k) = hk$ is the canonical comparison morphism, and the three conditions force it to be an isomorphism. This is a special case of the general principle that a group is an internal direct product if and only if the canonical map from the corresponding external direct product is an isomorphism.

**Remark (alternative proof via uniqueness of representation).** One can also prove the isomorphism by working from $G$ to $H \times K$, rather than the other direction. By (a), every $g \in G$ admits a factorization $g = hk$. We first show this factorization is *unique*: if $h_1k_1 = h_2k_2$ with $h_i \in H$, $k_i \in K$, then $h_2^{-1}h_1 = k_2k_1^{-1}$. The left side lies in $H$ and the right in $K$, so both lie in $H \cap K = \{e\}$ by (c), giving $h_1 = h_2$ and $k_1 = k_2$.

Now define $\psi : G \to H \times K$ by $\psi(g) = (h,k)$ where $g = hk$ is the unique factorization. This is well-defined by uniqueness, and is evidently the inverse of $\varphi$. To see that $\psi$ is a homomorphism (equivalently, that $\varphi$ is), one uses condition (b) exactly as in Step 1 above. This approach has the advantage of making the bijection between $G$ and $H \times K$ manifest before verifying the algebraic structure.

---

— End of Solutions —