MATH5353

Harley Caham Combest

Fa2025 Ch3 Quotient Groups and Homomorphisms Mk1

Ch 3: Historical Context

Overview. These are designed to test your memory on a few selected historical points on the basics of quotient groups and homomorphisms as presented in Ch3 of Dummit and Foote.

Before "groups": permutations and equations (1700s → early 1800s).

- **J. L. Lagrange** (Paris, 1770s–1780s). Studied permutations of polynomial roots, isolating the *parity* of permutations (even/odd) and anticipating the sign homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$ and the alternating group A_n. His orbit–stabilizer style counting presages what becomes *Lagrange's Theorem* on subgroup indices and orders.
- **A.-T. Vandermonde** and contemporaries (1770s). Worked explicitly with permutations; the fact that every permutation is a product of *transpositions* becomes standard in this era.

Birth of group thinking (early–mid 1800s).

- **A.-L. Cauchy** (Paris, 1815; 1845). Deepened the theory of permutations; proved what we now call *Cauchy's Theorem*: if a prime p divides $|G|$, then G has an element of order p. (Chapter 3 presents the abelian case early for pedagogy.)
- **É. Galois** (Paris, 1830–1832). Introduced groups to encode symmetries of roots. Emphasized subgroups stable under conjugation (*invariant* $\equiv$ *normal*) and used quotient-like reasoning. His criterion for solvability by radicals anticipates *solvable groups* via chains with abelian quotients.

Systematizing subgroups, normality, and quotients (late 1800s).

- **C. Jordan** (Paris, 1870). In *Traité des substitutions*, formalized permutations, *invariant/normal* subgroups, cosets, and laid foundations for the *Jordan–Hölder* perspective (maximal normal chains and their factors).
- **O. Hölder** (Leipzig, 1889). Proved the modern uniqueness: any two *composition series* have the same multiset of *composition factors* (up to order/isomorphism).
- **R. Dedekind**, **H. Weber**, and others (Germany, 1880s–1890s). Consolidated abstraction: standardized "normal" subgroups, clarified *quotient* constructions, and popularized the *normalizer* $N_G(H)$ and *centralizer* $C_G(H)$.

Isomorphism theorems and lattice viewpoint (1900–1930s).

- The three *Isomorphism Theorems* were implicit in 19th-century arguments (used in refinement/compare-factor proofs).
- **E. Noether** (Göttingen, 1920s). Gave a sweeping abstract formulation across algebra (groups, rings, modules), yielding the modern, unified statement of the isomorphism theorems. Chapter 3 presents the group-specialized forms.

Alternating groups and the sign map (thread through the 1800s).

- From Lagrange's parity arose the *sign* map and $A_n = \ker(\text{sgn})$. The simplicity of A_n for $n \geq 5$ (developed by late 19th century, with A_5 already in Galois's sights) becomes a pillar of finite group theory; Chapter 3 supplies the kernel/quotient machinery underpinning such results.

Why Chapter 3 matters (the "why").

- **Homomorphisms** make structure visible via maps; **kernels** and **images** encode what is forgotten and what is preserved.
- **Quotients** are controlled collapses by normal subgroups; they isolate new structure while retaining a group law.
- **Isomorphism Theorems** are the bookkeeping rules that relate subgroups, images, and preimages, enabling clean diagram chases and classification steps.
- **Lagrange & Cauchy** tie counting to structure: divisibility of orders forces existence of elements/subgroups of prescribed sizes.
- **Jordan–Hölder** gives a canonical "fingerprint" (up to order) via composition factors, guiding classification strategies.
- **Parity &** A_n provide a prototypical kernel/quotient narrative with wide ramifications.

Minimal timeline (anchor points).

- 1770s–1780s (Paris): **Lagrange** — parity, cycle thinking; subgroup-order divisibility in embryo.
- 1815–1845 (Paris): **Cauchy** — permutation theory; existence of p-torsion when $p \mid |G|$.
- 1830–1832 (Paris): **Galois** — invariant/normal subgroups; solvable chains, quotient intuition.
- 1870 (Paris): **Jordan** — invariant subgroups; early Jordan–Hölder framework.
- 1889 (Leipzig): **Hölder** — uniqueness of composition factors (modern form).
- 1920s (Göttingen): **Noether** — abstract isomorphism theorems across algebra.

Ch 3: Lingua Franca

Overview. These are designed to test your memory on the tools of the trade: the words, the axioms, the theorems, etc of the basics of quotient groups and homomorphisms as presented in Ch3 of Dummit and Foote.

Definition: Kernel of a Homomorphism.

Let $\varphi : G \to H$ be a group homomorphism. The *kernel* of φ is

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}.$$

Proposition: Basic Properties of Homomorphisms.

Let $\varphi : G \to H$ be a homomorphism. Then for all $g \in G$ and $n \in \mathbb{Z}$:

1. $\varphi(1_G) = 1_H$.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$.
3. $\varphi(g^n) = \varphi(g)^n$.
4. $\ker \varphi \leq G$.
5. $\operatorname{im} \varphi \leq H$.

Intuition. Homomorphisms carry the group law across: identities to identities, inverses to inverses, powers to powers; kernels and images inherit subgroup closure.

Proof. **Step 1.** $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G)$, hence $\varphi(1_G) = 1_H$ by cancellation in H.

Step 2. $1_H = \varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, so $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Step 3. For $n \geq 0$, use induction with multiplicativity; for $n < 0$, combine Step 2 with the positive case.

Step 4. If $x, y \in \ker \varphi$, then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H$, so $xy^{-1} \in \ker \varphi$; nonempty since $1_G \in \ker \varphi$.

Step 5. If $x = \varphi(a)$ and $y = \varphi(b)$ lie in $\operatorname{im} \varphi$, then $xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \operatorname{im} \varphi$. □

Definition: Quotient Group via a Homomorphism.

If $\varphi : G \to H$ is a homomorphism with kernel $K = \ker \varphi$, the *quotient group* G/K has as elements the fibers (i.e., the left cosets of K in G). Multiplication is defined by multiplying images in H: the product of the fibers above $a, b \in H$ is the fiber above ab.

Proposition: Fibers Are Cosets of the Kernel.

Let $\varphi : G \to H$ be a homomorphism with kernel K. If $X = \varphi^{-1}(a)$ is the fiber above $a \in H$ and $u \in X$, then $X = uK = \{uk \mid k \in K\}$; likewise $X = Ku$.

. . . . . .

Intuition. Elements mapping to the same a differ by kernel elements; each fiber is a translate of K on either side.

. . . . . .

Proof. **Step 1.** If $k \in K$, then $\varphi(uk) = \varphi(u)\varphi(k) = a \cdot 1_H = a$, so $uk \in X$; hence $uK \subseteq X$.

Step 2. If $g \in X$, then $\varphi(u^{-1}g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1_H$, so $u^{-1}g \in K$ and $g = uk \in uK$; thus $X \subseteq uK$.

Step 3. The right-coset statement is analogous. □

Definition: Left and Right Cosets.

For $N \leq G$ and $g \in G$, the *left coset* is $gN = \{gn \mid n \in N\}$ and the *right coset* is $Ng = \{ng \mid n \in N\}$. Any element of a coset is called a *representative*.

Proposition: Cosets Partition the Group; Equality Criterion.

Let $N \leq G$. The left cosets of N form a partition of G. Moreover, for $u, v \in G$,

$$uN = vN \iff v^{-1}u \in N.$$

Intuition. Cosets are translates of a subgroup; they tile G without overlap. Equality means the representatives differ by an element of N.

Proof. **Step 1.** For each $g \in G$, $g = g \cdot 1 \in gN$, so $\bigcup_{g \in G} gN = G$.

Step 2. If $uN \cap vN \neq \varnothing$, take $x = un = vm$. Then $u = vmn^{-1} \in vN$ and similarly $v \in uN$, hence $uN = vN$.

Step 3. $uN = vN \iff u \in vN \iff u = vn$ for some $n \in N \iff v^{-1}u \in N$. □

Proposition: Well-Defined Coset Multiplication and Criterion.

Let $N \leq G$.

1. The rule $(uN) \cdot (vN) = (uv)N$ is well-defined on left cosets iff $gng^{-1} \in N$ for all $g \in G$, $n \in N$.

2. If it is well-defined, this rule makes the set of left cosets a group with identity $1N$ and inverse $(gN)^{-1} = g^{-1}N$.

.....

Intuition. Changing representatives must not change the product; this forces stability under conjugation by every g.

.....

Proof. **Step 1 ($\Rightarrow$).** Assume well-defined. Take $u = 1$, $u_1 = n \in N$, $v = v_1 = g^{-1}$. Then $1 \cdot g^{-1}N = n \cdot g^{-1}N$, so $g^{-1}N = ng^{-1}N$. Hence $ng^{-1} = g^{-1}n'$ for some $n' \in N$, i.e., $gng^{-1} = n' \in N$.

Step 2 ($\Leftarrow$). Assume $gng^{-1} \in N$ for all g, n. If $u_1 = un$ and $v_1 = vm$ with $n, m \in N$, then $u_1v_1 = unvm = u(vnv^{-1})vm = (uv)(n'm)$ with $n' \in N$, so $u_1v_1 \in (uv)N$ and $(u_1N)(v_1N) = (uv)N$.

Step 3. Associativity, identity $1N$, and inverses $g^{-1}N$ descend from G. □

Definition: Normality, Conjugates, Normalizer.

For $g \in G$ and $n \in N$, the element gng^{-1} is the *conjugate* of n by g; the set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the conjugate of N. An element g *normalizes* N if $gNg^{-1} = N$. A subgroup N is *normal* in G (written $N \trianglelefteq G$) if $gNg^{-1} = N$ for all $g \in G$.

Theorem: Characterizations of Normal Subgroups.

For $N \leq G$, the following are equivalent:

1. $N \trianglelefteq G$.
2. $N_G(N) = G$.
3. $gN = Ng$ for all $g \in G$.
4. The coset product in the previous proposition is well-defined and turns the set of left cosets into a group.
5. $gNg^{-1} \subseteq N$ for all $g \in G$.

.....

Intuition. "Normal" means conjugation-stable; this is exactly what makes arithmetic mod N independent of representatives and equates left/right cosets.

.....

Proof. **Step 1.** (1)⇔(5) is the definition.

Step 2. (5)⇒(4) by the well-definedness criterion above.

Step 3. (4)⇒(3): in the coset group, gN has inverse $g^{-1}N$, so both left and right cosets represent the same element, hence $gN = Ng$.

Step 4. (3)⇒(2): $gN = Ng$ implies $gNg^{-1} = N$, so $g \in N_G(N)$ for all g.

Step 5. (2)⇒(1): If every g normalizes N, then $N \trianglelefteq G$. □

Proposition: Kernels Are Exactly Normal Subgroups.

A subgroup $N \leq G$ is normal if and only if it is the kernel of some homomorphism.

. . . . . .

Intuition. Kernels are always conjugation-stable; conversely, the natural projection has kernel exactly N when $N \trianglelefteq G$.

. . . . . .

Proof. **Step 1 ($\Rightarrow$).** If $N = \ker \varphi$, then by the fiber–coset description, left and right cosets of N coincide; thus $N \trianglelefteq G$.

Step 2 ($\Leftarrow$). If $N \trianglelefteq G$, define $\pi : G \to G/N$ by $\pi(g) = gN$. The coset product is well-defined, so π is a homomorphism and $\ker \pi = \{g \mid gN = N\} = N$. $\square$

Definition: Natural Projection and Complete Preimage.

If $N \trianglelefteq G$, the *natural projection* $\pi : G \to G/N$ is given by $\pi(g) = gN$. If $A \leq G/N$, its *complete preimage* is $\pi^{-1}(A) \leq G$.

Theorem: Lagrange's Theorem.

If G is a finite group and $H \leq G$, then $|H| \mid |G|$, and the number of left cosets of H in G is $\dfrac{|G|}{|H|}$.

Intuition. Left cosets gH tile G in equal-sized blocks, each in bijection with H via $h \mapsto gh$. Counting blocks $\times$ block size gives $|G| = k\,|H|$.

Proof. **Step 1.** For each $g \in G$, the map $H \to gH$, $h \mapsto gh$ is bijective by left-cancellation, so $|gH| = |H|$.

Step 2. Distinct left cosets are disjoint and their union is G; let there be k cosets. Then $|G| = k\,|H|$, so $|H| \mid |G|$ and $k = \dfrac{|G|}{|H|}$. □

Definition: Index of a Subgroup.

For $H \leq G$, the *index* of H in G, denoted $|G : H|$, is the number of left cosets of H in G. If G is finite, then $|G : H| = \dfrac{|G|}{|H|}$.

Corollary: Order of an Element Divides $|G|$.

If G is finite and $x \in G$, then $|x| \mid |G|$. In particular, $x^{|G|} = 1$ for all $x \in G$.

Intuition. Apply Lagrange to the cyclic subgroup $\langle x \rangle$; its size is $|x|$ and must divide $|G|$.

Proof. **Step 1.** By Lagrange with $H = \langle x \rangle$, $|\langle x \rangle| = |x|$ divides $|G|$.
Step 2. Let $|G| = m|x|$. Then $x^{|G|} = (x^{|x|})^m = 1^m = 1$. □

Corollary: Groups of Prime Order are Cyclic.

If $|G| = p$ is prime, then G is cyclic and $G \cong \mathbb{Z}_p$.

. . . . . .

Intuition. Any nonidentity element generates a nontrivial subgroup whose order must divide p, hence equals p.

. . . . . .

Proof. **Step 1.** Pick $1 \neq x \in G$. Then $|\langle x \rangle| > 1$ and $|\langle x \rangle| \mid p$, so $|\langle x \rangle| = p$.

Step 2. Hence $\langle x \rangle = G$; therefore G is cyclic. A finite cyclic group of order p is isomorphic to $\mathbb{Z}_p$. □

Proposition: A Subgroup of Index 2 is Normal.

If $H \leq G$ with $|G : H| = 2$, then $H \trianglelefteq G$.

. . . . . .

Intuition. There are exactly two left cosets: H and gH. The right cosets must also be H and one other; by pigeonhole, the "other" equals gH, so left/right cosets coincide.

. . . . . .

Proof. **Step 1.** Since $|G : H| = 2$, the left cosets are $\{H, gH\}$ for some $g \notin H$.

Step 2. The right cosets are $\{H, Hg\}$. Both gH and Hg have size $|H|$ and are disjoint from H, hence $gH = Hg$.

Step 3. For all $g \in G$, $gH = Hg$; by a standard criterion, this is equivalent to $H \trianglelefteq G$. □

Definition: Product Set HK.

For subgroups $H, K \leq G$, define $HK = \{hk \mid h \in H,\ k \in K\}$.

Proposition: $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

If H and K are finite subgroups of G, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

.....

Intuition. HK is a union of distinct left cosets of K, one for each coset of $H \cap K$ inside H.

.....

Proof. **Step 1.** $HK = \bigcup_{h \in H} hK$ is a union of left cosets of K.

Step 2. $h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_1(H \cap K) = h_2(H \cap K)$.

Step 3. Thus the number of distinct cosets hK (with $h \in H$) equals $|H : H \cap K| = \dfrac{|H|}{|H \cap K|}$.

Step 4. Each such coset has $|K|$ elements; multiply to obtain $|HK| = \dfrac{|H|}{|H \cap K|} \cdot |K|$. □

Proposition: $HK \leq G$ **iff** $HK = KH$**.**

For subgroups $H, K \leq G$, the set HK is a subgroup of G if and only if $HK = KH$.

Intuition. Closure under taking ab^{-1} for $a, b \in HK$ forces the ability to commute H past K at the coset level.

Proof. **Step 1 ($\Rightarrow$).** Assume $HK \leq G$. Since $H, K \leq HK$, we have $KH \subseteq HK$. For $hk \in HK$, write $hk = a^{-1}$ with $a = h_1k_1 \in HK$. Then $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, so $HK \subseteq KH$.

Step 2 ($\Leftarrow$). Assume $HK = KH$. For $a = h_1k_1$, $b = h_2k_2$, we have $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Using $KH = HK$, write $k_1k_2^{-1}h_2^{-1} = h'k'$ with $h' \in H$, $k' \in K$, hence $ab^{-1} = h_1h'k' \in HK$. Thus HK is a subgroup by the subgroup test. $\square$

Corollary: If $H \subseteq N_G(K)$ then $HK \leq G$. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for all $H \leq G$.

. . . . . .

Intuition. If H normalizes K, then $hK = Kh$ for all $h \in H$, giving $HK = KH$.

. . . . . .

Proof. **Step 1.** If $H \subseteq N_G(K)$, then for each $h \in H$ and $k \in K$, $hkh^{-1} \in K$, so $hK = Kh$.

Step 2. Hence $HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$. Apply the previous proposition to conclude $HK \leq G$.

Step 3. If $K \trianglelefteq G$, then every $g \in G$ normalizes K, so the hypothesis holds for any $H \leq G$. $\square$

Definition: Normalizes / Centralizes.

If $A \subseteq N_G(K)$ (resp. $A \subseteq C_G(K)$), we say that A *normalizes* (resp. *centralizes*) K.

Theorem: First Isomorphism Theorem.

Let $\varphi : G \to H$ be a group homomorphism. Then $\ker \varphi \trianglelefteq G$ and

$$G/\ker \varphi \;\cong\; \varphi(G).$$

Intuition. Collapse the kernel to a point; cosets become elements of the quotient. The map $g \mapsto \varphi(g)$ depends only on the coset $g \ker \varphi$, giving an isomorphism onto the image.

Proof. **Step 1.** $\ker \varphi \leq G$ and is normal since for $g \in G$, $k \in \ker \varphi$, $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = 1$, so $gkg^{-1} \in \ker \varphi$.

Step 2. Define $\psi : G/\ker \varphi \to \varphi(G)$ by $\psi(g \ker \varphi) = \varphi(g)$.

Step 3. Well-defined: if $g \ker \varphi = h \ker \varphi$, then $h^{-1}g \in \ker \varphi$, so $\varphi(g) = \varphi(h)$.

Step 4. Homomorphism: $\psi(g \ker \varphi \cdot h \ker \varphi) = \psi(gh \ker \varphi) = \varphi(gh) = \varphi(g)\varphi(h)$.

Step 5. Surjective by definition of $\varphi(G)$; injective since $\psi(g \ker \varphi) = 1$ iff $\varphi(g) = 1$ iff $g \in \ker \varphi$ iff $g \ker \varphi = \ker \varphi$.

Conclusion. ψ is an isomorphism $G/\ker \varphi \cong \varphi(G)$. □

Corollary: Kernel/Injectivity and Index–Image Size.

Let $\varphi : G \to H$ be a homomorphism.

1. φ is injective $\iff \ker \varphi = \{1\}$.
2. $|G : \ker \varphi| = |\varphi(G)|$ (cardinalities; in particular for finite G, $|G| = |\ker \varphi|\,|\varphi(G)|$).

Intuition. A trivial kernel means distinct cosets and elements are identified only when equal. The First Isomorphism Theorem gives a bijection between $G/\ker \varphi$ and $\varphi(G)$.

Proof. **Step 1.** (1) Injective $\iff \varphi(g) = 1$ only for $g = 1 \iff \ker \varphi = \{1\}$.

Step 2. (2) By First Isomorphism, $G/\ker \varphi \cong \varphi(G)$ as sets, hence equal cardinalities. For finite G, $|G : \ker \varphi| = \frac{|G|}{|\ker \varphi|}$. □

Theorem: Second (Diamond) Isomorphism Theorem.

Let G be a group, $A, B \leq G$, and assume $A \leq N_G(B)$. Then:

1. $AB \leq G$ and $B \trianglelefteq AB$.
2. $A \cap B \trianglelefteq A$.
3. $AB/B \;\cong\; A/(A \cap B)$.

.....

Intuition. If A normalizes B, the product AB is a subgroup with B normal inside. Mapping $a \mapsto aB$ identifies A modulo $A \cap B$ with AB modulo B.

.....

Proof. **Step 1.** Since $A \leq N_G(B)$, for all $a \in A$ we have $aBa^{-1} = B$. By the sufficient condition, $AB \leq G$ and $B \trianglelefteq AB$.

Step 2. $A \cap B \trianglelefteq A$ because A normalizes B.

Step 3. Define $\phi : A \to AB/B$ by $\phi(a) = aB$. This is a homomorphism with image AB/B (surjective) and kernel $\{a \in A : aB = B\} = A \cap B$.

Step 4. By the First Isomorphism Theorem, $A/(A \cap B) \cong AB/B$. □

Theorem: Third Isomorphism Theorem.

Let $H, K \trianglelefteq G$ with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \;\cong\; G/K.$$

.....

Intuition. Passing to the quotient by H sends K to K/H. Modding out by K/H in G/H is the same as modding out by K in G ("invert and cancel").

.....

Proof. **Step 1.** $K/H \leq G/H$ and is normal since for $g \in G$, $(gH)(K/H)(gH)^{-1} = gKg^{-1}/H = K/H$.

Step 2. Define $\pi : G/H \to G/K$ by $\pi(gH) = gK$.

Step 3. Well-defined: if $gH = hH$, then $h^{-1}g \in H \leq K$, so $gK = hK$.

Step 4. π is a surjective homomorphism with kernel K/H.

Step 5. Apply the First Isomorphism Theorem: $(G/H)/(K/H) \cong G/K$. □

Theorem: Fourth (Lattice) Isomorphism Theorem.

Let $N \trianglelefteq G$. The map

$$\Phi: \ \{A \leq G \mid N \leq A\} \ \longrightarrow \ \{\, \overline{A} \leq G/N \,\}, \qquad A \mapsto \overline{A} := A/N$$

is a bijection with inverse $B \mapsto \pi^{-1}(B)$, where $\pi : G \to G/N$ is the natural projection. Moreover, for A, B with $N \leq A, B \leq G$:

1. $A \leq B \iff \overline{A} \leq \overline{B}$.
2. If $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$ (indices).
3. $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$ (joins correspond).
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$ (meets correspond).
5. $\overline{A} \trianglelefteq G/N \iff A \trianglelefteq G$.

Intuition. Collapsing N identifies subgroups containing N with subgroups downstairs; lattice operations and indices are preserved under this correspondence.

Proof. **Step 1.** If $N \leq A \leq G$, then $A/N \leq G/N$. Conversely, for $B \leq G/N$, $\pi^{-1}(B)$ is a subgroup of G containing N.

Step 2. Show $\pi^{-1}(A/N) = A$ and $\overline{\pi^{-1}(B)} = B$; hence Φ is a bijection with stated inverse.

Step 3. (1) $A \leq B \Rightarrow A/N \leq B/N$; conversely, $A/N \leq B/N \Rightarrow A \leq B$ by applying π^{-1}.

Step 4. (2) Cosets correspond bijectively: $B/A \ \leftrightarrow \ (B/N)/(A/N)$, so indices agree.

Step 5. (3)–(4) Images of joins and meets follow from properties of π and preimages.

Step 6. (5) Normality corresponds since conjugation commutes with the projection: $(gN)(A/N)(gN)^{-1} = (gAg^{-1})/N$. □

Proposition: Induced Maps on Quotients (Factor Through).

Let $\psi : G \to H$ be a homomorphism and let $N \trianglelefteq G$. The assignment

$$\overline{\psi} : G/N \to H, \qquad \overline{\psi}(gN) = \psi(g)$$

is a well-defined homomorphism *iff* $N \subseteq \ker \psi$. In that case, $\psi = \overline{\psi} \circ \pi$ (i.e., ψ factors through N).

. . . . . .

Intuition. A function on G descends to G/N exactly when it is constant on cosets—equivalently, when it kills N.

. . . . . .

Proof. **Step 1 ($\Rightarrow$).** If $\overline{\psi}$ is well-defined with $\psi = \overline{\psi} \circ \pi$, then for $n \in N$, $\psi(n) = \overline{\psi}(nN) = \overline{\psi}(N) = 1$, so $N \leq \ker \psi$.

Step 2 ($\Leftarrow$). If $N \subseteq \ker \psi$ and $gN = hN$, then $h^{-1}g \in N \subseteq \ker \psi$, so $\psi(g) = \psi(h)$; hence $\overline{\psi}$ is well-defined and a homomorphism.

Step 3. By definition, $\psi(g) = \overline{\psi}(gN)$, so $\psi = \overline{\psi} \circ \pi$. □

Proposition: In a finite abelian group, primes divide orders of elements.

If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

. . . . . .

Intuition. Induct on $|G|$. Either some element already has order divisible by p (take a p-power to drop to order p) or else pass to the proper quotient by $\langle x \rangle$ and lift a p-torsion element back.

. . . . . .

Proof. **Step 1 (Induction basis).** If $|G| = p$, any $1 \neq x \in G$ has order p.

Step 2 (Inductive hypothesis). Assume the claim holds for all nontrivial abelian groups of order $< |G|$.

Step 3 (Case 1: some x has $p \mid |x|$). Write $|x| = p^a m$ with $(p, m) = 1$ and $a \geq 1$. Then x^m has order p^a; in particular, $(x^m)^{p^{a-1}}$ has order p.

Step 4 (Case 2: no element has $p \mid |x|$). Fix $1 \neq x \in G$. Since G is abelian, $N = \langle x \rangle \trianglelefteq G$. Lagrange gives $|G/N| = \frac{|G|}{|N|}$, and $p \mid |G/N|$ because $p \nmid |N|$ by assumption.

Step 5 (Apply induction to the quotient). By the inductive hypothesis, G/N has some $\overline{y}$ of order p. Pick $y \in G$ with $yN = \overline{y}$. Then $(yN)^p = N$, so $y^p \in N$ but $y \notin N$; hence the order of yN is p.

Step 6 (Conclude). The coset yN has order p in G/N, so $y^p \in N$ while $y^k \notin N$ for $1 \leq k < p$. Consider y^m where m is minimal with $y^m \in N$. Using abelianity and minimality, deduce $p \mid m$ and that $y^{m/p}$ has order p in G. (Equivalently, step 5 already yields an element of order p by standard cyclic-subgroup arguments.) $\square$

Definition: Simple group.

A group G is *simple* if $|G| > 1$ and its only normal subgroups are $\{1\}$ and G.

Definition: Composition series and composition factors.

A chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

is a *composition series* if each quotient N_{i+1}/N_i is simple. The groups N_{i+1}/N_i are the *composition factors* of G.

Theorem: Jordan–Hölder.

Let G be a finite nontrivial group.

1. (*Existence*) G has a composition series.
2. (*Uniqueness up to order/isomorphism*) If

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_r = G, \qquad 1 = M_0 \trianglelefteq \cdots \trianglelefteq M_s = G$$

are composition series, then $r = s$ and there is a permutation σ of $\{1, \ldots, r\}$ such that

$$N_i/N_{i-1} \;\cong\; M_{\sigma(i)}/M_{\sigma(i)-1} \quad \text{for all } i.$$

.....

Intuition. Existence: repeatedly peel off a minimal nontrivial normal subgroup to build a chain. Uniqueness: any two such chains refine to a common refinement whose factors pairwise match via the Second/Third Isomorphism Theorems (Schreier refinement + Zassenhaus lemma).

.....

Proof. **Step 1 (Existence by induction).** If G is simple, the series $1 \trianglelefteq G$ works. Otherwise choose a nontrivial proper normal subgroup $N \trianglelefteq G$. By induction, N and G/N have composition series. Splice them (lifting the series of G/N via preimages) to obtain a composition series of G.

Step 2 (Refinement lemma). Any subnormal series of G can be refined (by inserting intermediate normal subgroups) to a composition series. (Refine each non-simple factor iteratively.)

Step 3 (Schreier refinement). Any two subnormal series of G admit equivalent refinements: there are refinements whose multiset of factors are pairwise isomorphic up to order. (Construct the "matrix" of intersections $N_i M_j$ and apply the Second Isomorphism Theorem to get factor isomorphisms.)

Step 4 (Apply to composition series). If both series are already composition series, their refinements must be themselves (no further proper normal subgroups exist in factors). Hence their factor multisets coincide, which yields $r = s$ and the stated bijection of factors. □

Definition: The Hölder Program (classification viewpoint).

(1) Classify all finite simple groups.
(2) Describe how to assemble (extend) simple groups to obtain all finite groups (the extension problem).

Definition: Solvable group.

A group G is *solvable* if there exists a chain

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that each quotient G_{i+1}/G_i is abelian.

Proposition: If N and G/N are solvable, then G is solvable.

Let $N \trianglelefteq G$. If N and G/N are solvable, then G is solvable.

Intuition. Lift a solvable chain from G/N to G via preimages, and splice it above a solvable chain inside N. Abelian factors remain abelian by the Third/Lattice Isomorphism Theorems.

Proof. **Step 1 (Chains).** Take $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_r = N$ with abelian N_{i+1}/N_i. Take $1 = \overline{G}_0 \trianglelefteq \cdots \trianglelefteq \overline{G}_t = G/N$ with abelian $\overline{G}_{j+1}/\overline{G}_j$.

Step 2 (Lift the quotient chain). Put $G_j = \pi^{-1}(\overline{G}_j)$, where $\pi : G \to G/N$. Then $N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_t = G$, and by the Third Isomorphism Theorem each factor $G_{j+1}/G_j \cong \overline{G}_{j+1}/\overline{G}_j$ is abelian.

Step 3 (Splice chains). Concatenate

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_r = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_t = G.$$

All successive quotients are abelian, so this is a solvable series for G. □

Definition: Transposition.

A *transposition* in S_n is a 2-cycle $(i\ j)$ that swaps i and j and fixes all other elements.

Proposition: Decomposing permutations into transpositions.

1. Every $\sigma \in S_n$ is a product of transpositions.

2. An r-cycle $(a_1\ a_2\ \dots\ a_r)$ equals $(a_1\ a_r)\,(a_1\ a_{r-1})\cdots(a_1\ a_2)$, a product of $(r-1)$ transpositions.

.....

Intuition. Write a permutation as a product of disjoint cycles; each r-cycle can be "built" by successively moving a_1 into place using transpositions.

.....

Proof. **Step 1.** Any σ is a product of disjoint cycles. If each cycle can be written as a product of transpositions, so can σ.

Step 2. Check $(a_1\ a_2\ \dots\ a_r) = (a_1\ a_r)\,(a_1\ a_{r-1})\cdots(a_1\ a_2)$ by evaluating both sides on $a_1, \dots, a_r$ (and noting they fix all other points).

Step 3. Thus every cycle, and hence every permutation, is a product of transpositions. □

Definition: Parity and sign of a permutation.

If $\sigma \in S_n$ is written as a product of transpositions in k factors, the *parity* of σ is the parity of k (even or odd). The *sign* of σ is

$$\operatorname{sgn}(\sigma) = (-1)^k.$$

Theorem: Parity is well-defined.

If $\sigma \in S_n$ is expressed as a product of transpositions in k ways with lengths k_1 and k_2, then $k_1 \equiv k_2 \pmod 2$. Equivalently, $\operatorname{sgn} : S_n \to \{\pm 1\}$ is well-defined.

Intuition. Each r-cycle uses exactly $(r-1)$ transpositions; disjoint cycles multiply lengths additively. Since changing a decomposition by inserting or removing a neutral pair $(i\,j)(i\,j)$ alters the count by 2, only the parity is invariant.

Proof. **Step 1.** From the cycle decomposition, $\sigma = \gamma_1 \cdots \gamma_t$ (disjoint), with γ_i of length r_i. By the previous proposition, γ_i is a product of $(r_i - 1)$ transpositions.

Step 2. Thus any such canonical construction yields a decomposition of σ into $\sum_i (r_i - 1)$ transpositions, whose parity is fixed.

Step 3. Any other decomposition differs by inserting/removing pairs $(\tau)(\tau)$ and by commutations of disjoint transpositions; these change the length by multiples of 2.

Step 4. Hence the parity is independent of the chosen decomposition, and $\operatorname{sgn}(\sigma)$ is well-defined. □

Proposition: $\mathrm{sgn} : S_n \to \{\pm 1\}$ **is a homomorphism;** $\ker(\mathrm{sgn}) = A_n$**.**

For $\sigma, \tau \in S_n$, $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. The kernel consists of the even permutations, i.e., the alternating group A_n.

. . . . . .

Intuition. Composition concatenates transposition factorizations; lengths add, so signs multiply. Even permutations are precisely those with sign $+1$.

. . . . . .

Proof. **Step 1.** Write σ and τ as products of k_σ and k_τ transpositions; then $\sigma\tau$ is a product of $k_\sigma + k_\tau$ transpositions, so $\operatorname{sgn}(\sigma\tau) = (-1)^{k_\sigma + k_\tau} = (-1)^{k_\sigma}(-1)^{k_\tau}$.

Step 2. The kernel is $\{\pi \in S_n \mid \operatorname{sgn}(\pi) = 1\}$, the set of even permutations, by definition. This is A_n. $\square$

Definition: Alternating group A_n.

The *alternating group* A_n is the subgroup of S_n consisting of all even permutations:

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = +1\}.$$

Proposition: $A_n \trianglelefteq S_n$ **and** $|A_n| = \dfrac{n!}{2}$ **for** $n \geq 2$**.**

A_n is a normal subgroup of S_n with index 2, hence $|A_n| = n!/2$.

. . . . . .

Intuition. sgn is a surjective homomorphism onto $\{\pm 1\}$; its kernel has index 2. Kernels are normal, and index-2 subgroups are always normal.

. . . . . .

Proof. **Step 1.** By the homomorphism property, $\text{sgn} : S_n \to \{\pm 1\}$ is surjective. Then $\ker(\text{sgn}) = A_n$.

Step 2. Kernels are normal, so $A_n \trianglelefteq S_n$.

Step 3. The image has size 2, thus $|S_n : A_n| = 2$, and for $n \geq 2$, $|A_n| = |S_n|/2 = n!/2$. □

Proposition: A_n **is generated by 3-cycles (for** $n \geq 3$**).**

Every even permutation in S_n is a product of 3-cycles. Hence $A_n = \langle \text{3-cycles} \rangle$.

. . . . . .

Intuition. A product of two transpositions is even; when the transpositions share a point, it is itself a 3-cycle; when disjoint, it is a product of two 3-cycles.

. . . . . .

Proof. **Step 1.** Any even permutation is a product of an even number of transpositions, so it suffices to write a product of two transpositions as a product of 3-cycles.

Step 2. If $(a\ b)(a\ c) = (a\ c\ b)$, which is a 3-cycle.

Step 3. If $(a\ b)$ and $(c\ d)$ are disjoint, then

$$(a\ b)(c\ d) = (a\ c\ b)(a\ d\ b),$$

a product of two 3-cycles (verify by action on a, b, c, d).

Step 4. Therefore any even permutation is a product of 3-cycles, and these generate A_n. $\square$

Proposition: Sign of an r-cycle.

If γ is a cycle of length r, then $\operatorname{sgn}(\gamma) = (-1)^{r-1}$.

. . . . . .

Intuition. Use the standard decomposition of an r-cycle into $(r-1)$ transpositions.

. . . . . .

Proof. **Step 1.** From the earlier decomposition, $\gamma = (a_1\ a_r)\cdots(a_1\ a_2)$ uses $(r-1)$ transpositions.
Step 2. Hence $\operatorname{sgn}(\gamma) = (-1)^{r-1}$ by definition of sign. □

Corollary: Exactly half of S_n is even, half is odd (for $n \geq 2$).

For $n \geq 2$, $|A_n| = |S_n \setminus A_n| = n!/2$.

. . . . . .

Intuition. Index-2 kernel of the sign map splits S_n into two equal-sized cosets: A_n and any odd coset.

. . . . . .

Proof. **Step 1.** Since sgn is surjective, $S_n/A_n \cong \{\pm 1\}$.

Step 2. Thus $|S_n : A_n| = 2$ and $|A_n| = n!/2$. The complement is the other coset, also of size $n!/2$. □

Ch 3: Priority Problems

Overview. These are designed to test your memory on a few selected problems on the basics of quotient groups and homomorphisms as presented in Ch3 of Dummit and Foote.

List.

1. 1.1: 1, 2, 7, 18, 34
2. 1.2: 4
3. 1.3: 2, 3
4. External Problems: 1, 2, 3, 4
5. 1.6: 1, 2, 3, 4, 7, 18, 20
6. 1.7: 15