Algebra I

September 10th, 2026

[0.0.1] Definition (*Permutation, Identity Permutation, Permutation Matrix*)

For any set S, we define a **permutation** p of S as a bijection $p : S \to S$. If p leaves all points in S fixed, we say p is the **identity permutation**. If $|S| < \infty$, we can define a **permutation matrix** P such that $Pe_k = e_{p(k)}$ for each standard basis vector e_k for $\mathbb{R}^{|S|}$.

[0.0.2] Example

Let $S = \{1, \ldots, 5\}$. Define the permutation $p : S \to S$ by the following table.

i	1	2	3	4	5
p(i)	3	5	4	1	2

It is common to represent permutations with *cycle notation*. To write a permutation p in cycle notation, we simply choose one index $i \in S$ and chase it with p until all elements in S are achieved, or until we hit a loop. For example, let $i = 3$. Then note $3 \to 4 \to 1$, where the arrow denotes applying p, and this completes one cycle. Since we did not complete cycling through S, we choose any other element from S. Choose $2 \in S$, then note $2 \to 5$. Thus our permutation's action is simply denoted by the sequence

$$3 \to 4 \to 1 \quad 2 \to 5,$$

where the arrow denotes applying p. In terser notation, we say $p = (3\ 4\ 1)(2\ 5)$.

An n-cycle is a cycle with n indices. A 2-cycle is said to be a *transposition*, since the permutation simply acts by swapping the two indices. For example, $(2\ 5)$ is a transposition, since 2 is swapped with 5 and vice versa under p. A 1-cycle is a fixed point under p, and we tend to omit it. If all elements of S are fixed points under p, then p is simply the identity permutation, denoted $p = 1$.

[0.0.3] Definition (*Sign and Parity of Finitary Permutation*)

Suppose $p : S \to S$ is a permutation over a finite set S. Then we define the **sign** of the permutation p, denoted $\operatorname{sgn}(p)$, by the determinant of the permutation matrix P induced by p. Immediately we have that $\operatorname{sgn}(p) \in \{1, -1\}$—we say that p is **even** if $\operatorname{sgn}(p) = 1$, otherwise p is **odd** ($\operatorname{sgn}(p) = -1$).

[0.0.4] Remark (*Equivalent Characterizations of Sign of Finitary Permutation*)

There are two equivalent ways to view the sign of a permutation. From the linear-algebraic perspective, $\operatorname{sgn}(p)$ is simply the determinant of the permutation matrix induced by p. From the group-theoretic perspective, every cycle

$$p = (a_1\ \ldots\ a_k)$$

may be decomposed into transpositions as

$$p = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2).$$

Thus a k-cycle is a product of $k - 1$ transpositions. More generally, every permutation of a finite set can be written as a product of transpositions, say

$$p = \tau_1 \tau_2 \cdots \tau_m,$$

and we may equivalently define

$$\operatorname{sgn}(p) = (-1)^m.$$

Although such a decomposition is not unique, the parity of m is strictly independent of the chosen decomposition.

[0.0.5] Definition (*Group, Abelian Group*)

A **group** is a set G together with a map $G \times G \to G$, called the **group operation**, satisfying the following requirements.

(1) **Associativity.** For any $a, b, c \in G$, applying the group operation to (ab, c) yields the same element in G as applying it to (a, bc).

(2) **Identity.** There is some element $1 \in G$ such that, for any $g \in G$, we have that $(g, 1) \mapsto g$ and $(1, g) \mapsto g$.

(3) **Inverse.** For every $g \in G$, there is some element $g^{-1} \in G$ such that $(g, g^{-1}) \mapsto 1$ and $(g^{-1}, g) \mapsto 1$.

If, for any $a, b \in G$, we have that (a, b) and (b, a) have the same image under the group operation, the group operation is commutative. A group together with a commutative operation is said to be an **abelian** group.

[0.0.6] Example (*Examples of Groups, Symmetric and General Linear Group*)

The group of integers together with the addition operation forms an abelian group. Note that $\mathbb{Z}$ together with multiplication is *not* a group (elements like 2 have no multiplicative inverse in $\mathbb{Z}$), but the set of non-zero rationals $\mathbb{Q} \setminus \{0\}$ together with multiplication is.

Fix $n \in \mathbb{Z}_+$. The **symmetric group** of order n, denoted S_n, is the group of all permutations on the set $\{1, \ldots, n\}$, where the group operation is function composition. The **general linear group** of order n, denoted $GL_n(\mathbb{F})$, is the group of all $n \times n$ invertible matrices over a field $\mathbb{F}$, where the group operation is matrix multiplication.

From now on, we will explicitly denote additive and multiplicative groups on a set S by S^+ and $S^\times$ to avoid ambiguity. Note that we use $\mathbb{Z}_+$ to denote the set of positive integers, while we use $\mathbb{Z}^+$ to denote the additive group of integers.

Let X be any finite set of size n. Consider the group formed by taking all permutations of X, together with the function composition operation. This group is *very* similar to S_n in terms of action. If we were to index each element of X by a positive integer, then simply call each element by its index, there would be virtually no structural difference between this relabeled version of X and S_n as sets that "respect" the group operation. We say that this group is **isomorphic** to S_n, a concept we will expand upon later. Indeed, the group of permutations on any finite set X is perfectly isomorphic to $S_{|X|}$.

Note that if X is not finite, then the set of permutations on X is not isomorphic to any finite symmetric group. We denote the group of all permutations on X by $\mathrm{Sym}(X)$, where the group operation is function composition. This group behaves quite differently from finite symmetric groups.

[0.0.7] Remark (*Conventions for Group Operation, Implicit Assumptions in Group Axioms*)

A group is typically said to be either "multiplicative" or "additive", and the operation is said to be multiplication or addition respectively. Multiplication is denoted by juxtaposition, whereas addition is denoted by $+$. Unless otherwise stated, we take a group to be multiplicative and its operation to be denoted by juxtaposition.

Fix a group G. By definition, note that for any $a, b \in G$, we have that $ab \in G$ (again, recall ab is simply the group operation applied to a and b). When a structure is such that an operation on it keeps elements in the set, we say that it is **closed**. Accordingly, G is inherently closed with respect to its group operation.

It is taken for granted that the identity and inverse elements are unique, as these fall out immediately from the axioms.

Note that, by induction, we may apply the group operation to n many elements of a group (written either $a_1 \cdots a_n$ or $a_1 + \cdots + a_n$). The empty product is simply the identity 1, vacuously. In the special case that each a_k is the same element a, we compactly write $a^n = a \cdot a \cdots a$ (or $na = a + a + \cdots + a$).

[0.0.8] Definition (*Group Order, Finite Group*)

The **order** of a group G is its cardinality as a set, denoted $|G|$. A group is said to be a **finite group** if its order is finite. For example, the symmetric group S_n has order $|S_n| = n!$.

[0.0.9] Definition (*Alphabet, Words, and the Free Group*)

Let S be a set, which we call an **alphabet** whose elements are **letters**. We formally construct a set of inverses $S^{-1} = \{s^{-1} : s \in S\}$. A **word** is a finite sequence of characters from $S \cup S^{-1}$. A word is **reduced** if it contains no adjacent inverse pairs ss^{-1} or $s^{-1}s$.

The **free group** generated by S, denoted $F(S)$, is the set of all reduced words. The group operation is string concatenation followed by reduction, and the identity is the empty word.

[0.0.10] Theorem (*Universal Property of the Free Group*)

Let S be an alphabet, G be an arbitrary group, and $f : S \to G$ be a map of sets assigning each letter to an element in G. There exists a unique group homomorphism $\varphi : F(S) \to G$ extending f, mapping each reduced word to the corresponding product in G.

[0.0.11] Definition (*Group Presentation*)

Let S be an alphabet and $R \subseteq F(S)$ be a set of words, called **relations** or constraints. To form a group where every word in R collapses to the identity, we must mod out by R. Because we can only quotient by normal subgroups, we define $N(R)$ as the **normal closure** of R in $F(S)$—the intersection of all normal subgroups containing R, which precisely consists of all finite products of conjugates of words in R.

The **group presentation** $\langle S \mid R \rangle$ is defined as the quotient group

$$\langle S \mid R \rangle = F(S)/N(R).$$

[0.0.12] Example (*The Symmetric Group S_3 and its Presentation*)

Consider S_3, which consists of all permutations on $\{1,2,3\}$. Let $x = (1\,2\,3)$ and $y = (1\,2)$. Computing their compositions, we note $x^3 = 1$, $y^2 = 1$, and $yx = (2\,3) = x^2y$.

This last constraint, $yx = x^2y$, forces the word $yxy^{-1}x^{-2}$ to equal the identity. We claim that S_3 is precisely the free group on $\{x, y\}$ modded out by the normal closure of these constraint words.

[0.0.13] Theorem (*Isomorphism of S_3 and its Presentation*)

$S_3 \cong \langle x, y \mid x^3 = 1, y^2 = 1, yx = x^2y \rangle$.

Proof. Let $G = \langle x, y \mid x^3 = 1, y^2 = 1, yx = x^2y \rangle$. Since G is generated by x and y, every element is a finite word in $\{x, y, x^{-1}, y^{-1}\}$. From the relations $x^3 = 1$ and $y^2 = 1$, we have $x^{-1} = x^2$ and $y^{-1} = y$, meaning every element can be written using only positive powers of x and y.

The relation $yx = x^2y$ allows us to shift any y appearing to the left of an x over to the right. By applying this relation repeatedly, every word in G can be reduced to the canonical form x^iy^j. Using the order relations, we may restrict the exponents to $i \in \{0,1,2\}$ and $j \in \{0,1\}$. Thus, G contains at most $3 \times 2 = 6$ elements, meaning $|G| \leq 6$.

Now consider S_3. Let $a = (1\,2\,3)$ and $b = (1\,2)$. We compute $a^3 = 1$, $b^2 = 1$, and $ba = (2\,3) = a^2b$. Since a and b satisfy the defining relations of G, there exists a group homomorphism $\varphi : G \to S_3$ mapping $x \mapsto a$ and $y \mapsto b$.

Since a and b generate S_3, the homomorphism φ is surjective. Because $|G| \leq 6$ and $|S_3| = 6$, a surjective map from G to S_3 must be a bijection. Thus φ is an isomorphism, and $G \cong S_3$.

[0.0.14] Definition (*Subgroup*)

Suppose G is a group. A subset $H \subseteq G$ is said to be a **subgroup** if the following properties are satisfied.

(1) **Closure.** For any $a, b \in H$, we have that $ab \in H$.

(2) **Identity.** We have that the identity 1 from G is contained in H.

(3) **Inverse.** Each element in H has an inverse contained in H.

Equivalently, H is a subgroup of G if H is a group with respect to the group operation inherited from G.

[0.0.15] Theorem (*Classification of Subgroups of $\mathbb{Z}^+$*)

All subgroups of $\mathbb{Z}^+$ take the form of either the trivial group $\{0\}$ or the set $a\mathbb{Z} = \{an : n \in \mathbb{Z}\}$, for some $a \in \mathbb{Z}_+$.

Proof. Suppose S is a nontrivial subgroup of $\mathbb{Z}^+$. Without loss of generality, choose a to be the smallest positive integer in S (since $-a \in S$, we can always choose a positive one). Then the group generated by a takes the form

$$\{\cdots, -2a, -a, 0, a, 2a, \cdots\},$$

which is precisely $a\mathbb{Z}$. Immediately, we have that $a\mathbb{Z} \subseteq S$. We prove that $S \subseteq a\mathbb{Z}$ to complete the proof. Indeed, let $s \in S$. Performing long division, we have that $s = qa + r$, with $0 \leq r < a$. Note that $r = s - qa \in S$, but since a is the smallest positive integer in S and $0 \leq r < a$, we are forced to take $r = 0$. Thus $s = qa$, meaning $S \subseteq a\mathbb{Z}$, completing the proof.

[0.0.16] Remark (*Intuition behind GCD and LCM*)

Fix $a, b \in \mathbb{Z}_+$. Note that $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b \mid a$ (i.e., b divides a). The logic is straightforward: a larger subgroup requires a smaller generator (step size). We will consider two natural set operations on $a\mathbb{Z}$ and $b\mathbb{Z}$, namely intersection and addition, to motivate their arithmetic counterparts.

First, consider $a\mathbb{Z} \cap b\mathbb{Z}$. Note that $x \in a\mathbb{Z} \cap b\mathbb{Z}$ if and only if x is a multiple of both a and b. It's quick to show $a\mathbb{Z} \cap b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$, and so

$$a\mathbb{Z} \cap b\mathbb{Z} = d\mathbb{Z}$$

for some unique positive integer d. Because d generates the set of all common multiples, it must be the smallest positive number in the intersection, which is precisely the least common multiple of a, b. Thus $d = \text{lcm}(a, b)$.

Now consider the sum

$$a\mathbb{Z} + b\mathbb{Z} = \{ra + sb : r, s \in \mathbb{Z}\},$$

which is the smallest subgroup of $\mathbb{Z}^+$ containing both $a\mathbb{Z}$ and $b\mathbb{Z}$. Note this sum must also equal $c\mathbb{Z}$ for a unique positive integer c. The inclusions $a\mathbb{Z} \subseteq c\mathbb{Z}$ and $b\mathbb{Z} \subseteq c\mathbb{Z}$ force $c \mid a$ and $c \mid b$, making c a common divisor; because $c\mathbb{Z}$ is the minimal subgroup containing both, its generator c must have the largest possible step size, identifying c uniquely as $\gcd(a, b)$. As an immediate corollary, since $c \in c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, there exist integers $r, s \in \mathbb{Z}$ such that $ra + sb = \gcd(a, b)$, a result famously known as Bézout's Lemma.

September 15th, 2026

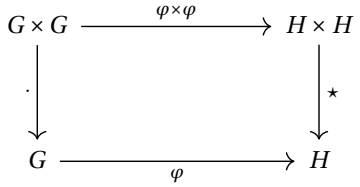
[0.0.17] Definition (*Homomorphism*)

Let G and H be groups with operations $\cdot$ and $*$ respectively. Then a map of sets $\varphi : G \to H$ is said to be a **homomorphism** if

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b)$$

for every $a, b \in G$.

A homomorphism is simply a map between groups that respects the multiplicative structure of the group, in the sense that the following diagram commutes.



This is a *commutative diagram*, in the sense that tracing any path between two objects in the diagram yields the exact same result, no matter which path is taken. This diagram dictates that applying the group operation and then the homomorphism is identical to applying the homomorphism and then the group operation. A map of sets generally does not do this (it may be dependent on the group operation and disrupt the structure). Due to this, we really only consider homomorphisms as the valid morphisms between groups to ensure the group operation is preserved.

[0.0.18] Example (*Examples of Homomorphisms*)

$$\begin{aligned} |\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times \quad & |a \times b| = |a| \times |b|. \\ \det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times \quad & \det(AB) = \det(A)\det(B). \\ \exp : \mathbb{R}^\times \to \mathbb{R}^+ \quad & \exp(ab) = \exp(a)\exp(b). \\ \ln : \mathbb{R}^+ \to \mathbb{R}^\times \quad & \ln(a) + \ln(b) = \ln(ab). \end{aligned}$$

[0.0.19] Theorem (*Homomorphisms Preserve Identity and Inverse Element*)

Let G and H be any groups with a homomorphism $\varphi : G \to H$. Then $\varphi(\mathrm{id}_G) = \mathrm{id}_H$. Moreover, for any $g \in G$, note that $\varphi(g^{-1}) = [\varphi(g)]^{-1}$.

Proof. First, we show $\varphi(\mathrm{id}_G) = \mathrm{id}_H$. Let $g \in G$ be any element. Then note $\mathrm{id}_G g = g$, and so

$$\varphi(g) = \varphi(\mathrm{id}_G g) = \varphi(\mathrm{id}_G)\varphi(g).$$

Multiplying both sides on the right by $[\varphi(g)]^{-1}$ yields

$$\varphi(g)[\varphi(g)]^{-1} = \varphi(\mathrm{id}_G)\varphi(g)[\varphi(g)]^{-1} \implies \mathrm{id}_H = \varphi(\mathrm{id}_G)\mathrm{id}_H \implies \mathrm{id}_H = \varphi(\mathrm{id}_G)$$

as desired. Next, we show $\varphi(g^{-1}) = [\varphi(g)]^{-1}$ in general. Fix $g \in G$, and note

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(\mathrm{id}_G) = \mathrm{id}_H.$$

Thus $\varphi(g^{-1})$ is indeed the inverse of $\varphi(g)$, and so $\varphi(g^{-1}) = [\varphi(g)]^{-1}$, completing the proof.

This is a useful example of why homomorphisms are needed. Since the group operation and the homomorphism can freely commute, we are able to easily deduce highly desirable conditions on how the map acts (as demonstrated by the previous theorem). This is the exact sense in which a homomorphism preserves the "structure" of a group.

[0.0.20] Definition (*Image and Kernel of Homomorphism*)

Let $\varphi : G \to H$ be a homomorphism. Define the **kernel** and **image** of φ by

$$\ker(\varphi) = \{g \in G : \varphi(g) = \mathrm{id}_H\},$$

$$\mathrm{im}(\varphi) = \varphi(G).$$

That is, $\ker(\varphi)$ is the set of all elements in G whose image under φ is id_H, and $\mathrm{im}(\varphi)$ is the set of all elements in H that are reached by φ.

[0.0.21] Theorem (*Kernel and Image of Homomorphisms are Subgroups*)

Let $\varphi : G \to H$ be a homomorphism. Then $\ker(\varphi)$ is a subgroup of G and $\mathrm{im}(\varphi)$ is a subgroup of H.

Proof. We show that both subsets are closed, contain the identity, and possess inverses for all elements.

(1) **Closure.** If $a, b \in \ker(\varphi)$, then $\varphi(a) = \varphi(b) = \mathrm{id}_H$. Then $\varphi(ab) = \varphi(a)\varphi(b) = (\mathrm{id}_H)^2 = \mathrm{id}_H$. If $a, b \in \mathrm{im}(\varphi)$, then there exist $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Thus $\varphi(xy) = \varphi(x)\varphi(y) = ab \in \mathrm{im}(\varphi)$ as desired.

(2) **Identity.** By the previous theorem, $\varphi(\mathrm{id}_G) = \mathrm{id}_H$. This immediately implies $\mathrm{id}_G \in \ker(\varphi)$, and since $\mathrm{id}_G \in G$, it also implies $\mathrm{id}_H \in \mathrm{im}(\varphi)$.

(3) **Inverse.** Fix any $k \in \ker(\varphi)$. Then note $\varphi(k) = \mathrm{id}_H$. Thus note $\varphi(k^{-1}) = [\varphi(k)]^{-1} = [\mathrm{id}_H]^{-1} = \mathrm{id}_H$, meaning $k^{-1} \in \ker(\varphi)$. Fix $y \in \mathrm{im}(\varphi)$. Then $\varphi(x) = y$ for some $x \in G$, and so $\varphi(x^{-1}) = [\varphi(x)]^{-1} = y^{-1}$, meaning $y^{-1} \in \mathrm{im}(\varphi)$.

[0.0.22] Definition (*Isomorphism, Automorphism, Endomorphism*)

Let G and H be any two groups. A homomorphism $\varphi : G \to H$ is said to be an **isomorphism** if there is some homomorphism $\varphi^{-1} : H \to G$ such that $\varphi \circ \varphi^{-1} = \mathrm{id}_H$ and $\varphi^{-1} \circ \varphi = \mathrm{id}_G$. An **endomorphism** is any homomorphism from G to G. An **automorphism** is an isomorphic endomorphism.

If $\varphi : G \to H$ is an isomorphism, then it is bijective. Treating φ as a map of sets, we can consider the inverse $\varphi^{-1} : H \to G$ as a pure set function. This is automatically a homomorphism (and thus an isomorphism), with a proof so trivial even the dog won't write it.

φ^{-1} inherits all the natural properties of inverses as per usual (consider uniqueness and being invertible itself).

[0.0.23] Example (*Example of Automorphism*)

Let G be a group with any fixed $g \in G$. Then we may define a **conjugation map** $\Phi_g : G \to G$ by

$$\Phi_g(a) = gag^{-1}.$$

It is trivial to show $\Phi_g^{-1}(a) = g^{-1}ag$, and so Φ_g is an automorphism. Note that conjugation automorphisms are occasionally called **inner automorphisms**. Outer automorphisms are elements of $\mathrm{Aut}(G)/\mathrm{Inn}(G)$, where $\mathrm{Aut}(G)$ is the group of all automorphisms on G and $\mathrm{Inn}(G)$ is the normal subgroup of inner/conjugation automorphisms on G.

[0.0.24] Definition (*Cyclic Group*)

Recall that a group can be generated from a generating set by taking the finite words from the set and its formal inverses. We say that a group is **cyclic** if it is generated by a single element x. In other words, a group G is cyclic if it takes the form

$$G = \langle x \rangle = \{\cdots, x^{-2}, x^{-1}, \mathrm{id}_G, x^1, x^2, \cdots\}.$$

[0.0.25] Definition (*Order of an Element of Group*)

Suppose G is a group and $g \in G$. The **order** of g, denoted $\mathrm{ord}(g)$ or $|g|$, is defined to be the number $n \in \mathbb{Z}_+$ such that $g^n = \mathrm{id}_G$. If no such number exists, we say $\mathrm{ord}(g) = \infty$.

Immediately, note that the order of a group element g is precisely the order of the generated group $\langle g \rangle$.

Fix a group G together with some $x \in G$. Consider the evaluation map

$$\varphi : \mathbb{Z}^+ \to G \quad \varphi(k) = x^k.$$

Note that $\mathrm{im}(\varphi) = \{\cdots, x^{-2}, x^{-1}, \mathrm{id}_G, x^1, x^2, \cdots\} = \langle x \rangle$. Because φ is a homomorphism from the integers to the generated group, we can elegantly use the kernel of this map to characterize finite and infinite cyclic groups.

[0.0.26] Remark (*Kernel of Map Determines Finiteness of Cyclic Subgroup*)

Fix a group G together with some $x \in G$, where $\varphi(k) = x^k$ as per before. Suppose $x^r = x^s$ for some $r, s \in \mathbb{Z}$. Rearranging yields $x^{r-s} = \mathrm{id}_G$. Thus $r - s \in \ker(\varphi)$.

Suppose $\ker(\varphi) = \{0\}$. Then $x^k = \mathrm{id}_G$ if and only if $k = 0$, meaning $x^r \neq x^s$ for all $r \neq s$. Thus $\langle x \rangle$ is an *infinite* cyclic group.

Conversely, recall that $\ker(\varphi)$ is a subgroup of the domain (which is $\mathbb{Z}^+$). If it is nontrivial, the subgroup classification theorem tells us it must take the form $\ker(\varphi) = n\mathbb{Z}$. Then $x^n = 1$ is the smallest positive n to satisfy this, meaning

$$\langle x \rangle = \{\mathrm{id}_G, x^1, x^2, \ldots, x^{n-1}\}$$

is a *finite* cyclic group of order n (since $x^n = 1, x^{n+1} = x^n x^1 = x^1, \ldots$ causes the group to wrap around).

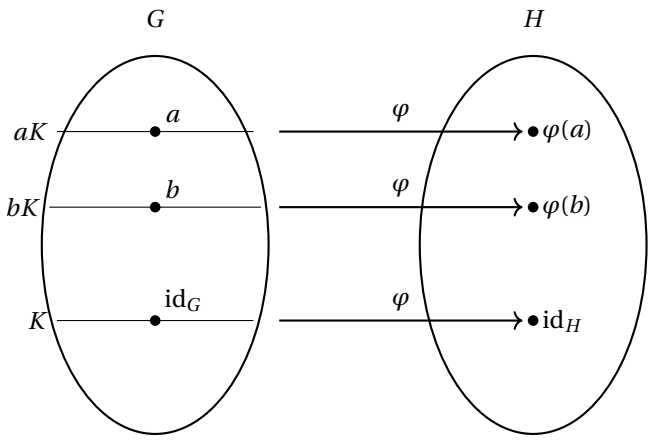
Note that each finite cyclic group of order n is inherently isomorphic to $\mathbb{Z}/n\mathbb{Z}$. We can use the aforementioned evaluation map to build the isomorphism, simply taking the domain to be $(\mathbb{Z}/n\mathbb{Z})$ and the codomain to be $\langle x \rangle$.

[0.0.27] Remark (*Fibers of a Homomorphism and Cosets of the Kernel*)

Let $\varphi : G \to H$ be any homomorphism, and let $K = \ker(\varphi)$. The map φ partitions G into *fibers*, which are the sets of elements in G that map to the same target element in H. Fix some $a \in G$. We seek to characterize the fiber containing a, namely all $b \in G$ such that $\varphi(a) = \varphi(b)$. Indeed, suppose $b \in G$ is any such element. Rewriting yields

$$\varphi(b) = \varphi(a) \implies [\varphi(a)]^{-1}\varphi(b) = \mathrm{id}_H \implies \varphi(a^{-1}b) = \mathrm{id}_H.$$

Thus $a^{-1}b \in \ker(\varphi)$, meaning there is some $k \in K$ such that $a^{-1}b = k$, or $b = ak$. By the rigid conditions homomorphisms impose on the algebraic structure, two elements in G have the same image under φ if and only if one can be written as the other multiplied by an element of the kernel. This means the fiber over $\varphi(a)$ is precisely the set of all elements of the form ak for $k \in K$.



Note that the cosets of $\ker(\varphi)$ is in bijection with $\mathrm{im}(\varphi)$. This idea culminates into an extremely powerful structure theorem for homomorphisms of groups, which we will discuss later.

This geometric picture—where the subgroup K acts as a slice that can be translated across G by multiplying by different elements—motivates a more general group-theoretic construction. We can shift *any* subgroup, not just kernels, in this exact manner.

[0.0.28] Definition (*Left and Right Cosets*)

Let H be an arbitrary subgroup of a group G, and fix $a \in G$. We define the **left coset** of H with respect to a as the set

$$aH = \{ah : h \in H\}.$$

Similarly, we define the **right coset** of H with respect to a as the set

$$Ha = \{ha : h \in H\}.$$

[0.0.29] Remark (*Cosets as Equivalence Classes and Partitions*)

Let $H \subseteq G$ be a subgroup. To show that these general cosets neatly partition G exactly as the fibers of a homomorphism do, we define a relation $\sim$ on G by declaring $a \sim b$ if and only if $a = bh$ for some $h \in H$.

This forms an equivalence relation. It is reflexive (since $a = a\mathrm{id}_G$ and $\mathrm{id}_G \in H$), symmetric (since $a = bh \implies b = ah^{-1}$, and H is closed under inversion so $h^{-1} \in H$), and transitive (since $a = bh_1$ and $b = ch_2$ implies $a = c(h_2h_1)$, and H is closed under multiplication so $h_2h_1 \in H$).

Under this relation, the equivalence class of an element $b \in G$ is exactly the set of all elements of the form bh for $h \in H$. This is precisely the left coset bH. Because equivalence classes strictly partition a set, this cleanly demonstrates that the left cosets of H completely partition the group G into a family of disjoint subsets.

As a brief aside, while left and right cosets both independently partition the group, they do not necessarily coincide with one another (i.e., aH need not equal Ha). This relies on a special condition.

September 17th, 2026

Recall that, for a subgroup $H \subseteq G$, the left cosets $\{aH : a \in G\}$ of H form a partition G, since it is the set of equivalence classes from the equivalence relation $x \sim y$ if and only if $x, y \in G$ belong to the same left coset.

[0.0.30] Theorem (*Cosets are the Same Order as Subgroup*)

Suppose H is some subgroup of G. Then $|aH| = |Ha| = |H|$ for every $a \in G$.

Proof. Fix some $a \in G$. Then consider the map $f : aH \to H$ given by $f(x) = a^{-1}x$. For each $h \in H$, note that $f(ah) = a^{-1}(ah) = h$, and so f is surjective. Moreover, if $h_1, h_2 \in aH$ are such that $f(h_1) = f(h_2)$, then note

$$a^{-1}h_1 = a^{-1}h_2 \implies h_1 = h_2,$$

and so f is injective. Thus f is bijective, and so $|aH| = |H|$ as desired.

An analogous procedure can be performed to show $g : Ha \to H$ given by $g(x) = xa^{-1}$ is also a bijection.

From now on, note that using the number of left cosets is interchangeable with using the number of right cosets.

[0.0.31] Definition (*Index of a Subgroup*)

Let H be a subgroup of G. Then the **index** of H, denoted $[G : H]$, is the number of left cosets H has.

Recall that the left cosets of a subgroup H partition the group G, and that the left cosets of H all have the same order, which is $|H|$. This lets us relate the order of G with the cosets of H.

[0.0.32] Proposition (*Counting Formula*)

Let H be a subgroup of G. Then $|G| = [G : H] \times |H|$.

This theorem reads that the order of a group G is the number of cosets a subgroup has, multiplied by the size of each coset, which is obviously true. Since $[G : H]$ is an integer, we note that $|H|$ is an integer multiple of $|G|$

[0.0.33] Theorem (*Lagrange's Theorem*)

Let G be a group. Then, for any subgroup $H \subseteq G$, we have that $|H|$ divides $|G|$.

Lagrange's theorem gives rise to multiple important structure theorems about groups.

[0.0.34] Theorem (*Element Order Divides Group Order*)

Let G be a group. For every $g \in G$, note $|g|$ divides $|G|$.

Proof. Note $\langle g \rangle$ is a subgroup of G of order g. The result follows by Lagrange.

[0.0.35] Theorem (*Groups of Prime Order are Cyclic*)

Suppose G is a group such that $|G| = p$ for some prime p. Then $G \cong C_p$ for all cyclic groups of order p.

Proof. G is not of order 1, since 1 is not prime. Thus there must be some $g \in G$ such that $g \neq \mathrm{id}_G$. Notably, since $|g|$ divides $|G| = p$, we either have that $|g| = 1$ or $|g| = p$. Note that $|g| \neq 1$ since $g \neq \mathrm{id}_G$, and so $|g| = p$. Thus $\langle g \rangle$ is a subgroup of G with the same order as G, and so $\langle g \rangle = G$, completing the proof.

Note that all cyclic groups of order n are isomorphic to one another. Indeed, for any cyclic group $G = \langle g \rangle$ of order n, the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi(k) = g^k$ forms an explicit isomorphism. Since every cyclic group of order n is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, they are all isomorphic to one another by transitivity.

[0.0.36] Theorem (*Counting Formula for Homomorphisms*)

Let $\varphi : G \to H$ be a homomorphism of finite groups. Then $|G| = |\ker\varphi| \times |\operatorname{im}\varphi|$.

Proof. Recall from earlier that there are exactly $|\operatorname{im}\varphi|$ number of cosets of $\ker(\varphi)$ that partition G, each of which has order $|\ker(\varphi)|$.

[0.0.37] Definition (*Normal Subgroup*)

Let H be a subgroup of G. Then H is said to be a **normal subgroup** if, for all $g \in G$ and $h \in H$, we have that $ghg^{-1} \in H$. That is, a subgroup is normal if conjugation of its elements is a closed operation.

[0.0.38] Theorem (*Equivalent Characterizations of Normal Subgroups*)

Let G be a group and H a subgroup. Then the following statements are equivalent.

(1) For every $g \in G$ and $h \in H$, $ghg^{-1} \in H$.

(2) For every $g \in G$, $gHg^{-1} \subseteq H$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

(3) For every $g \in G$, $gHg^{-1} = H$.

(4) For every $g \in G$, $gH = Hg$.

Proof. (1) $\implies$ (2): Fix $g \in G$. Since $ghg^{-1} \in H$ for every $h \in H$, note that $gHg^{-1} \subseteq H$ as desired.

(2) $\implies$ (3): Note that $gHg^{-1} \subseteq H$ for all $g \in G$, so we seek to show $H \subseteq gHg^{-1}$. Note that $g^{-1}Hg \subseteq H$ as well, and so conjugation of both sides yields

$$g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1} \implies H \subseteq gHg^{-1},$$

and so $gHg^{-1} = H$.

(3) $\implies$ (4): Suppose $gHg^{-1} = H$ for all $g \in G$. Right multiplying both sides by g yields $gH = Hg$.

(4) $\implies$ (1): Suppose $gH = Hg$ for every $g \in G$. Fix $g \in G$. For any $h \in H$, there exists some $h' \in H$ such that $gh = h'g$. Then note $ghg^{-1} = h' \in H$ for every $h \in H$. Since g was arbitrary, this holds for every $g \in G$, completing the proof.

Now we show some general groups we work with are normal subgroups.

[0.0.39] Theorem (*Subgroups of Abelian Groups are Normal*)

Suppose G is abelian. Then all subgroups H of G are normal.

Proof. Fix any subgroup $H \subseteq G$ and $g \in G$. Then note $ghg^{-1} = gg^{-1}h = h \in H$ for every $h \in H$, and so H is normal.

[0.0.40] Theorem (*Subgroups of Index 2 are Normal*)

Suppose G is a group and H is a subgroup such that $[G:H]=2$. Then H is a normal subgroup.

Proof. Since $[G:H]=2$, note that H partitions G into exactly two left cosets and exactly two right cosets. Because H itself is always a coset, the two left cosets must be H and its complement $G\setminus H$. Symmetrically, the two right cosets must also be H and $G\setminus H$.

We show that $gH=Hg$ for any $g\in G$. If $g\in H$, then $gH=H=Hg$ immediately. If $g\in G\setminus H$, then $gH\neq H$. Since left cosets partition G, gH must be the only other available left coset, namely $G\setminus H$. Symmetrically, $Hg\neq H$, meaning Hg must be the only other available right coset, which is also $G\setminus H$. Thus $gH=G\setminus H=Hg$. In all cases, $gH=Hg$, proving H is normal.

[0.0.41] Definition (*Center of Group*)

Let G be a group. The **center** of G, denoted $Z(G)$, is the set of elements in G that commute with every $g\in G$. That is,

$$Z(G)=\{z\in G: zg=gz \text{ for all } g\in G\}.$$

[0.0.42] Theorem (*Center is a Normal Subgroup*)

Let G be a group. Then $Z(G)$ is a normal subgroup.

Proof. Fix $g\in G$, and let $h\in Z(G)$ be arbitrary. Then note $ghg^{-1}=gg^{-1}h=h\in Z(G)$, and so $Z(G)$ is normal.

[0.0.43] Theorem (*Kernel of Homomorphism is Normal Subgroup*)

Let $\varphi: G\to H$ be a homomorphism. Then $\ker(\varphi)$ is a normal subgroup of G.

Proof. Fix $g\in G$. Suppose $h\in\ker(\varphi)$. Then note

$$\varphi(ghg^{-1})=\varphi(g)\varphi(h)\varphi(g^{-1})=\varphi(g)\varphi(g^{-1})=\varphi(\mathrm{id}_G)=\mathrm{id}_H,$$

and so $ghg^{-1}\in\ker(\varphi)$ as desired.

[0.0.44] Theorem (*Pushforward and Pullback on Normal Subgroups*)

Let $\varphi: G\to G'$ be a homomorphism. Let H be a subgroup of G and H' a subgroup of G'.

(1) $\varphi^{-1}(H')$ is a normal subgroup of G.

(2) $\varphi(H)$ is a normal subgroup of G' if φ is surjective.

Proof.

(1) Fix $g\in G$, and let $\varphi^{-1}(H')$. We show that, for any $k\in\varphi^{-1}(H)$, we also have that $gkg^{-1}\in\varphi^{-1}(H)$, making $\varphi^{-1}(H)$ normal. Note that H' is normal, and so $\varphi(g)\varphi(k)[\varphi(g)]^{-1}\in H'$ by definition. Thus $\varphi(gkg^{-1})\in H'$, and so $gkg^{-1}\in\varphi^{-1}(H')$ as desired.

(2) Let $y\in\varphi(H)$ and $g'\in G'$. We seek to show that $g'y(g')^{-1}\in\varphi(H)$. Because $y\in\varphi(H)$, there is some $h\in H$ such that $\varphi(h)=y$. Furthermore, because φ is surjective, there is some $g\in G$ such that $\varphi(g)=g'$. Substituting these yields

$$g'y(g')^{-1}=\varphi(g)\varphi(h)[\varphi(g)]^{-1}=\varphi(ghg^{-1}).$$

Since H is a normal subgroup of G, we have that $ghg^{-1} \in H$. Thus its image $\varphi(ghg^{-1})$ is strictly contained in $\varphi(H)$, meaning $g'y(g')^{-1} \in \varphi(H)$. Thus $\varphi(H)$ is normal in G'.

September 22nd, 2026

Recall that subgroups can be pushed forward and pulled back by a homomorphism. Indeed, the image and preimage of a subgroup are subgroups. Moreover, the preimage of a normal subgroup is also a normal subgroup, and the image of a normal subgroup is normal as well, if the image is surjective.

[0.0.45] Theorem (*Correspondence Theorem*)

Suppose $\varphi : G \to G'$ is a surjective homomorphism. Let $K = \ker(\varphi)$.

(1) There is a bijective correspondence

$$\{\text{subgroups of } G \text{ containing } K\} \longleftrightarrow \{\text{subgroups of } G'\}$$

given by $H \mapsto \varphi(H)$ and $\varphi^{-1}(H') \mapsfrom H'$.

(2) Suppose H, a subgroup of G containing K, corresponds to H' under this mapping.

- H is a normal subgroup of G if and only if H' is a normal subgroup of G'.
- The restriction $\varphi|_H : H \to H'$ is a surjective homomorphism with kernel K.
- $|H| = |K| \times |H'|$.

Proof.

(1) We first verify the mappings are well-defined and mutual inverses. We know the image and preimage of a subgroup under a homomorphism are always subgroups. Furthermore, for any subgroup $H' \subseteq G'$, note $\varphi(K) = \{\mathrm{id}_{G'}\} \subseteq H'$, meaning $K \subseteq \varphi^{-1}(H')$. Thus the domains and codomains of the bijection are correct.

To show they are inverses, note that $\varphi(\varphi^{-1}(H')) = H'$ follows immediately from the surjectivity of φ. Conversely, we show $\varphi^{-1}(\varphi(H)) = H$ for any subgroup H containing K. The inclusion $H \subseteq \varphi^{-1}(\varphi(H))$ is trivial. Let $x \in \varphi^{-1}(\varphi(H))$. Then $\varphi(x) = \varphi(h)$ for some $h \in H$. Rewriting yields $\varphi(h^{-1}x) = \mathrm{id}_{G'}$, meaning $h^{-1}x \in K$. Because $K \subseteq H$, we have $h^{-1}x \in H$, and since $h \in H$, closure forces $x \in H$. Thus $\varphi^{-1}(\varphi(H)) \subseteq H$, meaning $\varphi^{-1}(\varphi(H)) = H$, establishing the bijection.

(2) Suppose $H = \varphi^{-1}(H')$ and $H' = \varphi(H)$.

- We previously proved that the preimage of a normal subgroup is always normal, and the image of a normal subgroup is normal provided the homomorphism is surjective. The result comes immediately.
- The restriction $\varphi|_H : H \to H'$ is inherently a homomorphism. It is surjective because $H' = \varphi(H)$. The kernel of this restricted map is precisely $\{x \in H : \varphi(x) = \mathrm{id}_{G'}\} = H \cap K$. Because $K \subseteq H$, this collapses to K, and so $\ker(\varphi|_H) = K$.
- By applying the standard counting formula to the restricted map $\varphi|_H$, we immediately yield $|H| = |\ker(\varphi|_H)| \times |\mathrm{im}(\varphi|_H)| = |K| \times |H'|$.

[0.0.46] Remark

This proof is mostly straightforward, but some remarks are in order for (1). In general, the identity $\varphi^{-1}(\varphi(H)) = H$ is false. If you push a set forward and then pull it back, the set can get bigger because you accidentally grab extra elements that map to the same place. By our previous theorem, however, the set of all elements mapping to $\varphi(h)$ is exactly the coset hK. This is precisely why the assumption $K \subseteq H$ is so crucial. By the closure of H, multiplying any $h \in H$ by elements of $K \subseteq H$ keeps you strictly inside H. Thus, the entire pulled-back coset hK lies completely within H. The "extra" elements we grabbed were already inside H to begin with, ensuring the set does not actually grow.

Let G be a group together with a subgroup N. We already know that G/N, as a set, is the set of all left cosets of N. We ask if G/N can be endowed with some natural operation that can make it into a group. The answer is yes, but we require N to be a normal subgroup, for reasons we will see soon.

[0.0.47] Definition (*Coset Multiplication, Quotient Group*)

Suppose G is a group together with a normal subgroup N. For any two cosets $aN, bN \in G/N$, define **coset multiplication** by

$$(aN)(bN) = (ab)N.$$

Then G/N forms a group under this operation.

Note that G/N is not a subgroup of G, which is simultaneously obvious and surprising. It is not immediately clear that this forms a well-defined group operation. Indeed, since $aN = a'N$ if $a' \in aN$, we need to show that the choice of representative for the coset does not alter the result of multiplication.

[0.0.48] Theorem (*Well-Definedness of Coset Multiplication*)

Let N be a subgroup of G. The operation $(aN)(bN) = (ab)N$ is well-defined on the set of left cosets if and only if N is a normal subgroup of G.

Proof. We show that if N is normal, the operation is strictly independent of the chosen representatives. Suppose $aN = a'N$ and $bN = b'N$. We wish to show that $(a'b')N = (ab)N$.

By the equivalence class properties of cosets, we can write $a' = an_1$ and $b' = bn_2$ for some $n_1, n_2 \in N$. Then note

$$a'b' = (an_1)(bn_2) = a(n_1 b)n_2.$$

Because N is normal, its left and right cosets coincide, meaning $Nb = bN$. Thus, for our element $n_1 \in N$, there exists some $n_3 \in N$ such that $n_1 b = bn_3$. Substituting this yields

$$a'b' = a(bn_3)n_2 = ab(n_3 n_2).$$

Since N is a subgroup and is closed under multiplication, $n_3 n_2 \in N$. Thus $a'b'$ can be written as ab multiplied by an element of N, which immediately implies $a'b' \in abN$. Consequently, $(a'b')N = (ab)N$.

If N were not normal, the element $n_1 b$ could permanently escape bN, shifting the product into a completely different coset and causing the entire operation to be ill-defined.

Thus the subgroup for which quotienting by yields a group is precisely a normal subgroup. Having established that the operation is completely independent of the chosen representatives when N is normal, we may proceed to quickly verify the standard group axioms.

[0.0.49] Theorem (*Quotient Group Structure*)

Let N be a normal subgroup of G. The set of left cosets G/N forms a group under coset multiplication.

Proof.

(1) **Closure.** Since $a, b \in G$, their product $ab \in G$ by closure of the parent group, and so $(ab)N$ is indeed a valid coset in G/N.

(2) **Associativity.** For any $aN, bN, cN \in G/N$, note that

$$[(aN)(bN)](cN) = (ab)N \cdot cN = ((ab)c)N.$$

Because the operation in G is inherently associative, $((ab)c)N = (a(bc))N$. Thus

$$(a(bc))N = aN \cdot (bc)N = (aN)[(bN)(cN)],$$

satisfying associativity.

(3) **Identity.** The coset of the identity, $\mathrm{id}_G N = N$, serves as the identity element. For any $aN \in G/N$, we have

$$(aN)(N) = (a\mathrm{id}_G)N = aN, \quad \text{and} \quad (N)(aN) = (\mathrm{id}_G a)N = aN.$$

(4) **Inverse.** The inverse of aN is precisely $a^{-1}N$. Indeed,

$$(aN)(a^{-1}N) = (aa^{-1})N = \mathrm{id}_G N = N,$$

and symmetrically $(a^{-1}N)(aN) = N$.

Earlier, we proved that the kernel of any homomorphism is inherently a normal subgroup. We now resolve the natural converse: is every normal subgroup the kernel of some homomorphism? Having constructed the quotient group G/N, the answer is yes.

[0.0.50] Definition (*Canonical Projection Map*)

Let G be a group and N a normal subgroup of G. We define the **canonical projection map** $\pi : G \to G/N$ by

$$\pi(a) = aN.$$

[0.0.51] Theorem

The canonical projection map $\pi : G \to G/N$ is a surjective homomorphism with $\ker(\pi) = N$.

Proof. First, we show π is a homomorphism. For any $a, b \in G$, the definition of coset multiplication yields

$$\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b),$$

and so π preserves the group structure. Surjectivity is trivial, as any coset $aN \in G/N$ is immediately mapped to by $a \in G$. Finally, we determine the kernel. The identity element in G/N is the coset $\mathrm{id}_G N = N$. Thus, $a \in \ker(\pi)$ if and only if $\pi(a) = N$, meaning $aN = N$. This occurs if and only if $a \in N$. Therefore, $\ker(\pi) = N$.

Thus, a subgroup is normal if and only if it is the kernel of a homomorphism.

Having classically constructed the quotient group G/N by defining operations on cosets, we now take a step back. The quotient construction is not something exclusive to groups; it is a fundamental, structural mechanism that works with several constructions (sets, rings, topological spaces, and more). To truly understand what a quotient *is*, we must examine it by working with abstract objects, not simply groups. We start with sets.

Let A and B be arbitrary sets, and let $\sim$ be an equivalence relation on A. Recall that the equivalence classes of $\sim$ partition the set A, and we denote the equivalence class of an element $x \in A$ by $[x]_\sim$. We can define the **projection map** $\pi : A \to A/\sim$ by $\pi(x) = [x]_\sim$.

Suppose we have a function $f : A \to B$. We ask if we can push this function down through the quotient to define a new map on $A/\sim$. For this to make sense, the original function must be blind to the differences between equivalent elements.

[0.0.52] Definition (*Respecting an Equivalence Relation*)

Let $f : A \to B$ be a function and $\sim$ be an equivalence relation on A. We say that f **respects the equivalence relation** $\sim$ if f is constant on equivalence classes. That is, for all $x, y \in A$:

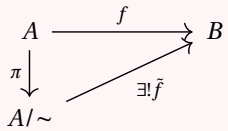
$$x \sim y \implies f(x) = f(y).$$

If f respects the equivalence relation, it guarantees that f acts on entire equivalence classes uniformly, allowing for a powerful factorization of the action of f.

[0.0.53] Theorem (*Universal Property of Quotients in* Set)

Let $\sim$ be an equivalence relation on a set A, and let $\pi : A \to A/\sim$ be the canonical projection map. For any set B and any function $f : A \to B$ that respects the equivalence relation $\sim$, there exists a unique function $\tilde{f} : A/\sim \to B$ such that $f = \tilde{f} \circ \pi$.

Equivalently, the following diagram commutes:



Proof. We must establish both the existence and the uniqueness of $\tilde{f}$.

- **Existence.** We define $\tilde{f}$ directly on the equivalence classes in $A/\sim$ by setting $\tilde{f}([x]_\sim) = f(x)$. Because elements of $A/\sim$ are sets (equivalence classes) rather than individual elements of A, we must verify this function is well-defined. Suppose $[x]_\sim = [y]_\sim$. This implies $x \sim y$. Because we assumed f respects the equivalence relation, $f(x) = f(y)$, and therefore $\tilde{f}([x]_\sim) = \tilde{f}([y]_\sim)$. The definition is independent of the chosen representative, so $\tilde{f}$ is a well-defined function. Furthermore, for any $x \in A$, we have $(\tilde{f} \circ \pi)(x) = \tilde{f}([x]_\sim) = f(x)$, ensuring the diagram commutes.
- **Uniqueness.** Suppose there is another function $g : A/\sim \to B$ such that $g \circ \pi = f$. We wish to show $g = \tilde{f}$. Let $[x]_\sim$ be an arbitrary element of $A/\sim$. Because π is inherently surjective, $[x]_\sim = \pi(x)$ for some $x \in A$. Then $g([x]_\sim) = g(\pi(x)) = f(x)$. But we already know $f(x) = \tilde{f}(\pi(x)) = \tilde{f}([x]_\sim)$. Thus $g([x]_\sim) = \tilde{f}([x]_\sim)$ for all classes in the quotient, forcing $g = \tilde{f}$.

[0.0.54] Remark (*The Canonical Decomposition in* Set)

The universal property of quotients gives us a powerful tool to mechanically "repair" arbitrary functions. Let $f : A \to B$ be any generic set function. Generally, f fails to be a bijection (an isomorphism in the category of sets) for two reasons. First, it may fail surjectivity (missing elements in B). Second, it may fail injectivity (collapsing distinct elements of A to the same target).

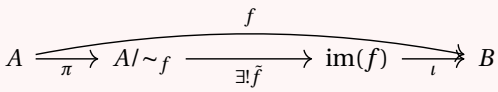
We can resolve both of these flaws. First, we fix surjectivity by restricting our codomain to the image, $\mathrm{im}(f)$. The map from A to $\mathrm{im}(f)$ is trivially surjective, and we can seamlessly include $\mathrm{im}(f)$ back into B via an injective inclusion map $\iota : \mathrm{im}(f) \to B$.

Second, we fix injectivity by defining a natural equivalence relation on A induced by the function itself. Define $x \sim_f y$ if and only if $f(x) = f(y)$. By definition, f trivially respects the equivalence relation $\sim_f$. Quotienting A by $\sim_f$ "glues" all elements that map to the same target into a single equivalence class. Immediately, we see that the universal property of quotients yields a unique map $\tilde{f} : A/\sim_f \to \mathrm{im}(f)$.

Because we restricted the codomain to $\mathrm{im}(f)$, $\tilde{f}$ is surjective. Because we quotiented out the exact elements that caused collisions, $\tilde{f}$ is strictly injective. Thus, $\tilde{f}$ is a forced bijection.

[0.0.55] Theorem (*Canonical Decomposition of Functions*)

Any function $f : A \to B$ can be uniquely factored as the composition of a surjection, a bijection, and an injection. This factorization, $f = \iota \circ \tilde{f} \circ \pi$, is captured by the following commutative diagram:



where $\pi : A \to A/\sim_f$ is the surjective projection map, $\tilde{f} : A/\sim_f \to \mathrm{im}(f)$ is a natural bijection, and $\iota : \mathrm{im}(f) \to B$ is the injective inclusion map.

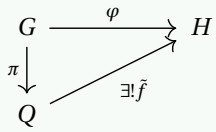
Any function f is secretly just a bijection wrapped in layers of redundancy (collapsing elements) and deficiency (missing the target). In our canonical decomposition diagram, the first part of the sequence (the projection π) acts as the quotient fix to resolve injectivity issues, while the last part (the inclusion ι) acts as the embedding fix to resolve surjectivity issues. By quotienting the domain and restricting the codomain, we strip away these flaws to isolate $\tilde{f}$, a faithful representation capturing the core mechanism as to how f operates.

We now transport this idea into the category of groups. Previously, we classically constructed the quotient group G/N by defining coset multiplication, proving that it forms a group if and only if N is a normal subgroup of G. Instead of building the quotient from the ground up and verifying it works, we can equivalently *define* the quotient entirely by demanding it satisfies a universal property analogous to the one in Set, and then locate the object that fits the description.

[0.0.56] Definition (*Categorical Quotient Group*)

Let G be a group and N a normal subgroup of G. The **quotient of G by N** is a group Q together with a surjective homomorphism $\pi : G \to Q$ with $\ker(\pi) = N$, satisfying the following universal property.

For any group H and any homomorphism $\varphi : G \to H$ where $N \subseteq \ker(\varphi)$, there exists a unique homomorphism $\tilde{f} : Q \to H$ such that $\tilde{f} \circ \pi = \varphi$.



One might wonder why we still constrain N to be a normal subgroup in a supposedly pure, structural definition. Because we explicitly demand π to be a homomorphism with $\ker(\pi) = N$, and the kernel of any homomorphism is inherently normal, the rigid structure of groups strictly prohibits non-normal subgroups from ever acting as kernels. Thus, in the categorical lens, a normal subgroup is not an arbitrary set-theoretic restriction, but simply the name we give to a subgroup capable of being a kernel for some homomorphism.

Furthermore, the condition $N \subseteq \ker(\varphi)$ is exactly the group-theoretic translation of a set function respecting an equivalence relation. If elements in N get crushed to the identity by φ, then φ is completely blind to differences between elements that differ by an element of N.

Before we confirm our classical coset space fits this definition, we must show that this universal property is actually rigid. By a standard diagram chase, any two objects satisfying this property are uniquely isomorphic, meaning the quotient is structurally unique.

[0.0.57] Theorem (*Uniqueness of the Categorical Quotient*)

Let (Q_1, π_1) and (Q_2, π_2) be two quotients of G by N satisfying the universal property. Then there exists a unique isomorphism $\alpha : Q_1 \to Q_2$ such that $\alpha \circ \pi_1 = \pi_2$.

Proof. Since (Q_1, π_1) satisfies the universal property and $\pi_2 : G \to Q_2$ is a homomorphism with $\ker(\pi_2) = N \subseteq \ker(\pi_2)$ (trivially), there exists a unique homomorphism $\alpha : Q_1 \to Q_2$ such that $\alpha \circ \pi_1 = \pi_2$.

Symmetrically, since (Q_2, π_2) satisfies the universal property and $\pi_1 : G \to Q_1$ is a homomorphism with $N \subseteq \ker(\pi_1)$, there exists a unique homomorphism $\beta : Q_2 \to Q_1$ such that $\beta \circ \pi_2 = \pi_1$.

Substituting the first identity into the second yields $\beta \circ (\alpha \circ \pi_1) = \pi_1$, which we reassociate as $(\beta \circ \alpha) \circ \pi_1 = \pi_1$.

Now, consider the universal property of Q_1 applied to the homomorphism $\pi_1 : G \to Q_1$. We seek a unique map $u : Q_1 \to Q_1$ such that $u \circ \pi_1 = \pi_1$. The identity map id_{Q_1} trivially satisfies this. However, we just showed that $\beta \circ \alpha$ also satisfies this. By the strict uniqueness guaranteed by the universal property, we are forced to conclude $\beta \circ \alpha = \mathrm{id}_{Q_1}$.

By an identical symmetric argument, $\alpha \circ \beta = \mathrm{id}_{Q_2}$. Thus α is a bijection, and since it is inherently a homomorphism, it is an isomorphism. This establishes that $Q_1 \cong Q_2$.

We now confirm that our classically constructed set of cosets is indeed the exact object requested by this universal property.

[0.0.58] Theorem (*Coset Space Satisfies the Universal Property*)

The classically constructed coset space G/N equipped with coset multiplication $(aN)(bN) = (ab)N$, paired with the canonical projection $\pi(a) = aN$, satisfies the universal property of the quotient group.

Proof. Let $\varphi : G \to H$ be a homomorphism such that $N \subseteq \ker(\varphi)$. We must show there exists a unique homomorphism $\tilde{f} : G/N \to H$ making the diagram commute.

- **Well-definedness.** We propose $\tilde{f}(aN) = \varphi(a)$. Because we are defining this on cosets (equivalence classes), we must check it is strictly independent of the representative. Suppose $aN = bN$. This means $b^{-1}a \in N$. Because $N \subseteq \ker(\varphi)$, this implies $\varphi(b^{-1}a) = \mathrm{id}_H$. Since φ is a homomorphism, $\varphi(b)^{-1}\varphi(a) = \mathrm{id}_H$, meaning $\varphi(a) = \varphi(b)$. Thus $\tilde{f}(aN) = \tilde{f}(bN)$, so $\tilde{f}$ is well-defined.
- **Homomorphism.** We verify that $\tilde{f}$ respects the group operation. Indeed, note
$$\tilde{f}((aN)(bN)) = \tilde{f}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{f}(aN)\tilde{f}(bN).$$
Thus $\tilde{f}$ is a valid group homomorphism. By construction, $\tilde{f}(\pi(a)) = \tilde{f}(aN) = \varphi(a)$, ensuring the diagram commutes.
- **Uniqueness.** Suppose $g : G/N \to H$ is another homomorphism satisfying $g \circ \pi = \varphi$. For any coset $aN \in G/N$, we have $g(aN) = g(\pi(a)) = \varphi(a)$. But $\varphi(a) = \tilde{f}(aN)$. Since g and $\tilde{f}$ agree on all elements, $g = \tilde{f}$.

[0.0.59] Remark (*The Canonical Decomposition in* Grp)

We conclude by applying our canonical decomposition setup from Set to group homomorphisms. Let $\varphi : G \to H$ be an arbitrary homomorphism. Like any general function, it may fail to be an isomorphism due to a lack of injectivity or a lack of surjectivity.

We resolve surjectivity by mapping onto the image $\mathrm{im}(\varphi)$, which is a valid subgroup of H. We resolve injectivity by defining the equivalence relation $a \sim_\varphi b \iff \varphi(a) = \varphi(b)$. In the language of groups, $\varphi(a) = \varphi(b)$ implies $a^{-1}b \in \ker(\varphi)$. Thus, the equivalence classes $[a]_{\sim_\varphi}$ are exactly the left cosets $a\ker(\varphi)$.

Because the kernel of any homomorphism is inherently a normal subgroup of G, the quotient space $G/\ker(\varphi)$ naturally forms a group. By its very definition, φ respects the equivalence relation generated by its own kernel. The universal property immediately gives us a unique, well-defined homomorphism $\tilde{f} : G/\ker(\varphi) \to \mathrm{im}(\varphi)$.

Because we quotiented by the exact subgroup causing injectivity collisions, $\tilde{f}$ is injective. Because we restricted the codomain, $\tilde{f}$ is surjective. Therefore, $\tilde{f}$ is an isomorphism.

The First Isomorphism Theorem is not a standalone group-theoretic trick. It is the realization of the universal canonical decomposition of maps in an arbitrary category, simply applied to Grp. Injectivity is factored out by quotienting by the kernel, surjectivity is factored out by restricting to the image, and we are left with $\tilde{f}$, the underlying isomorphism that faithfully represents φ.

[0.0.60] Theorem (*First Isomorphism Theorem*)

Let $\varphi : G \to H$ be a group homomorphism. Then φ induces a canonical isomorphism
$$G/\ker(\varphi) \cong \mathrm{im}(\varphi)$$
given by the map $\tilde{f}(a\ker(\varphi)) = \varphi(a)$.

September 24th, 2026