# MATH 343 — Group Theory

Chapter 0: Preliminaries

# Chapter 0 — Preliminaries

**What this chapter provides.** The integer facts, induction principles, equivalence relations and function language that every later chapter of MATH 343 assumes.

**Reference.** Gallian, *Contemporary Abstract Algebra*, 10th ed., Chapter 0.

**Four parts.**

1. Properties of the integers — divisibility, gcd, lcm, primes
2. Modular arithmetic
3. Mathematical induction
4. Equivalence relations, partitions, and functions

# Part 1 — Properties of the Integers

**GOAL.** Establish the arithmetic facts used throughout the course:

## IN THIS PART

- Well Ordering Principle
- Divisibility, primes, multiples
- The Division Algorithm (Thm 0.1)
- gcd as a linear combination (Thm 0.2) and its corollary
- Euclid's Lemma (Lemma 0.1)
- Fundamental Theorem of Arithmetic (Thm 0.3)
- lcm and the $\gcd \cdot \operatorname{lcm}$ identity

# Well Ordering Principle

**Axiom (Well Ordering Principle).** Every nonempty set of **positive** integers contains a smallest member.

**Why an axiom.** It cannot be derived from the usual arithmetic properties of $\mathbb{Z}$, so we assume it.

**Where it is used.** It is the engine behind the Division Algorithm (Thm 0.1), Theorem 0.2, and both principles of induction.

**CAUTION.** "Positive" is essential. The set $\{\ldots, -3, -2, -1\}$ is a nonempty set of integers with **no** smallest member.

# Divisibility

**DEFINITION.** A nonzero integer $t$ is a **divisor** of an integer $s$ if there exists an integer $u$ with $s = tu$.

**NOTATION.** $t \mid s$ means "$t$ divides $s$"; $t \nmid s$ means "$t$ does not divide $s$".

**DEFINITION.** An integer $s$ is a **multiple** of $t$ if $s = tu$ for some integer $u$.

**DEFINITION.** A **prime** is a positive integer greater than 1 whose only positive divisors are 1 and itself.

**Warning on notation.** $t \mid s$ is a **statement** (true or false); $t/s$ is a **number**. Never write $t \mid s = 0$.

# The Division Algorithm (Theorem 0.1)

**Theorem 0.1 (Division Algorithm).** Let $a$ and $b$ be integers with $b > 0$. Then there exist **unique** integers $q$ and $r$ with

$$a = bq + r, \qquad 0 \leq r < b.$$

**Two assertions, not one.**

- **Existence** of a pair $(q, r)$ — proved from the Well Ordering Principle.
- **Uniqueness** of that pair — proved separately.

---

**TERMINOLOGY.** $q$ is the **quotient** and $r$ the **remainder** on dividing $a$ by $b$.

# Division Algorithm — Examples

**EXAMPLE 1.** $a = 17, b = 5$: $17 = 5 \cdot 3 + 2$, so $q = 3, r = 2$.

**EXAMPLE 2.** $a = -23, b = 6$: $-23 = 6(-4) + 1$, so $q = -4, r = 1$.

**Note the negative case.** The remainder is still required to satisfy $0 \leq r < b$, so $r = 1$, **not** $r = -5$. A calculator that returns $-23/6 = -3.83$ gives $q = -4$ only after rounding **down**.

**Standard proof strategy.** To show $b \mid a$, write $a = bq + r$ with $0 \leq r < b$ and then argue that $r = 0$.

# Quick Check — Division Algorithm

**Apply the Division Algorithm to −23 with divisor 6: write $-23 = 6q + r$ with $0 \le r < 6$.**

**(A)** $q = -3, r = -5$

**(B)** $q = -4, r = 1$

**(C)** $q = -3, r = 1$

**(D)** $q = -4, r = -1$

Vote now — one answer only.

# Greatest Common Divisor

**DEFINITION.** The **greatest common divisor** of two nonzero integers $a$ and $b$ is the largest of all common divisors of $a$ and $b$. Written $\gcd(a, b)$.

**DEFINITION.** When $\gcd(a, b) = 1$ we say $a$ and $b$ are **relatively prime**.

**EXAMPLES.**

- $\gcd(4,15) = 1$, so $4$ and $15$ are relatively prime.
- $\gcd(4,10) = 2$, so $4$ and $10$ are not.
- $\gcd\left(2^2 \cdot 3^2 \cdot 5,\ 2 \cdot 3^3 \cdot 7^2\right) = 2 \cdot 3^2$.

# gcd as a Linear Combination (Theorem 0.2)

**THEOREM 0.2.** For any nonzero integers $a$ and $b$ there exist integers $s$ and $t$ with

$$\gcd(a, b) = as + bt.$$

Moreover, $\gcd(a, b)$ is the **smallest positive integer** of the form $as + bt$.

**Existence, not construction.** The theorem guarantees that $s, t$ exist; it does not produce them. The Euclidean algorithm, run backwards, does.

**Not unique.** $\gcd(4,10) = 2 = 4(-2) + 10(1) = 4(3) + 10(-1)$.

# Corollary — Relatively Prime Characterization

**Corollary (to Theorem 0.2).** Integers $a$ and $b$ are relatively prime **if and only if** there exist integers $s$ and $t$ with

$$as + bt = 1.$$

**Both directions matter.**

- ($\Rightarrow$) is Theorem 0.2 applied when $\gcd(a, b) = 1$.
- ($\Leftarrow$) any common divisor of $a$ and $b$ divides $as + bt = 1$, hence equals $\pm 1$.

**EXAMPLES.** $4 \cdot 4 + 15(-1) = 1$, confirming $\gcd(4,15) = 1$.

# Application: Polynomial Expressions

**Example (Gallian, Ch. 0, Example 3).** For every integer $n$, the integers $n+1$ and $n^2+n+1$ are relatively prime.

**PROOF.** Observe

$$\left(n^2+n+1\right)-n(n+1)=n^2+n+1-n^2-n=1.$$

So $\left(n^2+n+1\right)\cdot 1+(n+1)(-n)=1.$

By the Corollary to Theorem 0.2, $\gcd\left(n+1,\ n^2+n+1\right)=1.$ ▫

**Why this is the standard technique.** To prove two polynomial expressions are relatively prime, exhibit an explicit integer combination equal to $1$.

# Euclid's Lemma (Lemma 0.1)

**Lemma 0.1 (Euclid's Lemma).** If $p$ is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

**PROOF.** Suppose $p \mid ab$. If $p \mid a$ we are done, **so assume** $p \nmid a$ **and show** $p \mid b$**.**

Since $p$ is prime and $p \nmid a$, the only positive common divisors of $p$ and $a$ are $1$, so $\gcd(p, a) = 1$.

By the Corollary to Theorem 0.2 there are integers $s, t$ with $1 = as + pt$.

Multiply by $b$: $b = abs + ptb$.

Now $p \mid ab \Rightarrow p \mid abs$, and $p \mid p \Rightarrow p \mid ptb$.

Hence $p \mid (abs + ptb) = b$. ▫

# Euclid's Lemma — Primality Is Essential

**The hypothesis cannot be dropped.**

Take $p = 6, a = 4, b = 3$:

$$6 \mid (4 \cdot 3) = 12, \qquad \text{but} \qquad 6 \nmid 4 \quad \text{and} \quad 6 \nmid 3.$$

**Diagnosis.** $6 = 2 \cdot 3$ is composite, so its prime factors can split between $a$ and $b$.

**Look ahead.** This is exactly the phenomenon behind zero divisors: in $\mathbb{Z}_6$, $4 \cdot 3 = 0$ although $4 \neq 0$ and $3 \neq 0$.

# Fundamental Theorem of Arithmetic (Theorem 0.3)

**THEOREM 0.3.** Every integer greater than 1 is a prime or a product of primes. This product is unique except for the order of the factors.

**Precisely.** If

$$n = p_1 p_2 \cdots p_r \quad \text{and} \quad n = q_1 q_2 \cdots q_s$$

with all $p_i, q_j$ prime, then $r = s$ and, after renumbering, $p_i = q_i$ for all $i$.

**Two assertions again.** Existence (every $n > 1$ factors) and uniqueness (the factorisation is essentially one). Uniqueness rests on Euclid's Lemma.

# Application: Irrationality of $\sqrt[n]{2}$

**CLAIM.** For every integer $n > 1$, $\sqrt[n]{2}$ is irrational.

**PROOF.** Suppose $\sqrt[n]{2} = a/b$ with $a, b$ positive integers and $\gcd(a, b) = 1$.

Then $2 = a^n/b^n$, so $2b^n = a^n$.

So $2 \mid a^n$, and since $2$ is prime, **Euclid's Lemma** gives $2 \mid a$.

Write $a = 2c$. Then $2b^n = (2c)^n = 2^n c^n$, so $b^n = 2^{n-1}c^n$.

Since $n > 1$ we have $n - 1 \geq 1$, so $2 \mid b^n$, and by Euclid's Lemma again $2 \mid b$.

But then $2 \mid \gcd(a, b) = 1$, a contradiction. ▫

# Least Common Multiple

**DEFINITION.** The **least common multiple** of nonzero integers $a$ and $b$ is the smallest **positive** integer that is a multiple of both. Written $\text{lcm}(a, b)$.

**EXAMPLES.**

- $\text{lcm}(4,6) = 12$
- $\text{lcm}(4,8) = 8$
- $\text{lcm}(10,12) = 60$
- $\text{lcm}(6,5) = 30$
- $\text{lcm}\left(2^2 \cdot 3^2 \cdot 5,\ 2 \cdot 3^3 \cdot 7^2\right) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2$

# gcd and lcm Together

**IDENTITY.** For positive integers $a, b$:

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab.$$

**CHECK.** $a = 4, b = 6$: $\gcd = 2$, $\operatorname{lcm} = 12$, and $2 \cdot 12 = 24 = 4 \cdot 6$. ✓

**From prime factorizations.** If $a = \prod p_i^{\alpha_i}$ and $b = \prod p_i^{\beta_i}$ then

$$\gcd = \prod p_i^{\min(\alpha_i,\beta_i)}, \qquad \operatorname{lcm} = \prod p_i^{\max(\alpha_i,\beta_i)},$$

and $\min + \max = \alpha_i + \beta_i$ gives the identity.

**Where this returns.** Orders of elements in $\mathbb{Z}_n$ and in direct products (Chapters 4 and 8).

# Part 2 — Modular Arithmetic

**GOAL.** Define $a \bmod n$, establish the one property that makes computation practical, and see it applied.

**Why it matters here.** $\mathbb{Z}_n$ under addition modulo $n$ is the first infinite family of groups in this course, and the first family of *cyclic* groups.

# Motivation: Counting Cyclically

**QUESTION.** If it is September, what month will it be $25$ months from now?

**Answer.** October, since $25 = 2 \cdot 12 + 1$ — two full years plus one month.

**QUESTION.** If it is Wednesday, what day will it be in $23$ days?

**Answer.** Friday, since $23 = 7 \cdot 3 + 2$.

**Key insight.** We do not count sequentially; we use **remainders**. The Division Algorithm is doing the work.

# The mod Notation

**DEFINITION.** Let $n > 0$. By Theorem 0.1 write $a = qn + r$ with $0 \leq r < n$. Then

$$a \bmod n = r.$$

**Two hypotheses that are easy to lose.**

- $n > 0$;
- $0 \leq r < n$ — the remainder is always taken in $\{0,1, \ldots, n-1\}$.

# The mod Notation — **EXAMPLES**

- $3 \bmod 2 = 1$ since $3 = 1 \cdot 2 + 1$
- $6 \bmod 2 = 0$ since $6 = 3 \cdot 2 + 0$
- $11 \bmod 3 = 2$ since $11 = 3 \cdot 3 + 2$
- $62 \bmod 85 = 62$ since $62 = 0 \cdot 85 + 62$
- $-2 \bmod 15 = 13$ since $-2 = (-1) \cdot 15 + 13$

# The Key Property

**THEOREM.** $a \bmod n = b \bmod n$ **if and only if** $n \mid (a - b)$.

**Consequence (mod first).** For any $a, b$:

$$(a + b) \bmod n = \big((a \bmod n) + (b \bmod n)\big) \bmod n,$$

$$(ab) \bmod n = \big((a \bmod n)(b \bmod n)\big) \bmod n.$$

**EXAMPLE.** Compute $(27 \cdot 36) \bmod 11$.

- $27 \bmod 11 = 5$ and $36 \bmod 11 = 3$
- $(27 \cdot 36) \bmod 11 = (5 \cdot 3) \bmod 11 = 15 \bmod 11 = 4$

# Common Errors with mod

**Cancellation fails.** $6 \cdot 2 \equiv 6 \cdot 7 \pmod{10}$ (both are $2$), but $2 \not\equiv 7 \pmod{10}$. You may **not** cancel the $6$.

Cancellation of $c$ modulo $n$ is valid only when $\gcd(c, n) = 1$.

**Exponents are not reduced modulo $n$.** $2^5 \bmod 5 = 32 \bmod 5 = 2$, whereas $2^{5 \bmod 5} = 2^0 = 1$.

**Division is not defined.** $a/b \bmod n$ has no meaning in general; $3$ has no multiplicative inverse modulo $6$.

# Quick Check — Cancellation mod n

**Suppose $6a \equiv 6b \pmod{10}$. What may you correctly conclude?**

**(A)** $a \equiv b \pmod{10}$

**(B)** $a \equiv b \pmod{5}$

**(C)** $a = b$

**(D)** Nothing at all

Vote now — one answer only.

# Application: Check Digits

**US Postal Service money orders.** A $10$-digit identification number is followed by a check digit equal to that number modulo $9$.

**EXAMPLE.** $3953988164$ has check digit $2$, since $3953988164 \bmod 9 = 2$.

*(Digit sum* $3 + 9 + 5 + 3 + 9 + 8 + 8 + 1 + 6 + 4 = 56$ *and* $56 \bmod 9 = 2$*.)*

**Error detection.** If $39539881642$ is mistyped as $39559881642$, the machine recomputes the check digit as $4$ but reads $2$ — error detected.

**Limitation.** A mod-$9$ scheme cannot detect a transposition of two digits, since digit order does not affect the digit sum.

# Part 3 — Mathematical Induction

**GOAL.** State both induction principles precisely and see when each is the right tool.

**Both rest on the Well Ordering Principle.**

# First Principle of Induction (Theorem 0.5)

**THEOREM 0.5.** Let $S$ be a set of integers containing $a$. Suppose $S$ has the property that whenever an integer $n \geq a$ belongs to $S$, then $n + 1$ also belongs to $S$. Then $S$ contains every integer greater than or equal to $a$.

**In practice.** To prove a statement $P(n)$ for all $n \geq a$, take $S = \{n: P(n) \text{ is true}\}$ and verify:

1. **Base case:** $P(a)$ holds.
2. **Inductive step:** $P(n) \Rightarrow P(n+1)$ for every $n \geq a$.

# Induction — Worked Example

**CLAIM.** For every integer $n \geq 1$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

**Base case.** $n = 1$: left side $= 1$, right side $= \frac{1 \cdot 2}{2} = 1$. ✓

**Inductive step.** Assume $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for some $n \geq 1$. Then

$$1 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2}$$
$$= \frac{(n+1)(n+2)}{2},$$

which is the claim for $n + 1$.

By Theorem 0.5 the formula holds for all $n \geq 1$. ▫

# Second Principle of Induction (Theorem 0.6)

**Theorem 0.6 (Strong Induction).** Let $S$ be a set of integers containing $a$. Suppose $n$ belongs to $S$ whenever **every** integer $m$ with $a \leq m < n$ belongs to $S$. Then $S$ contains every integer greater than or equal to $a$.

**When to use it.** When establishing $P(n)$ needs $P(m)$ for several smaller $m$, not just $P(n-1)$.

**NOTE.** No separate base case is written: the hypothesis applied at $n = a$ is vacuous, and forces $a \in S$.

# Strong Induction — Worked Example

**Claim (existence half of Theorem 0.3).** Every integer $n > 1$ is a prime or a product of primes.

**PROOF.** Let $n > 1$ and assume the claim holds for every integer $m$ with $1 < m < n$.

- If $n$ is prime, we are done.
- Otherwise $n = ab$ with $1 < a < n$ and $1 < b < n$.

By the inductive hypothesis each of $a, b$ is a prime or a product of primes, hence so is $ab = n$.

By Theorem 0.6 the claim holds for all $n > 1$. ▫

**Why the first principle would not do.** The factors $a$ and $b$ are not $n - 1$.

# Part 4 — Equivalence Relations and Functions

**GOAL.** The two structural tools used constantly from Chapter 6 onward.

## IN THIS PART

**Equivalence relations and partitions** — the mechanism behind cosets (Ch. 7) and factor groups (Ch. 9).

**Functions** — one-to-one, onto, composition, inverses; the language of isomorphism (Ch. 6) and homomorphism (Ch. 10).

# Equivalence Relations — Motivation

**In different contexts, different objects count as "the same".**

- $2 + 1$ and $4 + 4$ differ in $\mathbb{Z}$, but agree modulo $5$ (both give $3$).
- Congruent triangles in different positions.
- Vectors with the same magnitude and direction.

**Need.** A formal mechanism for declaring when two objects are to be treated as equivalent — and a guarantee that doing so partitions the set cleanly.

# Definition of Equivalence Relation

**DEFINITION.** An **equivalence relation** on a set $S$ is a set $R$ of ordered pairs **of elements of** $S$ such that:

1. **Reflexive:** $(a, a) \in R$ for all $a \in S$
2. **Symmetric:** $(a, b) \in R$ implies $(b, a) \in R$
3. **Transitive:** $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$

**NOTATION.** Write $a \sim b$ in place of $(a, b) \in R$.

**Equivalence class.** $[a] = \{x \in S \mid x \sim a\}$.

# Examples of Equivalence Relations

**Example 1 — Similar triangles.**

- $S =$ all triangles in the plane
- $a \sim b$ if $a$ and $b$ are similar (equal corresponding angles)

**Example 2 — Polynomials with the same derivative.**

- $S = \mathbb{R}[x]$, polynomials with real coefficients
- $f \sim g$ if $f' = g'$
- $[f] = \{f + c \mid c \in \mathbb{R}\}$

**Non-example.** On $\mathbb{Z}$, "$a \sim b$ if $a \mid b$" is reflexive and transitive but **not symmetric**: $2 \mid 4$ while $4 \nmid 2$.

# Modular Congruence

**Example 3 — Congruence modulo $n$.** Fix a positive integer $n$ on $S = \mathbb{Z}$:

$$a \equiv b \pmod{n} \quad \text{means} \quad n \mid (a - b).$$

**Verification.**

- **Reflexive:** $a - a = 0$ and $n \mid 0$, so $a \equiv a$. ✓
- **Symmetric:** if $n \mid (a - b)$ then $n \mid -(a - b) = (b - a)$, so $b \equiv a$. ✓
- **Transitive:** if $n \mid (a - b)$ and $n \mid (b - c)$ then $n$ divides the sum $(a - b) + (b - c) = a - c$, so $a \equiv c$. ✓

**Equivalence classes.** $[a] = \{a + kn \mid k \in \mathbb{Z}\}$ — these are the elements of $\mathbb{Z}_n$.

# Rational Numbers as Equivalence Classes

**Example 4 — Fraction equivalence.**

- $S = \{(a, b) \mid a, b \in \mathbb{Z},\ b \neq 0\}$
- $(a, b) \sim (c, d)$ if $ad = bc$

**Verification.**

- **Reflexive:** $ab = ba$.
- **Symmetric:** $ad = bc \Rightarrow cb = da$.
- **Transitive:** if $ad = bc$ and $cf = de$, then $adf = bcf = bde$; since $d \neq 0$, cancel to get $af = be$.

**Interpretation.** $[(a, b)]$ *is* the rational number $a/b$; equal fractions are exactly equivalent pairs.

# Partitions

**DEFINITION.** A **partition** of a set $S$ is a collection of nonempty, **pairwise disjoint** subsets of $S$ whose union is $S$.

**Example (Gallian, Ch. 0, Example 21).** The sets

$$\{0\}, \qquad \{1,2,3,\dots\}, \qquad \{\dots,-3,-2,-1\}$$

form a partition of $\mathbb{Z}$.

**Non-example (Gallian, Example 22).** The nonnegative integers together with the nonpositive integers do **not** partition $\mathbb{Z}$: both sets contain $0$, so they are not disjoint.

**Key point.** Nonempty, disjoint, and covering — all three are required.

# Equivalence Classes Form Partitions (Theorem 0.7)

**THEOREM 0.7.** The equivalence classes of an equivalence relation on a set $S$ constitute a partition of $S$.

**Converse.** For any partition $P$ of $S$ there is an equivalence relation on $S$ whose equivalence classes are precisely the members of $P$.

**Big picture.** Equivalence relations and partitions are two descriptions of one structure.

**Where this is used.** The left cosets of a subgroup $H \leq G$ are the equivalence classes of $a \sim b \Leftrightarrow a^{-1}b \in H$ — which is why they partition $G$ (Chapter 7).

# Proof Strategy for Theorem 0.7

**To show the equivalence classes partition $S$:**

1. **Nonempty:** each $[a]$ contains $a$, by reflexivity.
2. **Union is $S$:** every $a \in S$ lies in $[a]$, so the classes cover $S$.
3. **Disjoint:** if $[a] \neq [b]$ then $[a] \cap [b] = \varnothing$.

**Step 3, in detail.** Suppose $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$.

By **symmetry**, $a \sim c$; then by **transitivity** with $c \sim b$ we get $a \sim b$, and hence $[a] = [b]$.

So, two classes are either equal or disjoint.

# Functions (Mappings)

**DEFINITION.** A **function** (or **mapping**) $\varphi$ from a set $A$ to a set $B$ is a rule assigning to each element $a \in A$ exactly one element $b \in B$.

**NOTATION.** $\varphi: A \to B$, and $\varphi(a) = b$.

**Gallian's terminology.**

- $A$ is the **domain** of $\varphi$
- $B$ is the **range** of $\varphi$
- $b$ is the **image** of $a$ under $\varphi$
- $\{\varphi(a) \mid a \in A\} \subseteq B$ is the **image of $A$ under $\varphi$**

# Terminology Warning: "Range"

> **This textbook is not standard here.** In Gallian's language "$\varphi$ is onto" is a genuine condition on $\varphi$; if *range* meant the image set, every function would be onto its range and the word would be empty. **In this course we follow Gallian —** read *range* carefully in outside sources.

| Term | Gallian's meaning | Meaning in most other texts |
|---|---|---|
| **range** of $\phi : A \to B$ | the set B | the set $\{ \phi(a) : a \in A \}$ |
| **codomain** | (not used) | the set B |
| **image of A** | $\{ \phi(a) : a \in A \}$ | same |

# Well-Definedness

**The issue.** When elements of the domain have more than one representation, a "rule" may fail to be a function.

**Bad example.** Define $\varphi(a/b) = a + b$ on $\mathbb{Q}$.

- $\varphi(1/2) = 1 + 2 = 3$
- $\varphi(2/4) = 2 + 4 = 6$
- But $1/2 = 2/4$, so $\varphi$ assigns two values to one element — not a function.

**Test.** A rule is well defined when $x_1 = x_2$ implies $\varphi(x_1) = \varphi(x_2)$.

**Where this returns.** Every map defined on cosets, $\varphi(aH) = \cdots$, must be checked this way (Chapters 9 and 10).

# Composition of Functions

**DEFINITION.** Let $\varphi: A \to B$ and $\psi: B \to C$. The **composition** $\psi\varphi$ is the map $A \to C$ given by

$$(\psi\varphi)(a) = \psi\big(\varphi(a)\big) \qquad \text{for all } a \in A.$$

**NOTATION.** We write $\psi\varphi$, not $\psi \circ \varphi$ — the circle is omitted throughout this book.

**Order.** $\psi\varphi$ means "$\varphi$ first, then $\psi$" — right to left.

# Composition — Example

**Example (Gallian, Ch. 0, Example 23).** Let $f(x) = 2x + 3$ and $g(x) = x^2 + 1$.

**At a point.**

- $(fg)(5) = f\big(g(5)\big) = f(26) = 55$
- $(gf)(5) = g\big(f(5)\big) = g(13) = 170$

**In general.**

- $(fg)(x) = f\big(x^2 + 1\big) = 2\big(x^2 + 1\big) + 3 = 2x^2 + 5$
- $(gf)(x) = g(2x + 3) = (2x + 3)^2 + 1 = 4x^2 + 12x + 10$

**Key point.** $fg \neq gf$ in general — composition is **not** commutative.

# One-to-One Functions

**DEFINITION.** $\varphi: A \to B$ is **one-to-one** if

$$\varphi(a_1) = \varphi(a_2) \;\Rightarrow\; a_1 = a_2 \qquad \text{for all } a_1, a_2 \in A.$$

**Equivalent (contrapositive).** $a_1 \neq a_2 \Rightarrow \varphi(a_1) \neq \varphi(a_2)$.

**Picture.** Each element of $B$ is the image of **at most one** element of $A$.

**How it is proved.** Assume $\varphi(a_1) = \varphi(a_2)$ and derive $a_1 = a_2$. This is the direction that works; the contrapositive form is harder to use.

# Onto Functions

**DEFINITION.** $\varphi: A \to B$ is **onto** $B$ if each element of $B$ is the image of at least one element of $A$.

**In symbols.** For every $b \in B$ there exists $a \in A$ with $\varphi(a) = b$.

**Picture.** Every element of $B$ is hit.

**How it is proved.** Take an arbitrary $b \in B$ and **construct** an $a \in A$ with $\varphi(a) = b$.

**Onto depends on $B$.** The map $x \mapsto x^2$ from $\mathbb{Z}$ to $\mathbb{Z}$ is not onto; from $\mathbb{Z}$ to $\{0,1,4,9, \dots\}$ it is.

# Properties of Functions (Theorem 0.8)

**THEOREM 0.8.** Given $\alpha: A \to B$, $\beta: B \to C$, $\gamma: C \to D$:

1. **Associativity:** $\gamma(\beta\alpha) = (\gamma\beta)\alpha$
2. If $\alpha$ and $\beta$ are one-to-one, then $\beta\alpha$ is one-to-one
3. If $\alpha$ and $\beta$ are onto, then $\beta\alpha$ is onto
4. If $\alpha$ is one-to-one and onto, then there is a function $\alpha^{-1}: B \to A$, onto $A$, with
5. $\left(\alpha^{-1}\alpha\right)(a) = a \ \ \forall a \in A, \qquad \left(\alpha\alpha^{-1}\right)(b) = b \ \ \forall b \in B$

**Converses fail.** $\beta\alpha$ one-to-one forces $\alpha$ one-to-one, but not $\beta$.

# Function Inverses

**When does $\alpha^{-1}$ exist?** Exactly when $\alpha: A \to B$ is both one-to-one and onto.

**Why both are needed.**

- **One-to-one** makes $\alpha^{-1}$ single valued (well defined).
- **Onto** makes $\alpha^{-1}$ defined on all of $B$.

**Defining property.** If $\alpha(s) = t$ then $\alpha^{-1}(t) = s$; equivalently

$$\left(\alpha^{-1}\alpha\right)(a) = a \ \ \forall a \in A, \qquad \left(\alpha\alpha^{-1}\right)(b) = b \ \ \forall b \in B.$$

$\alpha^{-1}$ undoes what $\alpha$ does.

# Example 24 — In Class: Fill In the Last Two Columns

$\mathbb{Z}$ = integers, $\mathbb{R}$ = reals, $\mathbb{N}$ = nonnegative integers.

| Rule | Domain | Codomain | One-to-one? | Onto? |
|---|---|---|---|---|
| $x^3$ | $\mathbb{Z}$ | $\mathbb{Z}$ | | |
| $x^3$ | $\mathbb{R}$ | $\mathbb{R}$ | | |
| $\lvert x \rvert$ | $\mathbb{Z}$ | $\mathbb{N}$ | | |
| $x^2$ | $\mathbb{Z}$ | $\mathbb{Z}$ | | |

Same rule, different domain or range — different answer.

# Example 24 — **ANSWERS**

| Rule | Domain | Codomain | One-to-one? | Onto? |
|---|---|---|---|---|
| $x^3$ | $\mathbb{Z}$ | $\mathbb{Z}$ | **Yes** | **No** |
| $x^3$ | $\mathbb{R}$ | $\mathbb{R}$ | **Yes** | **Yes** |
| $\lvert x \rvert$ | $\mathbb{Z}$ | $\mathbb{N}$ | **No** | **Yes** |
| $x^2$ | $\mathbb{Z}$ | $\mathbb{Z}$ | **No** | **No** |

**Rows 1-2:** $x^3 = y^3 \Rightarrow x = y$ by cube roots, so both are one-to-one. Row 1 is not onto (2 is no integer's cube); row 2 is onto (every real $b$ equals $\left(\sqrt[3]{b}\right)^3$).
**Row 3:** $|-1| = |1|$, not one-to-one; every $n \in \mathbb{N}$ is $|n|$, so onto.
**Row 4:** $(-1)^2 = 1^2$, not one-to-one; $-1$ is not a square, not onto.