Math 343 Group Theory

TEXTBOOK

Contemporary Abstract Algebra,. 10th Edition. Joseph A. Gallian

CH0 Preliminaries: Properties of Integers and Foundations

Well Ordering Principle

Axiom (Well Ordering Principle)

Every nonempty set of positive integers contains a smallest member.

Key Point: This property cannot be proved from usual arithmetic properties—we take it as an axiom.

Why Important: Foundation for mathematical induction and many fundamental theorems in number theory.

Divisibility

Definition: A nonzero integer t is a **divisor** of an integer s if there exists an integer u such that $s = tu$.

Notation:

- $t|s$ means "t divides s"
- $t \nmid s$ means "t does not divide s"

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

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

The Division Algorithm

Theorem (Division Algorithm)

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that:

$$a = bq + r, \quad \text{where } 0 \leq r < b$$

Terminology:

- q = quotient upon dividing a by b
- r = remainder upon dividing a by b

Examples of Division Algorithm

Example 1:

- For $a = 17$ and $b = 5$: $17 = 5 \cdot 3 + 2$
- For $a = -23$ and $b = 6$: $-23 = 6(-4) + 1$

Strategy for Divisibility Proofs:

To show b divides a, write $a = bq + r$ where $0 \leq r < b$, then use properties of a and b to show $r = 0$.

Greatest Common Divisor

Definition: The **greatest common divisor** of nonzero integers a and b is the largest of all common divisors of a and b.

Notation: $\gcd(a, b)$

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

GCD as Linear Combination

Theorem: For any nonzero integers a and b, there exist integers s and t such that:
$\gcd(a, b) = as + bt$

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

Corollary: Relatively Prime Characterization

Corollary: Integers a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.

Examples:

- $\gcd(4, 15) = 1$; $\gcd(4, 10) = 2$
- $\gcd(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$
- $4 \cdot 4 + 15(-1) = 1$
- $4(-2) + 10 \cdot 1 = 2$

Application: Polynomial Expressions

Example: For any integer n, the integers $n+1$ and n^2+n+1 are relatively prime.

Proof: We need to show $\mathbf{gcd}(n+1, n^2+n+1) = 1$.

Observe that:

$n^2+n+1-n(n+1) = n^2+n+1-n^2-n = 1$

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

By our corollary, $n+1$ and n^2+n+1 are relatively prime.

Euclid's Lemma

Lemma (Euclid's Lemma): If p is a prime that divides ab, then p divides a or p divides b.

Proof: Suppose $p|ab$ but $p \nmid a$.
Since p is prime and $p \nmid a$, we have $\gcd(p, a) = 1$.
By our corollary, there exist integers s and t such that $1 = as + pt$.
Multiplying by b: $b = abs + ptb$.
Since $p|ab$, we have $p|abs$.
Since $p|pt$, we have $p|ptb$.
Therefore $p|(abs + ptb) = b$.

Note: This fails when p is not prime: $6|(4 \cdot 3)$ but $6 \nmid 4$ and $6 \nmid 3$.

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic):
Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear.

That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ where the p_i's and q_j's are primes, then $r = s$ and after renumbering, $p_i = q_i$ for all i.

Key Point: Primes are the "building blocks" for all integers.

Application: Irrationality Proof

Example: For any integer $n > 1$, $\sqrt[n]{2}$ is irrational.

Proof: Suppose $\sqrt[n]{2} = a/b$ where a/b is in lowest terms.
Then $2 = a^n/b^n$, so $2b^n = a^n$.
By Fundamental Theorem, $2|a^n$, so $2|a$ (since 2 is prime).
Write $a = 2c$. Then $2b^n = (2c)^n = 2^n c^n$.
So $b^n = 2^{n-1} c^n$.
This implies $2|b^n$, so $2|b$.
But then $\gcd(a, b) \geq 2$, contradicting that a/b is in lowest terms.

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 a and b.

Notation: $\mathrm{lcm}(a, b)$

Examples:

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

Introduction to Modular Arithmetic

Motivation: How do we count cyclically?

- If it's September, what month will it be 25 months from now?
- Answer: October (since $25 = 2 \cdot 12 + 1$)
- If it's Wednesday, what day will it be in 23 days?
- Answer: Friday (since $23 = 7 \cdot 3 + 2$)

Key Insight: We don't count sequentially—we use remainders!

Modular Arithmetic Notation

Definition: When $a = qn + r$ where q is quotient and r is remainder upon dividing a by n, we write:

$a \bmod n = r$

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 $-2 = (-1) \cdot 15 + 13$

Key Property of Modular Arithmetic

Important Fact: $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

Computing Tip: When computing $(ab) \bmod n$ or $(a + b) \bmod n$, it's easier to "mod first."

Example: To compute $(27 \cdot 36) \bmod 11$:

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

Application: Check Digits

US Postal Service Money Orders:

- 10-digit identification number plus check digit
- Check digit = (10-digit number) mod 9
- Example: 3953988164 has check digit 2 since $\mathbf{3953988164 \bmod 9 = 2}$

Error Detection:

If 39539881642 is incorrectly entered as 39559881642, computer calculates check digit as 4, but entered check digit is 2 → Error detected!

Mathematical Induction: First Principle

Theorem (First Principle of Mathematical Induction):
Let S be a set of integers containing a. Suppose S has the property that whenever some 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.

Proof Strategy:

1. **Base Case:** Verify statement for $n = a$
2. **Inductive Step:** Assume true for n, prove true for $n + 1$

Second Principle of Mathematical Induction

Theorem (Second Principle/Strong Induction):
Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then S contains every integer greater than or equal to a.

When to Use: When proving statement for n requires knowing it's true for multiple previous values, not just $n - 1$.

Equivalence Relations

Motivation: In different contexts, different objects may be considered "the same":

- $2 + 1$ and 4 + 4 are different in arithmetic, same $mod\ 5$
- Congruent triangles in different positions
- Vectors with same magnitude and direction

Need: Formal mechanism to specify when objects are "equivalent"

Definition of Equivalence Relation

Definition: An equivalence relation on set S is a set R of ordered pairs 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 $a \sim b$ instead of $(a, b) \in R$

Equivalence Class: $[a] = \{x \in S \mid x \sim a\}$

Examples of Equivalence Relations

Example 1: Similar triangles

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

Example 2: Polynomials with same derivative

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

Modular Congruence

Example 3: Congruence modulo n

- S = integers, n = positive integer
- $a \equiv b \pmod{n}$ if $n|(a-b)$

Verification:

- **Reflexive:** $a \equiv a \pmod{n}$ since $n|(a-a) = n|0$ ✓
- **Symmetric:** If $a \equiv b \pmod{n}$, then $n|(a-b)$, so $n|(b-a)$, thus $b \equiv a \pmod{n}$ ✓
- **Transitive:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $n|(a-b)$ and $n|(b-c)$, so $n|((a-b)+(b-c)) = n|(a-c)$, thus $a \equiv c \pmod{n}$ ✓

Equivalence Classes: $[a] = \{a + kn \mid k \in \mathbb{Z}\}$

Rational Numbers as Equivalence Classes

Example 4: Fraction equivalence

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

Verification:

- **Reflexive:** $(a,b) \sim (a,b)$ since $ab = ba$ ✓
- **Symmetric:** If $(a,b) \sim (c,d)$, then $ad = bc$, so $cb = da$, thus $(c,d) \sim (a,b)$ ✓
- **Transitive:** If $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$, then $ad = bc$ and $cf = de$. Multiplying: $adf = bcf = bde$. Since $d \neq 0$, we get $af = be$, so $(a,b) \sim (e,f)$ ✓

Interpretation: (a,b) represents fraction a/b

Definition: Partition

Definition: A **partition** of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Examples of Partitions

Example 21: The sets $\{0\}$, $\{1, 2, 3, \ldots\}$, and $\{\ldots, -3, -2, -1\}$ constitute a partition of the set of integers.

Example 22: The set of nonnegative integers and the set of nonpositive integers do **NOT** partition the integers, since both contain 0.

Key Point: Partition subsets must be **disjoint** (no overlapping elements).

Equivalence Classes Form Partitions

Theorem 0.7 (Equivalence Classes Partition)
The equivalence classes of an equivalence relation on a set S constitute a partition of S.

Conversely: For any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

Big Picture: Equivalence relations and partitions are two ways of describing the same mathematical structure!

Proof Strategy

To show equivalence classes partition S:

1. **Non-empty:** Each $[a]$ is non-empty (reflexive property: $a \in [a]$)
2. **Union is S:** Every element belongs to some equivalence class
3. **Disjoint:** If $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$

Key Insight: If $c \in [a] \cap [b]$, then $c \sim a$ and $c \sim b$, which forces $[a] = [b]$ by transitivity.

Functions (Mappings)

Definition: A **function** (or **mapping**) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B.

Notation: $\phi : A \to B$

Terminology:

- A = **domain** of ϕ
- B = **range** of ϕ
- $\phi(a) = b$ means "b is the **image** of a under ϕ"

Function Well-Definedness

Important Issue: When elements have multiple representations, must verify function is **well-defined**.

Bad Example: $\phi(a/b) = a + b$ on rational numbers

- $\phi(1/2) = 1 + 2 = 3$
- $\phi(2/4) = 2 + 4 = 6$
- But $1/2 = 2/4$, so this is **not** a function!

Test: If $x_1 = x_2$, then $\phi(x_1) = \phi(x_2)$ must hold.

Composition of Functions

Definition: Let $\phi : A \to B$ and $\psi : B \to C$. The **composition** $\psi\phi$ is the mapping from A to C defined by:
$(\psi\phi)(a) = \psi(\phi(a))$ for all $a \in A$

Note: We write $\psi\phi$ instead of $\psi \circ \phi$ (no circle).

Composition Example

Example 23: Let $f(x) = 2x + 3$ and $g(x) = x^2 + 1$.

Specific Values:

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

General Forms:

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

Key Point: $fg \neq gf$ in general!

One-to-One Functions

Definition: A function $\phi : A \to B$ is **one-to-one** if: $\phi(a_1) = \phi(a_2) \implies a_1 = a_2$

Alternative: Different inputs give different outputs: $a_1 \neq a_2 \implies \phi(a_1) \neq \phi(a_2)$

Visual Interpretation: Each element of B can be the image of **at most one** element of A.

Onto Functions

Definition: A function $\phi : A \to B$ is **onto** B if each element of B is the image of at least one element of A.

In Symbols: For each $b \in B$, there exists $a \in A$ such that $\phi(a) = b$.

Visual Interpretation: Every element of B is "hit" by some element from A.

Properties of Functions

Theorem 0.8: Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$:

1. **Associativity:** $\gamma(\beta\alpha) = (\gamma\beta)\alpha$
2. **One-to-one preserved:** If α and β are one-to-one, then $\beta\alpha$ is one-to-one
3. **Onto preserved:** If α and β are onto, then $\beta\alpha$ is onto
4. **Inverses exist:** If α is one-to-one and onto, then α^{-1} exists

Function Inverses

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

Properties of α^{-1}:

- $(\alpha^{-1}\alpha)(a) = a$ for all $a \in A$
- $(\alpha\alpha^{-1})(b) = b$ for all $b \in B$

Key Insight: If $\alpha(s) = t$, then $\alpha^{-1}(t) = s$

α^{-1} "undoes" what α does!

Function Properties: Examples

Example 24: Let $\mathbb{Z}$ = integers, $\mathbb{R}$ = real numbers, $\mathbb{N}$ = nonnegative integers.

Domain	Range	Rule	One-to-One	Onto
$\mathbb{Z}$	$\mathbb{Z}$	$x \mapsto x^3$		
$\mathbb{R}$	$\mathbb{R}$	$x \mapsto x^3$		
$\mathbb{Z}$	$\mathbb{Z}$	$x \mapsto \lvert x \rvert$		
$\mathbb{N}$	$\mathbb{Z}$	$x \mapsto x^2$		