Introduction to Abstract Algebra

UT Knoxville, Fall 2023, MATH 351

David White, Alex Zhang

October 8, 2023

Contents

1 Introduction

TODO: Pentagon rotation and mirroring example

1.1 Relations

Definition 1.1.1 ▸ Relation

Let A and B be sets.

- A ***relation*** from A to B is a subset of the Cartesian product $A \times B$.
- A ***relation*** on A is a subset of the Cartesian product $A \times A$.

Given a relation ρ, we denote $(a, b) \in \rho$ as $a \mathrel{\rho} b$. If $(a, b) \notin \rho$, we write $a \not\rho\, b$.

Definition 1.1.2 ▸ Reflexive, symmetric, transitive, equivalence relation

Let ρ be a relation on a set A.

- ρ is ***reflexive*** if, for any $a \in A$, $a \mathrel{\rho} a$.
- ρ is ***symmetric*** if $a \mathrel{\rho} b$ implies $b \mathrel{\rho} a$.
- ρ is ***transitive*** if, whenever $a \mathrel{\rho} b$ and $b \mathrel{\rho} c$, we have $a \mathrel{\rho} c$.

If ρ satisfies all three properties, it is called an ***equivalence relation***. We often use $\sim$ to denote an equivalence relation.

Definition 1.1.3 ▸ Equivalence class

Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The ***equivalence class*** of a is a set defined as:

$$[a] \coloneqq \{b \in A \,:\, a \sim b\}$$

1.2 Functions

Definition 1.2.1 ▸ Function

Let X and Y be sets. A ***function*** from X to Y is a relation f from X to Y such that, for each $x \in X$, there exists exactly one $y \in Y$ where $x \ f \ y$. We write $f : X \to Y$ to mean f is a function from X to Y, and we write $f(x) = y$ to mean $x \ f \ y$.

Definition 1.2.2 ▸ Injective, surjective, bijective

Let $f : X \to Y$ be a function.

- f is ***injective*** if, for all x_1 and x_2 where $x_1 \neq x_2$, we have $f(x_1) \neq f(x_2)$.
- f is ***surjective*** if, for all $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- f is ***bijective*** if it is both injective and surjective.

Definition 1.2.3 ▸ Permutation

A ***permutation*** of a set A is a function from A to A.

Definition 1.2.4 ▸ Binary operation

A ***binary operation*** on a set A is a function from $A \times A$ to A.

Wowzers

2 The Integers and Modular Arithmetic

Theorem 2.0.1 ▸ Well Ordering Axiom

If S is a nonempty subset of $\mathbb{N}$, then S has a minimum value.

Theorem 2.0.2 ▸ Principle of Mathematical Induction

For each $n \in \mathbb{N}$, let $P(n)$ denote a statement. Suppose that:

1. $P(1)$ is true, and
2. for each $n \in \mathbb{N}$, if $P(n)$ is true, then $P(n+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

2.1 Divisibility

Theorem 2.1.1 ▸ Division Algorithm

TODO: division algorithm

Definition 2.1.2 ▸ Divides

Let $a, b \in \mathbb{Z}$. We say a ***divides*** b if there exists an integer k such that $b = ka$. We write $a \mid b$ to mean a divides b.

Definition 2.1.3 ▸ Greatest common divisor (GCD)

Let $a, b \in \mathbb{Z}$ where at least one is non-zero. The ***greatest common divisor (GCD)*** of a and b is the largest positive integer g such that $g \mid a$ and $g \mid b$. We write $\gcd(a, b)$ or simply (a, b) to denote the greatest common divisor of a and b.

Definition 2.1.4 ▸ Relatively prime, coprime

Let $a, b \in \mathbb{Z}$, where at least one is non-zero. We say a and b are ***relatively prime*** (or ***coprime***) if $\gcd(a, b) = 1$.

Theorem 2.1.5

Let $a, b \in \mathbb{Z}$, where at least one is non-zero. Then there exist $u, v \in \mathbb{Z}$ where $\gcd(a, b) = au + bv$. Moreover, $\gcd(a, b)$ is the smallest possible number of all values of u and v.

Theorem 2.1.6 ▸ Euclidean Algorithm

TODO

2.2 Prime Factorization

Definition 2.2.1 ▸ Prime, composite

A natural number $p > 1$ is ***prime*** if its only positive divisors are 1 and p itself. Otherwise, p is ***composite***.

Theorem 2.2.2 ▸ Euclid's Lemma

Let $p \in \mathbb{N}$ where $p > 1$. p is prime if and only if, for any integers a and b where $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem 2.2.3 ▸ Fundamental Theorem of Arithmetic

For every natural number a greater than 1, there exists a unique set of primes $\{p_1, \ldots, p_n\}$ such that $a = p_1 \cdots p_n$.

2.3 Properties of Integers

2.4 Modular Arithmetic

Definition 2.4.1 ▸ Modular congruency

Let $n \in \mathbb{N}$ where $n > 1$, and let $a, b \in \mathbb{Z}$. We say a is ***congruent*** to b ***modulo*** n if $n \mid (a-b)$ (that is, if a and b have the same remainder when divided by n). We write $a \equiv b \pmod{n}$ to mean a is congruent to b modulo n.

Theorem 2.4.2

Let $n \in \mathbb{N}$ where $n > 1$. Then $a \equiv b \pmod{n}$ is an equivalence relation.

The equivalence classes of $a \equiv b \pmod{n}$ are conventionally written as:

$$[0], [1], \ldots, [n-1]$$

These are called the ***congruence classes modulo*** n, where:

$$\mathbb{Z}_n \coloneqq \{[0], [1], \ldots, [n-1]\}$$

On $\mathbb{Z}_n$, we define addition modulo n and multiplication modulo n as:

$$[a] + [b] = [a+b]$$
$$[a] \cdot [b] = [ab]$$

For example, in $\mathbb{Z}_7$, we have $[5] + [6] = [4]$. We will often shorten this as $5 + 6 = 4$ when the context is clear.

Theorem 2.4.3

Addition modulo n and multiplication modulo n are well-defined.

Proof. Fix $n \in \mathbb{N}$ where $n > 1$. Suppose $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. To prove addition modulo n is well-defined, we need to verify the following equality:

$$[a_1] + [b_1] = [a_2] + [b_2]$$

Note that:

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

Since $n \mid (a_1 - a_2)$ and $n \mid (b_1 - b_2)$, we have $n \mid [(a_1 + b_1) - (a_2 + b_2)]$, so addition is well-defined.
To prove multiplication is well-defined, we need to verify the following equality:

$$[a_1][b_1] = [a_2][b_2]$$

Note that:

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

So multiplication modulo n is also well-defined □

These operations follow similar properties as traditional integer addition and multiplication. Addition in $\mathbb{Z}_n$ is closed, associative, commutative, and has additive identity $[0]$ and additive inverse $[-a]$ for any $a \in \mathbb{Z}_n$.

Multiplication in $\mathbb{Z}_n$ is closed, associative, commutative, distributive, and has multiplicative identity $[1]$. However, not every $\mathbb{Z}_n$ has a multiplicative inverse for all elements.

Example 2.4.4 ▸ Multiplicative inverse in $\mathbb{Z}_n$

In $\mathbb{Z}_6$, does $ab = 0$ mean that $a = 0$ or $b = 0$? Not necessarily: $a = 3$ and $b = 2$ is a counterexample.
In $\mathbb{Z}_7$, does $ab = 0$ mean $a = 0$ or $b = 0$? For any $a \in \mathbb{Z}_7$ where $a \neq 0$, note that $\gcd(a, 7) = 1$. Thus, there exist $u, v \in \mathbb{Z}$ where $au + 7v = 1$. Rearranging, we get $7v = 1 - au$, so $7 \mid (au - 1)$. That means $[a][u] = [1]$, so u is the multiplicative inverse of a. Since our choice of a was arbitrary, then every element in $\mathbb{Z}_7$ has a multiplicative inverse.

Example 2.4.5

In $\mathbb{Z}_5$, what is 4^{91}?

$$\begin{aligned} 4^1 &= 4 \\ 4^2 &= 1 \\ 4^3 &= 4 \\ 4^4 &= 1 \\ &\vdots \\ 4^{91} &= 4 \end{aligned}$$

$3^1 = 3, 3^2 = 4, 3^2 = 2, 3^4 = 1$, so $3^{91} = (3^4)^{22} \cdot 3^3 = 2$.

Example 2.4.6

Find b satisfying:

$$\begin{aligned} b &\equiv 3 \pmod{5} \\ b &\equiv 4 \pmod{11} \\ b &\equiv 6 \pmod{14} \end{aligned}$$

Note that 5 and 11 are relatively prime, so there exist $u, v \in \mathbb{Z}$ where $5u + 11v = 1$. In this case, we can take $u = -2$ and $v = 1$. Note that:

$$\begin{aligned} 5(-2)4 + 11(1)3 &\equiv 3 \pmod{5} \\ 5(-2)4 + 11(1)3 &\equiv 4 \pmod{11} \end{aligned}$$

More generally, we can take $b = -7 + 55k$ for any $k \in \mathbb{Z}$.

Alternatively, we can let:

$$\begin{aligned} d_1 &:= 11 \cdot 14 = 154 \\ d_2 &:= 5 \cdot 14 = 70 \\ d_3 &:= 5 \cdot 11 = 55 \end{aligned}$$

Note that $\gcd(5, 154) = 1$, so:

$$5(31) + 154(-1) = 1 \implies 5 \cdot 31 \equiv 1 \pmod{5}$$

$$11(-19) + 70(3) = 1 \implies 70 \cdot 3 \equiv 1 \pmod{11}$$

$$14(4) + 55(-1) = 1 \implies 55(-1) \equiv 1 \pmod{14}$$

Let $b := 154(-1)(3) + 70(3)4 + 55(-1)6$. Then:

$$b \pmod{5} = 154(-1)(3) = 3$$

$$b \pmod{11} = 4$$

$$b \pmod{14} = 6$$

Theorem 2.4.7 ▸ Chinese Remainder Theorem

Let $n_1, \dots, n_k$ be positive integers, all greater than 1, where any two different n_i and n_j are relatively prime. If $a_1, \dots, a_n \in \mathbb{Z}$, we can find $b \in \mathbb{Z}$ satisfying $b \equiv a_i \pmod{n_i}$ for all $1 \leq i \leq k$. Moreover, if $c \equiv a_i \pmod{n_i}$, then $b \equiv c \pmod{n_1 n_2 \cdots n_k}$.

3

Introduction to Groups

3.1 The Basics

Definition 3.1.1 ▶ Group

A ***group*** is a set G together with a binary operation $*$ satisfying for any $a, b, c \in G$:

- ***closure*** under $*$, meaning $a * b \in G$;
- ***associativity*** under $*$, meaning $(a * b) * c = a * (b * c)$;
- existence of an ***identity element*** $e \in G$ satisfying $e * a = a * e$; and
- existence of an ***inverse*** for a, say $a^{-1} \in G$ where $a * a^{-1} = a^{-1} * a = e$.

A group is ***abelian*** if it is commutative under $*$, meaning $a * b = b * a$ for any $a, b \in G$.

Some examples of groups include $\mathbb{Z}$ under addition, $\mathbb{Z}_n$ where $n \geq 2$ under addition, and D_{10} under $\circ$, the dihedral group of the regular pentagon, often called D_5. (TODO: pentagon example)

Theorem 3.1.2 ▶ Uniqueness of identities and inverses

Let G be a group.

1. The identity of G is unique (that is, there is only one identity element in G).
2. For any $a \in G$, its inverse a^{-1} is unique.

Proof of 1. Let e and f be identity elements in G Then $ef = e$ because f is an identity, and $ef = f$ because e is an identity. Thus, $e = f$. ▢

Proof of 2. Let b and c be inverses of a. Then $bac = (ba)c = ec = c$, and $bac = b(ac) = be = b$. Thus, $b = c$. ▢

Theorem 3.1.3 ▶ Cancellation

Let G be a group, and let $a, b, c \in G$. If $ab = ac$ or $ba = ca$, then $b = c$.

Proof sketch. If $ab = ac$, then $a^{-1}(ab) = a^{-1}(ac)$ … so $b = c$. ▢

Theorem 3.1.4

Let G be a group, and let $a, b \in G$. Then there is a unique $c \in G$ satisfying $ac = b$, and there is a unique $d \in G$ satisfying $da = b$.

Intuition: $c = a^{-1}b$ and $d = ba^1$.

Definition 3.1.5 ▶ Permutation

A ***permutation*** on a set A is an injective function $\sigma : A \to A$, written as:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

to mean $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c$.

Since these are functions, we can compose two or more permutations.

Permutation example, composition example

The set of permutations, under function composition, is a ***group***.

- Closed
- Associativity
- Existence of an identity element e where $e \circ \sigma = \sigma \circ e$ for all σ. In this case, e is simply the identity function.
- Existence of an inverse for each σ. That is, for any σ, there exists τ where $\sigma \circ \tau = \tau \circ \sigma = e$.

Definition 3.1.6 ▶ Symmetric group (S_n)

The set of permutations on 3 elements under function composition is called S_3, the ***symmetric group*** on 3 elements.

Let $n \geq 2$. Let $U(n)$ denote the set of all $a \in \mathbb{Z}_n$ where $\gcd(a, n) = 1$, under the multiplication modulo n.

Definition 3.1.7 ▶ Direct product

Let G be a group with operation $*$, and let H be a group with operation $\cdot$. On the Cartesian product $G \times H$, define the operation $\diamond$ by:

$$(g_1, h_1) \diamond (g_2, h_2) \coloneqq (g_1 * g_2, h_1 \cdot h_2)$$

for all $g_i \in G, h_i \in H$. We call this the ***direct product*** of G and H.

Theorem 3.1.8 ▶ Direct product is always a group

The direct product of any two groups is itself a group.

Example 3.1.9 ▶ Simple direct product

Consider the direct product $\mathbb{Z}_3 \times S_3$.

- How many elements are in the direct product?
- What is the identity element?
- What is the inverse of $\left(2, \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)\right)$?

- There are 3 elements in $\mathbb{Z}_3$ and 6 elements in S_3, so there are a total of 18 elements in the direct product.
- The identity element is $\left(0, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right)$
- The inverse of $\left(2, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right)$ is $\left(1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right)$

matrix size

3.2 Order

Integer powers

In groups under an addition operation such as $\mathbb{Z}_{15}$, we write $7 \cdot 2$ instead of 2^7 to avoid ambiguity with the notation for integer powers.

Theorem 3.2.1 ▶ Properties of power

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Definition 3.2.2 ▶ Order

Let G be a group under operation $\cdot$.

- The ***order*** of G (denoted $|G|$) is the number of elements in G. G is ***finite*** if its order is finite; otherwise, it's an ***infinite*** group.
- The ***order*** of an element $a \in G$ (denoted $|a|$) is the smallest positive integer where:

$$\underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}} = e \quad (\text{the identity element of } G)$$

If such an n exists, a has ***finite order***; otherwise, a has ***infinite order***.

In any group, the identity element is the only element that has order 1.

Example 3.2.3 ▶ Order of common groups

- $|Z| = \infty$
- $|Z_{15}| = 15$
- $|D_{10}| = 10$
- $|S_5| = 5!$
- $|D_6 \times S_4| = 6 \cdot 4!$

Example 3.2.4 ▶ Order of elements in common groups

- Order of $2 \in Z_4$ is 2 because $2 + 2 = 0 = e$
- Order of $3 \in U(8)$ is 3 because $3^2 = 1 = e$
- Order of $\sigma := \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right) \in S_3$ is 3 because $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$

Theorem 3.2.5 ▶ Properties of order

Let G be a group, and let $a \in G$.

1. If a has infinite order, then $a^i = a^j$ if and only if $i = j$.
2. If a has order $n \in \mathbb{Z}^+$, then $a^i = a^j$ if and only if $n \mid (i - j)$.

Proof sketch. Consider i and j where $a^{i-j} = e$.

1. If a has infinite order, then $i - j = 0$.
2. If a has finite order, write $i - j = nq + r$ for $0 \leq r < n$ (by the division algorithm TODO: REF). Then:

$$a^{i-j} = (a^n)^q a^r = e$$

So $a^r = e$. But $r < n$, and n is the smallest positive integer satisfying $a^n = e$. Thus, $r = 0$.

$\square$

Corollary 3.2.6

Let G be a group, and let $a \in G$ where $|a| = n \in \mathbb{Z}^+$. Then $a^i = e$ if and only if $n \mid i$.

Example 3.2.7

Show that ab and ba have the same order.

Suppose $(ab)^n = e$. Then:

$$\begin{aligned}(ba)^n &= \underbrace{baba \cdots ba}_{n \text{ times}} \\ &= b(ab)^{n-1}a\end{aligned}$$

So $(ba)^n b = b(ab)^{n-1}ab = b(ab)^n = b$. Thus, $(ba)^n = e$. Thus, $n \mid |ba|$, or $|ab| \mid |ba|$.

3.3 Cyclic Groups

Definition 3.3.1 ▸ Cyclic

A group G is ***cyclic*** if there exists $a \in G$ where, for any $b \in G$:

$$b = a^n \quad \text{for some } n \in \mathbb{Z}$$

In other words, G is cyclic if there exists $a \in G$ where any element of G is a power of a. In this context, we say a is a ***generator*** of G and write $G = \langle a \rangle$, where:

$$\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$$

For example, $\mathbb{Z}$ under addition is a cyclic group. For any $n \in \mathbb{Z}$, we have:

$$1 \cdot n = n$$

Note here that $1 \cdot n$ reflects the idea of integer powers under addition. We apply the group operation of addition n-times. For example:

$$5 = 1^5 = 1 \cdot 51 + 1 + 1 + 1 + 1$$
$$-2 = 1^{-2} = 1 \cdot (-2) = -(1 + 1)$$

When dealing with additive operations, we usually omit the exponent notation and simply write the multiplicative expression. Note also that $\mathbb{Z}$ can be generated by -1. Thus, the generator of a cyclic group is not guaranteed to be unique.

Another example, in $\mathbb{Z}_{12}$, we have:

$$\langle 1 \rangle = \{0, 1, 2, \dots, 10, 11\}$$

$$\langle 4 \rangle = \{0, 4, 8\}$$

In fact, this $\langle 4 \rangle$ is itself a group under addition modulo 12.

Theorem 3.3.2 ▸ Every cyclic group is abelian

Let G be a group. If G is cyclic, then it is abelian.

3.4 Subgroups

Definition 3.4.1 ▸ Subgroup

Let G be a group under an operation $*$. Then a subset $H \subseteq G$ is considered a ***subgroup*** of G if H itself also a group under $*$. H is called a ***proper subgroup*** of G if $H \subsetneq G$.

Trivially, every group is a subgroup of itself. Also, $\{e\}$ is a subgroup of every group. More substantially, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, and $\mathbb{Q}$ is a subgroup of $\mathbb{R}$. This is sometimes written as $\mathbb{Z} \leq \mathbb{Q}$, and $\mathbb{Q} \leq \mathbb{R}$.

Theorem 3.4.2 ▸ Conditions for subgroup

Let G be a group under operation $*$, and let $H \subseteq G$. Then H is a subgroup of G if and only if:

1. $e \in H$ (the subset contains the identity);
2. for any $a, b \in H$, $a * b \in H$ (the subset is closed under $*$); and
3. for any $a \in H$, $a^{-1} \in H$ (the subset contains all inverses).

Example 3.4.3 ▶ Determining $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$

Consider the following set:

$$3\mathbb{Z} := \{3x : x \in \mathbb{Z}\}$$

We have:

1. $0 \in 3\mathbb{Z}$
2. For any $a, b \in 3\mathbb{Z}$, $a = 3m$ and $b = 3n$ for some $m, n \in \mathbb{Z}$. Thus, $a + b = 3m + 3n = 3(m + n) \in 3\mathbb{Z}$.
3. For any $a \in 3\mathbb{Z}$, $a^{-1} = -a = 3(-m)$.

Thus, we can confirm that $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Note that in the above example, we can also write:

$$3\mathbb{Z} := \langle 3 \rangle = \{3x : x \in \mathbb{Z}\}$$

Definition 3.4.4 ▶ Cyclic subgroup

Let G be a group, and let $a \in G$. The ***cyclic subgroup*** generated by a is defined as:

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$$

For example, in $\mathbb{Z}_{12}$, we have:

$$\begin{aligned}
\langle 0 \rangle &= \{0\} \\
\langle 1 \rangle &= \mathbb{Z}_{12} \\
\langle 2 \rangle &= \{0, 2, 4, 6, 8, 10\} \\
\langle 3 \rangle &= \{0, 3, 6, 9\} \\
\langle 4 \rangle &= \{0, 4, 8\} \\
\langle 5 \rangle &= \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12} \\
\langle 6 \rangle &= \{0, 6\} \\
\langle 7 \rangle &= \ldots = \mathbb{Z}_{12} \\
\langle 8 \rangle &= \{0, 8, 4\} \\
\langle 9 \rangle &= \{0, 9, 6, 3\} \\
\langle 10 \rangle &= \{0, 10, 8, 6, 4, 2\} = \langle 2 \rangle \\
\langle 11 \rangle &= \ldots = \mathbb{Z}_{12}
\end{aligned}$$

From this, it seems that numbers relatively prime with 12 can generate the entirety of $\mathbb{Z}_{12}$. In fact, if $|a| = n$, then $|a^i| = \frac{n}{\gcd(n,i)}$.

Check this fact!!!

Theorem 3.4.5 ▸ Cyclic subgroups are groups

Let G be a group, and let $a \in G$. $\langle a \rangle$ is a subgroup.

Proof sketch. We simply check the three conditions.

1. $e = a^0$.
2. $a^m a^n = a^{m+n}$
3. if $a^m \in \langle a \rangle$, then $a^{-m} \in \langle a \rangle$.

Thus, $\langle G \rangle$ is a subgroup of G. ▢

Theorem 3.4.6 ▸ Conditions for subgroup relaxed

Let G be a group, and let $H \subseteq G$. Then H is a subgroup G if and only if:

1. $e \in H$, and
2. $ab^{-1} \in H$ for any $a, b \in H$.

Proof sketch. Let $a \in H$. $e \in H$ by (1), so $1 \cdot a^{-1} \in H$.
Let $a, b \in H$. $b^{-1} \in H$ by the first statement, so then $a(b^{-1})^{-1} \in H$, so $ab \in H$. ▢

Theorem 3.4.7 ▸ Conditions for finite subgroup

Let G be a group, and let H be a **finite** subset of G. Then H is a subgroup of G if and only if:

1. $e \in H$, and
2. $ab \in H$ for any $a, b \in H$.

Intuition: This theorem is saying that if we take a finite subset of G, then these two conditions alone imply the existence of inverses, and vice versa. For any $a \in H$, we have:

$$\langle a \rangle = \{e, a, a^2, a^3, \dots\} \subseteq H$$

Since H is finite, then these a's must "wrap around" back to e. For example, we might have $a^5 = a^{17}$, which implies that $e = a^{12} = a(a^{11})$. Thus, the inverse of a is a^{11}.

Crucially, this theorem does not apply for infinite subsets/subgroups.

Definition 3.4.8 ▶ Center

Let G be a group. The ***center*** of G is defined as:

$$Z(G) := \{z \in G : az = za \text{ for all } a \in G\}$$

If G is abelian, then $Z(G) = G$.

TODO: dihedral groups, diagram thing

3.5 Cyclic Groups

Definition 3.5.1 ▶ Cyclic group, generator

A group G is ***cyclic*** if there exists $a \in G$ where every element is a power of a. We say a is a ***generator*** for G and write $G = \langle a \rangle$.

For any group G, we can easily attain a cyclic subgroup by choosing any $a \in G$ and seeing what it generates:

$$\langle a \rangle := \{a^n : n \in Z\}$$

Theorem 3.5.2 ▶ Properties of cyclic groups

For cyclic group G and any $a \in G$:

1. G is abelian.
2. $\langle a \rangle \leq G$ for any $a \in G$.
3. $|a| = |\langle a \rangle|$.
4. Any subgroup of G is also cyclic.
5. If k divides $|a|$, then $\langle a \rangle$ has exactly one subgroup of order k: $\left\langle a^{|a|/k} \right\rangle$.

Definition 3.5.3 ▶ Euler phi-function

The ***Euler phi-function*** is a function $\phi : \mathbb{N} \to \mathbb{N}$ where $\phi(n)$ is the number of integers $1 \leq i \leq n$ where $\gcd(i, n) = 1$.

- $|U(n)| = \phi(n)$
- For $\langle a \rangle$ and k where k divides $|a|$, the number of elements of order k in $\langle a \rangle$ is $\phi(k)$.

Theorem 3.5.4 ▶ Properties of euler phi with primes

For prime number p, and any positive integer m and n:

1. $\phi(p^n) = p^n - p^{n-1}$.
2. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

3.6 Cosets and Lagrange's Theorem

Definition 3.6.1 ▶ Congruence modulo a group

For $H \leq G$ and $a, b \in G$, a is ***congruent to*** b modulo H if $a^{-1}b \in H$. This is written as $a \equiv b \pmod{H}$.

For group G and $H \leq G$:

- Congruence modulo H is an equivalence relation on G.
- For any $g \in G$, its equivalence class $[g]$ is $\{gh : h \in H\}$.

Definition 3.6.2 ▶ Left coset

For $H \leq G$ and any $a \in G$, the ***left coset*** of a with respect to G is set $\{ah : h \in H\}$, written as aH. We also call aH a left coset of H in G.

Theorem 3.6.3 ▶ Left cosets partitioning

or $H \leq G$, the left cosets of H in G partition G.

Definition 3.6.4 ▶ Index

For $H \leq G$, the ***index*** of H in G is the number of distinct left cosets of H in G, written as $[G : H]$.

Theorem 3.6.5 ▶ Lagrange's Theorem

For finite group G and $H \leq G$, $|H|$ divides $|G|$.

Corollary 3.6.6 ▸ Corollaries to Lagrange's Theorem

For finite group G and $H \leq G$:

1. $[G : H] = {}^{|G|}/_{|H|}$.
2. $|a|$ divides $|G|$ for any $a \in G$.
3. Any group of prime order is cyclic.

4

Factor groups and Homomorphisms

4.1 Normal Subgroups

Definition 4.1.1 ▸ Normal subgroup

For $N \leq G$, N is ***normal*** if $gN = Ng$ for any $g \in G$. This is written as $N \trianglelefteq G$.

For example, $G \trianglelefteq G$, and $\{e\} \trianglelefteq G$.

Theorem 4.1.2 ▸ Any subgroup of index 2 is normal

If $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

Theorem 4.1.3 ▸ Equivalent definition of normal subgroup

$H \trianglelefteq G$ if and only if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.

Theorem 4.1.4

For $H \leq G$ and $K \leq G$, let $HK := \{hk : h \in H, k \in K\}$.

1. If H and K are both finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.
2. If $H \trianglelefteq G$ or $K \trianglelefteq G$, then $HK \leq G$.
3. If $H \trianglelefteq G$ and $K \trianglelefteq G$, then $HK \trianglelefteq G$.

4.2 Factor Groups

Definition 4.2.1 ▸ Factor groups

For $N \trianglelefteq G$, the ***factor group*** G/N is the set of all left cosets gN for all $g \in G$, with group operation $(aN)(bN) = (ab)N$.

Theorem 4.2.2 ▸ Properties of factor groups

For any group G and normal subgroup N:

1. G/N is a group of order $[G : N]$.
2. If G is abelian, then G/N is abelian.
3. If G is cyclic, then G/N is cyclic.
4. If g is of finite order, then $|gN|$ divides $|g|$.
5. Subgroups of G/N are of the form H/N, where $H \leq G$ and $N \subseteq H$.
6. $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

Theorem 4.2.3 ▸ Properties of factor groups involving the center

1. If $G/Z(G)$ is cyclic, then G is abelian.
2. $[G : Z(G)]$ cannot be prime.

4.3 Homomorphisms

Definition 4.3.1 ▸ Homomorphism, kernel

For groups G and H, a ***homomorphism*** from G to H is a function $\alpha : G \to H$ where, for all $g_1, g_2 \in G$:

$$\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$$

The ***kernel*** of α is:

$$\ker(\alpha) = \{g \in G : \alpha(g) = e\}$$

Theorem 4.3.2 ▸ Properties of homomorphism

For a homomorphism $\alpha : G \to H$:

1. $\alpha(e) = e$.
2. $\alpha(g^n) = (\alpha(g))^n$ for any $n \in \mathbb{Z}$.
3. If g is of finite order, then $|\alpha(g)|$ divides $|g|$.
4. $\ker(\alpha) \trianglelefteq G$.
5. α is injective if and only if $\ker(\alpha) = \{e\}$.

Theorem 4.3.3 ▶ Properties of homomorphism involving images/preimages

For a homomorphism $\alpha : G \to H$ and $L \subseteq G, M \subseteq H$:

1. If $L \leq G$, then $\alpha[L] \leq H$.
2. If $L \trianglelefteq G$, then $\alpha[L] \trianglelefteq \alpha(G)$.
3. If L is cyclic, then $\alpha[L]$ is cyclic.
4. If L is abelian, then $\alpha[L]$ is abelian.
5. α is surjective if and only if $\alpha[g] = H$.
6. If $M \leq H$, then $\alpha^{-1}[M] \leq G$.
7. If $M \trianglelefteq H$, then $\alpha^{-1}[M] \trianglelefteq G$.

Index

Definitions

Examples

Theorems

Corollarys