Topics in Discrete Mathematics

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 216

1. Algebra
   - Groups
   - Group Isomorphism
   - Subgroups
   - Fermat's Little Theorem

Subsection 1

Groups

Definition of Operation and Notation

Definition (Operation)

An **operation on** a set A is a function whose domain contains $A \times A$.

- Since $A \times A$ is the set of all ordered pairs whose entries are in A, an operation is a function whose input is a pair of elements from A.
- Example: Consider $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(a, b) = |a - b|$. In words, $f(a, b)$ gives the distance between a and b on a number line.
- We rarely write the operation symbol in front of the two elements on which we are operating. Rather, we write the operation symbol between the two elements, i.e., instead of $f(a, b)$, we write $a\ f\ b$.
- Furthermore, we usually do not use a letter to denote an operation. Instead, we use a special symbol such as $+$ or $\otimes$ or $\circ$.
- The symbols $+$ and $\times$ have preset meanings.
- A common symbol for a generic operation is $*$. Thus, instead of writing $f(a, b) = |a - b|$, we could write $a * b = |a - b|$.

Example

- Which of the following are operations on $\mathbb{N} : +, -, \times$ and $\div$?
  - Certainly addition $+$ is an operation defined on $\mathbb{N}$. Although it is more broadly defined on any two rational (or even real or complex numbers), it is a function whose domain includes any pair of natural numbers.
  - Likewise multiplication $\times$ is an operation on $\mathbb{N}$.
  - Furthermore, $-$ is an operation defined on $\mathbb{N}$. Note, however, that the result of $-$ might not be an element of $\mathbb{N}$. For example, $3, 7 \in \mathbb{N}$, but $3 - 7 \notin \mathbb{N}$.
  - Finally, division $\div$ does not define an operation on $\mathbb{N}$ because division by zero is undefined. However, $\div$ is an operation defined on the positive integers.

Properties of Operations I

Definition (Commutative Property)

Let $*$ be an operation on a set A. We say that $*$ is **commutative on** A provided $\forall a, b \in A, a * b = b * a$.

Definition (Closure Property)

Let $*$ be an operation on a set A. We say that $*$ is **closed on** A provided $\forall a, b \in A, a * b \in A$.

- Note that the definition of an operation does not require that the result of $*$ be an element of the set A. So, for example, $-$ is an operation defined on $\mathbb{N}$, but it is not closed on $\mathbb{N}$.

Definition (Associative property)

Let $*$ be an operation on a set A. We say that $*$ is **associative on** A provided $\forall a, b, c \in A, (a * b) * c = a * (b * c)$.

Properties of Operations II

- For example, the operations $+$ and $\times$ on $\mathbb{Z}$ are associative, but $-$ is not: $(3-4)-7 = -8$, but $3-(4-7)=6$.

Definition (Identity Element)

Let $*$ be an operation on a set A. An element $e \in A$ is called an **identity element** (or **identity** for short) **for** $*$ provided $\forall a \in A, a * e = e * a = a$.

- For example, 0 is an identity element for $+$, and 1 is an identity element for $\times$. An identity element for $\circ$ on S_n is the identity permutation ι.
- Not all operations have identity elements, e.g., subtraction of integers does not have an identity element.

Uniqueness of Identities

Proposition (Uniqueness of Identities)

Let $*$ be an operation defined on a set A. Then $*$ can have at most one identity element.

- Suppose there are two identity elements, e and e', in A with $e \neq e'$. Consider $e * e'$.
  - On the one hand, since e is an identity element, $e * e' = e'$.
  - On the other hand, since e' is an identity element, $e * e' = e$.

  Thus we have shown $e' = e * e' = e$, a contradiction to $e \neq e'$.

Inverses

Definition (Inverses)

Let $*$ be an operation on a set A and suppose that A has an identity element e. Let $a \in A$. We call element b an **inverse** of a provided $a * b = b * a = e$.

- Example: Consider the operation $+$ on the integers. The identity element for $+$ is 0. Every integer a has an inverse: The inverse of a is simply $-a$ because $a + (-a) = (-a) + a = 0$.
- Example: Now consider the operation $\times$ on the rational numbers. The identity element for multiplication is 1. Most, but not all, rational numbers have inverses. If $x \in \mathbb{Q}$, then $\frac{1}{x}$ is x's inverse, unless, of course, $x = 0$.

An Operation Via a Table

- Consider the operation $*$ defined on the set $\{e, a, b, c\}$ given in the following table:

$*$	e	a	b	c
e	e	a	b	c
a	a	a	e	e
b	b	e	b	e
c	c	e	e	c

- Element e is an identity element.
- Elements b and c are inverses of a because

$$a * b = b * a = e \quad \text{and} \quad a * c = c * a = e.$$

Groups

- If an operation has an identity element, it must be unique.
- But we saw that an element might have more than one inverse.
- For most "common" operations elements have at most one inverse:
  - If $a \in \mathbb{Z}$, there is exactly one integer b such that $a + b = 0$.
  - If $a \in \mathbb{Q}$, there is at most one rational number b such that $ab = 1$.
  - If $\pi \in S_n$, there is one $\sigma \in S_n$ such that $\pi \circ \sigma = \sigma \circ \pi = \iota$.
- The reason is that associativity implies uniqueness of inverses.

Definition (Group)

Let $*$ be an operation defined on a set G. The pair $(G, *)$ is a **group** if:

1. The set G is closed under $*$, i.e., $\forall g, h \in G, g * h \in G$.
2. The operation $*$ is associative, i.e., $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
3. There is an identity $e \in G$ for $*$, i.e., $\exists e \in G, \forall g \in G, g * e = e * g = g$.
4. For every $g \in G$, there is an inverse $h \in G$, i.e., $\forall g \in G, \exists h \in G, g * h = h * g = e$.

- The following are groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}^+, \times)$, $(\mathbb{Z}_n, \oplus)$, $(S_n, \circ)$.

Abelian Groups and Uniqueness of Inverses

- The group operation $*$ need not be commutative. E.g., $\circ$ is not a commutative operation on S_n.

Definition (Abelian Groups)

Let $(G, *)$ be a group. We call this group **Abelian** provided $*$ is a commutative operation on G, i.e., $\forall g, h \in G, g * h = h * g$.

- Example: $(\mathbb{Z}, +)$ and $(\mathbb{Z}_{10}, \oplus)$ are Abelian, but $(S_n, \circ)$ is not.

Proposition (Uniqueness of Inverses)

Let $(G, *)$ be a group. Every element of G has a unique inverse in G.

- By definition, every element in G has an inverse. Suppose that $g \in G$ has two distinct inverses, say $h, k \in G$, with $h \neq k$. This means $g * h = h * g = g * k = k * g = e$, where $e \in G$ is the identity for $*$ By the associative property, $h * (g * k) = (h * g) * k$. Furthermore, $h * (g * k) = h * e = h$ and $(h * g) * k = e * k = k$. Hence $h = k$, contradicting the fact that $h \neq k$.
- We speak of **the inverse** of g and write g^{-1}.

Examples

- $(\mathbb{Z}, +)$: Integers with addition is a group.
- $(\mathbb{Q}, +)$: Rational numbers with addition is a group.
- $(\mathbb{Q}, \times)$: Rational numbers with multiplication is not a group. The problem is that $0 \in \mathbb{Q}$ does not have an inverse. We can "repair" this example in two ways:
  - We can consider only the positive rational numbers: $(\mathbb{Q}^+, \times)$ is a group.
  - Another way to repair this example is simply to eliminate the number 0. $(\mathbb{Q} - \{0\}, \times)$ is a group.
- $(S_n, \circ)$ is a group called the **symmetric group**.
- If A_n be the set of all even permutations in S_n, then $(A_n, \circ)$ is a group called the **alternating group**.
- The set of symmetries of a square with $\circ$ is a group. This group is called a **dihedral group**.
- In general, if n is an integer with $n \geq 3$, the **dihedral group** D_{2n} is the set of symmetries of a regular n-gon with the operation $\circ$.

More Examples

- $(\mathbb{Z}_n, \oplus)$ is a group for all positive integers n.
- Let $G = \{(0,0),(0,1),(1,0),(1,1)\}$. Define an operation $*$ on G by

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

where $\oplus$ is addition mod 2. The $*$ table for this group is

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

This group is known as the **Klein 4-group**. Notice that $(0,0)$ is the identity element and every element is its own inverse.

- If A is a set, then $(2^A, \Delta)$ is a group.

The Group $(\mathbb{Z}_{10}^*, \otimes)$

- $(\mathbb{Z}_{10}, \otimes)$ is not a group.
  The problem is similar to $(\mathbb{Q}, \times)$, i.e., zero does not have an inverse. The remedy in this case is a bit more complicated, because we cannot just throw away the element 0. Notice that in $(\mathbb{Z}_{10} - \{0\}, \otimes)$ the operation $\otimes$ is no longer closed. For example, $2, 5 \in \mathbb{Z}_{10} - \{0\}$, but $2 \otimes 5 = 0 \notin \mathbb{Z}_{10} - \{0\}$.
  In addition to eliminating the element 0, we can discard those elements that do not have inverses. Then, we are left with the elements in $\mathbb{Z}_{10}$ that are relatively prime to 10, i.e., with $\{1, 3, 7, 9\}$.
  The $\otimes$ table for them is

$\otimes$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

This group is denoted $(\mathbb{Z}_{10}^*, \otimes)$.

The Group $(\mathbb{Z}_{14}^*, \otimes)$

Definition ($\mathbb{Z}_n^*$)

Let n be a positive integer. We define $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.

- Example: Consider $\mathbb{Z}_{14}^*$. The invertible elements in $\mathbb{Z}_{14}^*$ (i.e., the elements relatively prime to 14) are $1, 3, 5, 9, 11$ and 13. Thus, $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$. The $\otimes$ table for $\mathbb{Z}_{14}^*$ is

$\otimes$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

The inverses of the elements in $\mathbb{Z}_{14}^*$ are

$$1^{-1} = 1,\ 3^{-1} = 5,\ 5^{-1} = 3,\ 9^{-1} = 11,\ 11^{-1} = 9,\ 13^{-1} = 13.$$

Modular Multiplication Groups I

Proposition

Let n be a positive integer. Then $(\mathbb{Z}_n^*, \otimes)$ is a group.

- To prove that $(G, *)$ is a group, we need to prove that
  - G is closed under $*$;
  - $*$ is associative;
  - G contains an identity element for $*$;
  - every element of G has a $*$-inverse in G.
- We apply these to $(\mathbb{Z}_n^*, \otimes)$:
  - Let $a, b \in \mathbb{Z}_n^*$. Thus, a and b are relatively prime to n. So, we can find integers x, y, z, w such that $ax + ny = 1$ and $bw + nz = 1$. Multiplying, we get $1 = (ax + ny)(bw + nz) =$ $(ax)(bw) + (ax)(nz) + (ny)(bw) + (ny)(nz) =$ $(ab)(wx) + (n)[axz + ybw + ynz] = (ab)(X) + (n)(Y)$, for some integers X and Y. Therefore ab is relatively prime to n. Since increasing or decreasing ab by a multiple of n results in a number still relatively prime to n, $\gcd(a \otimes b, n) = 1$, and $a \otimes b \in \mathbb{Z}_n^*$.

Modular Multiplication Groups II

- We continue with the second point:
  - That $\otimes$ is associative has already been proved.
  - Clearly $\gcd(1, n) = 1$, so $1 \in \mathbb{Z}_n^*$. Since, also, for any $a \in \mathbb{Z}_n^*$, $a \otimes 1 = 1 \otimes a = (a \cdot 1) \bmod n = a$, 1 is an identity for $\otimes$.
  - Let $a \in \mathbb{Z}_n^*$. We saw that a has an inverse $a^{-1} \in \mathbb{Z}_n$. Is $a^{-1} \in \mathbb{Z}_n^*$? Since a^{-1} is itself invertible, a^{-1} is relatively prime to n, and so $a^{-1} \in \mathbb{Z}_n^*$.

  Therefore $(\mathbb{Z}_n^*, \otimes)$ is a group.

Proposition

Let n be an integer with $n \geq 2$. Then

$$|\mathbb{Z}_n^*| = \varphi(n),$$

where $\varphi(n)$ is Euler's totient.

- This holds by the definition of $\varphi(n)$ as the number of integers from 1 to n (inclusive) that are relatively prime to n.

Subsection 2

Group Isomorphism

Idea of Isomorphism

- Two groups may have identical structures.
- Consider the groups: $(\mathbb{Z}_4, \oplus)$, $(\mathbb{Z}_5^*, \otimes)$ and the Klein 4-group:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

- In the Klein 4-group every element is its own inverse.
- We can superimpose the operation tables for the two groups $(\mathbb{Z}_4, \oplus)$ and $(\mathbb{Z}_5^*, \otimes)$ on top of one another so they look the same.
- We pair:

$(\mathbb{Z}_4, \oplus)$		$(\mathbb{Z}_5^*, \otimes)$
0	$\leftrightarrow$	1
1	$\leftrightarrow$	2
2	$\leftrightarrow$	4
3	$\leftrightarrow$	3

$\oplus$ $\otimes$	0 1	1 2	2 4	3 3
0 1	0 1	1 2	2 4	3 3
1 2	1 2	2 4	3 3	0 1
2 4	2 4	3 3	0 1	1 2
3 3	3 3	0 1	1 2	2 4

Formalizing Isomorphism

- Let $f : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ be defined by
$$f(0) = 1,\ f(1) = 2,\ f(2) = 4,\ f(3) = 3.$$
f is a bijection and $f(x \oplus y) = f(x) \otimes f(y)$, where $\oplus$ is mod 4 addition and $\otimes$ is mod 5 multiplication.

Definition (Isomorphism of Groups)

Let $(G, *)$ and $(H, \star)$ be groups. A function $f : G \to H$ is called a **(group) isomorphism** provided f is one-to-one and onto and satisfies
$$\forall g, h \in G, f(g * h) = f(g) \star f(h).$$
When there is an isomorphism from G to H, we say G is **isomorphic** to H and we write $G \cong H$.

- The “is-isomorphic-to” relation is an equivalence relation, i.e.,
  - for any group G, $G \cong G$,
  - for any two groups G and H, if $G \cong H$, then $H \cong G$,
  - for any three groups G, H, and K, if $G \cong H$ and $H \cong K$, then $G \cong K$.

Generators and Cyclic Groups: Examples

- Element 1 of $(\mathbb{Z}_4, \oplus)$ generates all the elements of the group $(\mathbb{Z}_4, \oplus)$:
$$1 = 1,\ 1 \oplus 1 = 2,\ 1 \oplus 1 \oplus 1 = 3,\ 1 \oplus 1 \oplus 1 \oplus 1 = 0.$$
- The element 3 also generates all the elements of $(\mathbb{Z}_4, \oplus)$:
$$3 = 3,\ 3 \oplus 3 = 2,\ 3 \oplus 3 \oplus 3 = 1,\ 3 \oplus 3 \oplus 3 \oplus 3 = 0.$$
- Because $(\mathbb{Z}_5^*, \otimes)$ is isomorphic to $(\mathbb{Z}_4, \oplus)$, it, too, must have a generator: Since $1 \in \mathbb{Z}_4$ corresponds to $2 \in \mathbb{Z}_5^*$, we calculate
$$2 = 2,\ 2 \otimes 2 = 4,\ 2 \otimes 2 \otimes 2 = 3,\ 2 \otimes 2 \otimes 2 \otimes 2 = 1.$$
Thus element $2 \in \mathbb{Z}_5^*$ generates the group.
- The Klein 4-group does not have an element that generates the entire group. In this group, every element g has the property that $g * g = e = (0, 0)$. So there is no way that g, $g * g$, $g * g * g$, $\ldots$ can generate all the elements of the group.

Generators and Cyclic Groups

- There is no element of $\mathbb{Z}$ that generates $(\mathbb{Z}, +)$. The element 1 generates all the positive elements of $\mathbb{Z}$. If we allow 1's inverse, -1, to participate in the generation process, then we can get 0 (as $1 + (-1)$) and all the negative numbers.

Definition (Generator, Cyclic Group)

Let $(G, *)$ be a group. An element $g \in G$ is called a **generator** for G if every element of G can be expressed just in terms of g and g^{-1} using the operation $*$. If a group contains a generator, it is called **cyclic**.

- The special provision for g^{-1} is necessary only for groups with infinitely many elements. If $(G, *)$ is a finite group and $g \in G$, then we can always find a way to write $g^{-1} = \underbrace{g * g * \cdots * g}_{n \text{ factors, for some } n > 0}$.

Expressing g^{-1} in terms of g

Proposition

Let $(G,*)$ be a finite group and let $g \in G$. Then, for some positive integer n, we have $g^{-1} = \underbrace{g * g * \cdots * g}_{n \text{ times}}$.

- We write $g^n = \underbrace{g * g * \cdots * g}_{n \text{ times}}$.
- Let $(G,*)$ be a finite group and let $g \in G$. Consider the sequence $g^1, g^2, g^3, g^4, \ldots$. Since the group is finite, this sequence must, at some point, repeat itself. Suppose the first repeat is at $g^a = g^b$, where $a < b$.
- Claim: $a = 1$.
  - Suppose $a > 1$. Then, since $g^a = g^b$, by operating on the left by g^{-1}, we get $g^{-1} * g^a = g^{-1} * g^b$, which gives $g^{a-1} = g^{b-1}$. Thus, the first repeat is before $g^a = g^b$, a contradiction. Therefore, $a = 1$.

Expressing g^{-1} in terms of g: Proof (Cont'd)

- We considered $g^1, g^2, g^3, \ldots$, which repeats when $g^a = g^b$, for $a = 1$.
- So, if we stop at the first repeat, the sequence is $g^1, g^2, g^3, \ldots, g^b = g$. Notice that since $g = g^b$, if we operate on the left by g^{-1}, we get $e = g^{b-1}$.
  - If $b = 2$, we get $g^2 = g$. In this case, $g = e$ and so $g^1 = g^{-1}$, proving the result.
  - If $b > 2$, we can write $e = g^{b-1} = g^{b-2} * g$. Therefore, $g^{b-2} = g^{-1}$, proving again the result.

Structure of Finite Cyclic Groups

Theorem (Finite Cyclic Groups)

Let $(G, *)$ be a finite cyclic group. Then $(G, *)$ is isomorphic to $(\mathbb{Z}_n, \oplus)$, where $n = |G|$.

- Let $(G, *)$ be a finite cyclic group. Suppose $|G| = n$ and let $g \in G$ be a generator. We claim that $(G, *) \cong (\mathbb{Z}_n, \oplus)$. Define $f : \mathbb{Z}_n \to G$ by $f(k) = g^k$. To prove that f is an isomorphism, we must show that
  - f is one-to-one and onto;
  - $f(j \oplus k) = f(j) * f(k)$.

  We undertake one at a time:
  - f is one-to-one: Suppose $f(j) = f(k)$. This means that $g^j = g^k$. We want to prove that $j = k$. Suppose that $j \neq k$. Without loss of generality, $0 \leq j < k < n$. We can $*$ the equation $g^j = g^k$ on the left by $(g^{-1})^j$ to get $(g^{-1})^j * g^j = (g^{-1})^j * g^k$, i.e., $e = g^{k-j}$. Since $k - j < n$, this means that the sequence $g, g^2, g^3, \ldots$ repeats after $k - j$ steps, and therefore g does not generate the entire group (but only $k - j$ of its elements). However, g is a generator, which is a contradiction. Therefore f is one-to-one.

Structure of Finite Cyclic Groups (Cont'd)

- We have shown $f(k) = g^k$ is one-to-one. We continue with the remaining two steps.
  - f is onto: Let $h \in G$. We must find $k \in \mathbb{Z}_n$, such that $f(k) = h$. We know that the sequence $e = g^0, g = g^1, g^2, g^3, \ldots$ must contain all elements of G. Thus, h is somewhere on this list, say, at position k (i.e., $h = g^k$). Therefore, $f(k) = h$ and f is onto.
  - For all $j, k \in \mathbb{Z}_n$, we have $f(j \oplus k) = f(j) * f(k)$: Recall that $j \oplus k = (j + k) \bmod n = j + k + tn$, for some integer t. Therefore,

$$\begin{aligned} f(j \oplus k) &= g^{j+k+tn} = g^j * g^k * g^{tn} = g^j * g^k * (g^n)^t \\ &= g^j * g^k * e^t = g^j * g^k = f(j) * f(k). \end{aligned}$$

  Therefore, $f : \mathbb{Z}_n \to G$ is an isomorphism, and, hence, $(\mathbb{Z}_n, \oplus) \cong (G, *)$.

Subsection 3

Subgroups

Subgroups

- Consider the integers as a group: $(\mathbb{Z}, +)$. Within the set of integers, we find the set of even integers, $E = \{x \in \mathbb{Z} : 2 \mid x\}$. $(E, +)$ is also a group: it satisfies the four required properties.
  - $+$ is closed on E (the sum of two even integers is again even);
  - addition is associative;
  - E contains the identity element 0;
  - if x is an even integer, then $-x$ is also, so inverses are in E.

  In this case, we call $(E, +)$ a subgroup of $(\mathbb{Z}, +)$.

Definition (Subgroup)

Let $(G, *)$ be a group and let $H \subseteq G$. If $(H, *)$ is also a group, we call it a **subgroup of** $(G, *)$.

- The operation for the group and the operation for its subgroup must be the same: It is incorrect to say that $(\mathbb{Z}_{10}, \oplus)$ is a subgroup of $(\mathbb{Z}, +)$; it is true that $\mathbb{Z}_{10} \subseteq \mathbb{Z}$, but the operations $\oplus$ and $+$ are different.

Subgroups of $(\mathbb{Z}_{10}, \oplus)$

- The subgroups of $(\mathbb{Z}_{10}, \oplus)$ are
$$\begin{array}{ll} \{0\}, & \{0,1,2,3,4,5,6,7,8,9\}, \\ \{0,5\}, & \{0,2,4,6,8\}. \end{array}$$
- How can we verify that our answer is correct?
  - For each subset H we listed, is $(H, \oplus)$ a group?
  - Are there other subsets $H \subseteq \mathbb{Z}_{10}$ that we missed?
- If $(G, *)$ is a group, to determine whether $(H, *)$ is a subgroup of $(G, *)$:
  - First, we check $H \subseteq G$.
  - Second, we show that $(H, *)$ is a group:
    - To check closure, we need to prove that if $g, h \in H$, then $g * h \in H$.
    - We do not have to check associativity: $(G, *)$ is a group and therefore $*$ is associative on G. Since $H \subseteq G$, we must have that $*$ is already associative on H.
    - Next, we check that the identity element is in H.
    - Finally, we know that every element of H has an inverse (because every element of $G \supseteq H$ has an inverse). If $g \in H$, we must show $g^{-1} \in H$.

Back to the Subgroups of $(\mathbb{Z}_{10}, \oplus)$

- Are $\{0\}$, $\{0,1,2,3,4,5,6,7,8,9\}$, $\{0,5\}$ and $\{0,2,4,6,8\}$ truly subgroups of $(\mathbb{Z}_{10}, \oplus)$?
- We check these claims:
  - $H = \{0\}$ is a subgroup of $(\mathbb{Z}_{10}, \oplus)$.
    - Since $0 \oplus 0 = 0$, we see that H is closed under $\oplus$.
    - It contains the identity.
    - Since 0's inverse is 0, the inverse of every element in H is also in H.
  - $H = \mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ is a subgroup of $(\mathbb{Z}_{10}, \oplus)$. Since $(\mathbb{Z}_{10}, \oplus)$ is a group, it is a subgroup of itself.
  - $H = \{0,5\}$ is a subgroup of $(\mathbb{Z}_{10}, \oplus)$.
    - H is closed under $\oplus$ since $0 \oplus 0 = 5 \oplus 5 = 0$ and $0 \oplus 5 = 5 \oplus 0 = 5$.
    - Clearly $0 \in H$.
    - 0 and 5 are their own inverses.
  - $H = \{0,2,4,6,8\}$ is a subgroup of $(\mathbb{Z}_{10}, \oplus)$.
    - Reduction mod 10 of an even number is even.
    - $0 \in H$.
    - The inverses of 0, 2, 4, 6, 8 are 0, 8, 6, 4, 2, respectively.

Any More Subgroups of $(\mathbb{Z}_{10}, \oplus)$?

- Are there other subgroups of $(\mathbb{Z}_{10}, \oplus)$?
- Suppose $H \subseteq \mathbb{Z}_{10}$ and that $(H, \oplus)$ is a subgroup of $(\mathbb{Z}_{10}, \oplus)$. Since $(H, \oplus)$ is a group, we must have $0 \in H$. If the only element of H is 0, we have $H = \{0\}$. Otherwise the following analysis applies:
  - Suppose $1 \in H$. Then $1 \oplus 1 = 2 \in H$. Also $1 \oplus 2 = 3 \in H$. Continuing, we get $H = \mathbb{Z}_{10}$. Thus, if $1 \in H$, $H = \mathbb{Z}_{10}$.
  - Suppose $3 \in H$. Then $3 \oplus 3 = 6 \in H$ and $3 \oplus 6 = 9 \in H$. Since $9 \in H$, so is its inverse, $1 \in H$. But, if $1 \in H$, then $H = \mathbb{Z}_{10}$.
  - If $7 \in H$ or if $9 \in H$, then we can show that $1 \in H$, and then $H = \mathbb{Z}_{10}$.
  - Suppose $5 \in H$. We have $H \supseteq \{0, 5\}$. If $2 \in H$, then $2 \oplus 5 = 7 \in H$, whence $H = \mathbb{Z}_{10}$. Similarly, if any even is in H, then $H = \mathbb{Z}_{10}$. So if $5 \in H$, then either $H = \{0, 5\}$ or $H = \mathbb{Z}_{10}$.
  - If all elements in H are even:
    - If $2 \in H$, then $4, 6, 8 \in H$, so $H = \{0, 2, 4, 6, 8\}$.
    - If $4 \in H$, then $4 \oplus 4 \oplus 4 = 2 \in H$, and $H = \{0, 2, 4, 6, 8\}$.
    - Similarly, if 6 or 8 is in H, again $H = \{0, 2, 4, 6, 8\}$.

Examples of Cardinalities of Subgroups

- The four subgroups of $(\mathbb{Z}_{10}, \oplus)$ have cardinalities 1, 2, 5, and 10. These four numbers are divisors of 10.
- We list all the subgroups of $(S_3, \circ)$, i.e., of the set of all permutations of $\{1, 2, 3\}$ with the composition operation. Recall $S_3 = \{(1)(2)(3), (12)(3), (13)(2), (1)(23), (123), (132)\}$. Its subgroups are

$$\{(1)(2)(3)\}$$
$$\{(1)(2)(3), (12)(3)\} \quad \{(1)(2)(3), (13)(2)\} \quad \{(1)(2)(3), (1)(23)\}$$
$$\{(1)(2)(3), (123), (132)\}$$
$$\{(1)(2)(3), (12)(3), (13)(2), (1)(23), (123), (132)\}.$$

The cardinalities of these subgroups are 1, 2, 3 and 6. Note, again, that they are all divisors of 6.

Congruence Modulo a Subgroup

Definition (Congruence Modulo a Subgroup)

Let $(G, *)$ be a group and let $(H, *)$ be a subgroup. Let $a, b \in G$. We say that a is **congruent to** b **modulo** H if $a * b^{-1} \in H$. We write this as $a \equiv b \pmod{H}$.

- Example: Consider the group $(\mathbb{Z}_{25}^*, \otimes)$. We have $\mathbb{Z}_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$. Let $H = \{1, 7, 18, 24\}$. The operation table for $\otimes$ restricted to H is

$\otimes$	1	7	18	24
1	1	7	18	24
7	7	24	1	18
18	18	1	24	7
24	24	18	7	1

H is a subgroup of $\mathbb{Z}_{25}$:

- H is closed under $\otimes$.
- The identity element $1 \in H$.
- The inverse of every element of H is in H.

Do we have $2 \equiv 3 \pmod{H}$? Calculate $2 \otimes 3^{-1} = 2 \otimes 17 = 9 \notin H$. Therefore $2 \not\equiv 3 \pmod{H}$.
Since $2 \otimes 11^{-1} = 2 \otimes 16 = 7 \in H$, we have $2 \equiv 11 \pmod{H}$.

Congruence Modulo a Subgroup is an Equivalence Relaion

Lemma

Let $(G, *)$ be a group and let $(H, *)$ be a subgroup. Then congruence modulo H is an equivalence relation on G.

- Congruence modulo H is reflexive, symmetric, and transitive:
  - Congruence modulo H is reflexive: Let $g \in G$. We need to show that $g \equiv g \pmod{H}$. To do that, we need to show $g * g^{-1} \in H$. Since $g * g^{-1} = e$ and, since $e \in H$, we have $g \equiv g \pmod{H}$.
  - Congruence modulo H is symmetric: Suppose $a \equiv b \pmod{H}$. Then $a * b^{-1} \in H$. Therefore, $(a * b^{-1})^{-1} \in H$. But $(a * b^{-1})^{-1} = (b^{-1})^{-1} * a^{-1} = b * a^{-1} \in H$. Thus, we have $b \equiv a \pmod{H}$.
  - Congruence modulo H is transitive: Suppose $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. Thus, $a * b^{-1}, b * c^{-1} \in H$. Since H is a subgroup and, therefore, closed under $*$, $(a * b^{-1}) * (b * c^{-1}) = a * (b^{-1} * b) * c^{-1} = a * c^{-1} \in H$. Therefore $a \equiv c \pmod{H}$.

Therefore congruence modulo H is an equivalence relation on G.

Example of Equivalence Classes

- Since congruence mod H is an equivalence relation, we may consider the equivalence classes of this relation.
- Recall the group $(\mathbb{Z}_{25}, \otimes)$ and its subgroup $H = \{1, 7, 18, 24\}$ we considered in the previous slide. For the congruence mod H relation, what is the equivalence class [2]?
  This is the set of all elements of $\mathbb{Z}_{25}$ that are related to 2, i.e., $[2] = \{a \in \mathbb{Z}_{25} : a \equiv 2 \pmod{H}\}$. By testing all 20 elements of $\mathbb{Z}_{25}$, we find that $[2] = \{2, 11, 14, 23\}$. The other equivalence classes are

  $$[1] = \{1, 7, 18, 24\} \quad [2] = \{2, 11, 14, 23\} \quad [3] = \{3, 4, 21, 22\}$$
  $$[6] = \{6, 8, 17, 19\} \quad [9] = \{9, 12, 13, 16\}$$
- These are all the equivalence classes of congruence mod H, since every element of $\mathbb{Z}_{25}$ is in exactly one of these classes.
- We know the equivalence classes form a partition of the group.
- The class [1] equals the subgroup $H = \{1, 7, 18, 24\}$.
- The equivalence classes all have the same size.

Size of Equivalence Classes

Lemma

Let $(G, *)$ be a group and let $(H, *)$ be a finite subgroup. Then any two equivalence classes of the congruence mod H relation have the same size.

- Let $g \in G$ be arbitrary. It is enough to show that $[g] = [e]$. Note $[e] = \{a \in G : a \equiv e \pmod{H}\} = \{a \in G : a * e^{-1} \in H\} = \{a \in G : a \in H\} = H$. To show that $[g] = H$, we define a function $f : H \to [g]$ and we prove that f is one-to-one and onto. For $h \in H$, define $f(h) = h * g$.
  - Clearly f is a function defined on H.
  - Is $f : H \to [g]$? Since $f(h) * g^{-1} = (h * g) * g^{-1} = h * (g * g^{-1}) = h \in H$, $f(h) \equiv g \pmod{H}$, whence $f(h) \in [g]$.
  - Now, we show that f is one-to-one. Suppose $f(h) = f(h')$. Then, $h * g = h' * g$. So $(h * g) * g^{-1} = (h' * g) * g^{-1}$, whence $h = h'$.
  - Finally, we show that f is onto. Let $b \in [g]$. This means that $b \equiv g \pmod{H}$, whence $b * g^{-1} \in H$. Let $h = b * g^{-1}$. Then $f(h) = f(b * g^{-1}) = (b * g^{-1}) * g = b * (g * g^{-1}) = b$. So f is onto $[g]$.

Lagrange's Theorem

Theorem (Lagrange)

Let $(H, *)$ be a subgroup of a finite group $(G, *)$ and let $a = |H|$ and $b = |G|$. Then $a \mid b$.

- Let $(G, *)$ be a finite group and let $(H, *)$ be a subgroup.
- By the preceding lemma, the equivalence classes of the "is-congruent-to-mod-H" relation all have the same cardinality as H.
- Since the equivalence classes form a partition of G, $|H|$ must be a divisor of $|G|$.

Subsection 4

Fermat's Little Theorem

Fermat's Little Theorem: An Example

Theorem (Fermat's Little Theorem)

Let p be a prime and let a be an integer. Then $a^p \equiv a \pmod{p}$.

- Example: If $p = 23$, then the powers of 5 taken modulo 23 are

$$\begin{array}{lllll}
5^1 \equiv 5 & 5^2 \equiv 2 & 5^3 \equiv 10 & 5^4 \equiv 4 & 5^5 \equiv 20 \\
5^6 \equiv 8 & 5^7 \equiv 17 & 5^8 \equiv 16 & 5^9 \equiv 11 & 5^{10} \equiv 9 \\
5^{11} \equiv 22 & 5^{12} \equiv 18 & 5^{13} \equiv 21 & 5^{14} \equiv 13 & 5^{15} \equiv 19 \\
5^{16} \equiv 3 & 5^{17} \equiv 15 & 5^{18} \equiv 6 & 5^{19} \equiv 7 & 5^{20} \equiv 12 \\
5^{21} \equiv 14 & 5^{22} \equiv 1 & 5^{23} \equiv 5 & 5^{24} \equiv 2 & 5^{25} \equiv 10
\end{array}$$

where all congruences are mod 23.

Fermat's Little Theorem: First Proof

- We first prove by induction the result for $a \geq 0$, i.e., that if p is prime and $a \in \mathbb{N}$, then $a^p \equiv a \pmod{p}$.
  - Basis case: If $a = 0$, $a^p = 0^p = 0 = a$, so $a^p \equiv a \pmod{p}$.
  - Induction Hypothesis: Suppose $k^p \equiv k \pmod{p}$.
  - Induction Step: We show $(k+1)^p \equiv k+1 \pmod{p}$. By the Binomial Theorem, $(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k + 1$. All but the first and last terms on the right are of the form $\binom{p}{j}k^{p-j}$, where $0 < j < p$. The binomial coefficient $\binom{p}{j}$ is an integer: $\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1)!}{j!(p-j)!}$. Factor the numerator and the denominator into primes and cancel matching primes. Since p is a prime factor of the numerator but not of the denominator, this integer must be a multiple of p. So $k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{p-1}k + 1 \equiv k^p + 1 \pmod{p}$. Since, $k^p \equiv k \pmod{p}$, $(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod{p}$.
- We finally show that $(-a)^p \equiv (-a) \pmod{p}$ where $a > 0$.
  - If $p = 2$, $(-a)^2 \equiv a^2 \equiv a \equiv -a \pmod{2}$.
  - If $p > 2$, we have $(-a)^p = (-1)^p a^p = -(a^p) \equiv -a \pmod{p}$.

Fermat's Little Theorem: Second Proof I

- We again assume a is a positive integer. The case $a = 0$ is trivial, and the case $a < 0$ is handled as in the previous proof.
- With p a prime and a a positive integer, we ask: How many length p lists can be formed in which the elements of the list are chosen from $\{1, 2, \ldots, a\}$? The answer to this question is a^p.
- We define an equivalence relation R on these lists: Two lists are **equivalent** if we can get one from the other by cyclically shifting its entries. For example $12334 \; R \; 41233 \; R \; 34123 \; R \; 33412 \; R \; 23341$.
- How many nonequivalent length p lists can be formed in which the elements of the list are chosen from $\{1, 2, \ldots, a\}$? I.e., can we count the number of R-equivalence classes?
- Example: Consider the case $a = 2$ and $p = 3$. There are eight lists we can form:
$$111, 112, 121, \; 122, \; 211, \; 212, \; 221, \; 222.$$
These fall into four equivalence classes: $\{111\}$, $\{222\}$, $\{112, 121, 211\}$ and $\{122, 212, 221\}$.

Fermat's Little Theorem: Example Showcasing Proof

- Example: Consider the case $a = 3$ and $p = 5$. There are $3^5 = 243$ possible lists (from 11111 to 33333). There are three equivalence classes that contain just one list, namely $\{11111\}, \{22222\}$ and $\{33333\}$. The remaining lists fall into equivalence classes containing more than one element. For example, the list 12113 is in the following equivalence class: $[12113] = \{12113, 31211, 13121, 11312, 21131\}$. By experimenting, notice that all the equivalence classes with more than one list contain exactly five lists. Thus there are three equivalence classes that contain only one list and the remaining $3^5 - 3$ lists fall into classes containing exactly five lists each. There are $\frac{3^5-3}{5}$ such classes. Thus, all told, there are $3 + \frac{3^5-3}{5} = 51$ different equivalence classes. The number $\frac{3^5-3}{5}$ is an integer. Therefore $3^5 - 3$ is divisible by 5, i.e., $3^5 \equiv 3 \pmod 5$.

Fermat's Little Theorem: Second Proof II

- How many elements does an equivalence class contain?
  - For lists all of whose elements are the same, the equivalence classes contain exactly one list.
  - For a list with (at least) two different elements $x_1x_2\cdots x_{p-1}x_p$, where the elements are drawn from $\{1,2,\ldots,a\}$, the equivalence class of this list contains $x_1x_2x_3\cdots x_{p-1}x_p$, $x_2x_3\cdots x_{p-1}x_px_1$, $x_3\cdots x_{p-1}x_px_1x_2$, $\ldots$, $x_px_1x_2\cdots x_{p-1}$. Are there p lists in this equivalence class, or is there a repetition?
  - Claim: If the elements of the list $x_1x_2x_3\cdots x_{p-1}x_p$ are not all the same, then the p lists above are all different.
  - Thus there are a equivalence classes of size 1 and the remaining $a^p - a$ lists form equivalence classes of size p. All together, there are $a + \frac{a^p-a}{p}$ different equivalence classes. Since this number must be an integer, $a^p - a$ is divisible by p, i.e., $a^p \equiv a \pmod{p}$.

Fermat's Little Theorem: Proof of the Claim

- Claim: If the elements of the list $x_1x_2x_3\cdots x_{p-1}x_p$ are not all the same, then the p lists above are all different.
  - Suppose that $x_ix_{i+1}\cdots x_{i-1}=x_jx_{j+1}\cdots x_{j-1}$, with $1\leq i<j\leq p$. Then $x_i=x_j$, $x_{i+1}=x_{j+1}$, $\ldots$, $x_{i-1}=x_{j-1}$. Therefore, if we cyclically shift the list $x_1x_2x_3\cdots x_{p-1}x_p$ by $j-i$ steps, the resulting sequence is identical to the original. Thus, $x_1=x_{1+(j-i)}$. If we shift the list another $j-i$ steps, we again return to the original: $x_1=x_{1+2(j-i)}$. We always add or subtract a multiple of p so that the subscript on x lies in the set $\{1,2,\ldots,p\}$. So we get

$$x_1=x_{1+(j-i)}=x_{1+2(j-i)}=x_{1+3(j-i)}=\cdots=x_{1+(p-1)(j-i)}.$$

But this equation says that $x_1=x_2=\cdots=x_p$, a contradiction!

A Handy Lemma

Lemma

Let $(G, *)$ be a finite group, with identity e, and let $g \in G$. Then $g^{|G|} = e$.

- Consider the sequence $g^1, g^2, g^3, \ldots$. Since $(G, *)$ is finite, this sequence must repeat, i.e., $g^i = g^j$, for some $1 \leq i < j$. $*$ both sides by $(g^{-1})^i$ to get $e = g^{j-i}$. Thus, there is $k > 0$, such that $g^k = e$.
- By the Well-Ordering Principle, there is a least positive integer k such that $g^k = e$. Define the **order of the element** g, denoted $|g|$, to be the smallest such positive integer.
- Claim: $\langle g \rangle = \{e, g, g^2, g^3, \ldots\}$ is a subgroup of G, with $|\langle g \rangle| = |g|$.
  - Clearly, it is closed under $*$;
  - It contains e;
  - Every element g^i has an inverse: Let $i = kq + r$, with $0 \leq r < k$. Then $g^i * g^{k-r} = g^{(kq+r)+(k-r)} = g^{k(q+1)} = e$, whence $(g^i)^{-1} = g^{k-r}$.
- By Lagrange's Theorem, $|\langle g \rangle| = |g|$ divides $|G|$. Therefore $g^{|G|} = g^{k|g|} = (g^{|g|})^k = e^k = e$.

Fermat's Little Theorem: Third Proof

- We work in the group $(\mathbb{Z}_p^*, \otimes)$ and prove the result only for $a > 0$.
- If a is a multiple of p, then $a^p \equiv a \equiv 0 \pmod{p}$.
- If we increase (or decrease) a by a multiple of p, there is no change modulo p in the value of a^p: $(a+kp)^p =$
  $a^p + \binom{p}{1}a^{p-1}(kp)^1 + \binom{p}{2}a^{p-2}(kp)^2 + \cdots + \binom{p}{p}a^0(kp)^p \equiv a^p \pmod{p}$.
- Therefore we may assume that a is an integer in the set $\{1, 2, \ldots, p-1\} = \mathbb{Z}_p^*$.
- The equation $a^p \equiv a \pmod{p}$ is equivalent to $\underbrace{a \otimes a \otimes \cdots \otimes a}_{p \text{ times}} = a$.

  This can be rewritten $a^p = a$. If we $\otimes$ both sides by a^{-1}, we have $a^{p-1} = 1$. Conversely, if we can prove $a^{p-1} = 1$ in $\mathbb{Z}_p^*$, then our proof will be complete. This, however, was the content of the preceding lemma!

Euler's Theorem: Example

- Fermat's Little Theorem does not hold for any non-prime moduli, i.e., it is not the case that $a^n \equiv a \pmod{n}$ for any positive integer n.
- Example: Consider $n = 9$. We have

$$\begin{array}{lll} 1^9 \equiv 1 & 2^9 \equiv 8 \not\equiv 2 & 3^9 \equiv 0 \not\equiv 3 \\ 4^9 \equiv 1 \not\equiv 4 & 5^9 \equiv 8 \not\equiv 5 & 6^9 \equiv 0 \not\equiv 6 \\ 7^9 \equiv 1 \not\equiv 7 & 8^9 \equiv 8 & 9^9 \equiv 0 \equiv 9 \end{array}$$

  where all congruences are modulo 9. So, the formula $a^p \equiv a \pmod{p}$ does not extend to non prime values of p.
- A clue is gotten by looking more closely to the third proof: The key was that $a^{p-1} = 1$ in $\mathbb{Z}_p^*$. This holds because:
  - $a \in \mathbb{Z}_p^*$;
  - the exponent $p - 1$ is the number of elements in $\mathbb{Z}_p^*$. In general, however, $|\mathbb{Z}_n^*| = \varphi(n)$, Euler's totient.
- Example: We replace the exponent 9 with the exponent $\varphi(9) = 6$ in the previous example. We have $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ and $\varphi(9) = 6$. Raising the integers 1 through 9 to the power 6 $\pmod{9}$ gives

$$\begin{array}{lllll} 1^6 \equiv 1 & 2^6 \equiv 1 & 3^6 \equiv 0 & 4^6 \equiv 1 & 5^6 \equiv 1 \\ 6^6 \equiv 0 & 7^6 \equiv 1 & 8^6 \equiv 1 & 9^6 \equiv 0. & \end{array}$$

Euler's Theorem

- We have seen that if $a \in \mathbb{Z}_n^*$, then $a^{|\mathbb{Z}_n^*|} = 1$. Since $|\mathbb{Z}_n^*| = \varphi(n)$, this can be rewritten $a^{\varphi(n)} = 1$, with multiplication in $\mathbb{Z}_n^*$.

Theorem (Euler's Theorem)

Let n be a positive integer and let a be an integer relatively prime to n. Then

$$a^{\varphi(n)} = 1 \pmod{n}.$$

- Let a be relatively prime to n. Dividing a by n, we have $a = qn + r$, where $0 \leq r < n$. Since a is relatively prime to n, so is r. Thus we may assume that $a \in \mathbb{Z}_n^*$. Now, by a preceding lemma, $\varphi(n) = |\mathbb{Z}_n^*|$ implies $a^{\varphi(n)} = 1$ in $\mathbb{Z}_n^*$, which is equivalent to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Primality Testing

- Fermat's Little Theorem states that if p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a. We can write this symbolically as
$$p \text{ is a prime } \Rightarrow \forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}.$$
- The contrapositive of this statement is
$$\neg[\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}] \Rightarrow p \text{ is not a prime},$$
which can be rewritten
$$\exists a \in \mathbb{Z}, a^p \not\equiv a \pmod{p} \Rightarrow p \text{ is not a prime}.$$
- This says that, if there is some integer a such that $a^p \not\equiv a \pmod{p}$, then p is not a prime. Therefore, we have shown:

Theorem

Let a and n be positive integers. If $a^n \not\equiv a \pmod{n}$, then n is not prime.

- This theorem can be used for showing that an integer is not prime.
- But, if we have positive integers a and n with $a^n \equiv a \pmod{n}$, then we cannot conclude that n is prime!