CMSC/Math 456: Cryptography (Fall 2022)

Lecture 10

Daniel Gottesman

Administrative

Problem set #4 should have been turned in. Solutions for problem set #3 are on ELMS.

Problem set #5 is available now, due next Thursday, Oct. 7.

This class is being recorded

$\mathbb{Z}_N$ and $\mathbb{Z}_N^*$

We have been working numbers modulo N. I will start using the notation $\mathbb{Z}_N$ to refer to this.

But, as we have seen, nice things happen if we restrict attention to g that is relatively prime to N, $\gcd(g, N) = 1$:

- Division is well-defined for such g
- $\exists r$ (="there exists r") such that $g^r = 1 \bmod N$. That is, exponentiation cycles back to 1.

Definition: Let $\mathbb{Z}_N^* \subseteq \mathbb{Z}_N$ be the set of $g \in \{0, \ldots, N-1\}$ such that $\gcd(g, N) = 1$.

Closure of $\mathbb{Z}_N^*$

Proposition: If $\gcd(g, N) = 1$ and $\gcd(h, N) = 1$, then $\gcd(gh, N) = 1$ as well. I.e., $\mathbb{Z}_N^*$ is closed under multiplication.

Closure of $\mathbb{Z}_N^*$

Proposition: If $\gcd(g, N) = 1$ and $\gcd(h, N) = 1$, then $\gcd(gh, N) = 1$ as well. I.e., $\mathbb{Z}_N^*$ is closed under multiplication.

Proof:

Recall that x^{-1} is well-defined mod N iff $\gcd(x, N) = 1$.

This class is being recorded

Closure of $\mathbb{Z}_N^*$

Proposition: If $\gcd(g, N) = 1$ and $\gcd(h, N) = 1$, then $\gcd(gh, N) = 1$ as well. I.e., $\mathbb{Z}_N^*$ is closed under multiplication.

Proof:

Recall that x^{-1} is well-defined mod N iff $\gcd(x, N) = 1$.

But $(gh)^{-1} = h^{-1}g^{-1}$:

$$(h^{-1}g^{-1})(gh) = h^{-1} \cdot 1 \cdot h \bmod N = 1 \bmod N$$

Closure of $\mathbb{Z}_N^*$

Proposition: If $\gcd(g, N) = 1$ and $\gcd(h, N) = 1$, then $\gcd(gh, N) = 1$ as well. I.e., $\mathbb{Z}_N^*$ is closed under multiplication.

Proof:

Recall that x^{-1} is well-defined mod N iff $\gcd(x, N) = 1$.

But $(gh)^{-1} = h^{-1}g^{-1}$:

$$(h^{-1}g^{-1})(gh) = h^{-1} \cdot 1 \cdot h \bmod N = 1 \bmod N$$

This means that gh has an inverse and therefore $\gcd(gh, N) = 1$.

Groups

Definition: A group (G, *) is a set G of elements along with a binary operation $*: G \times G \to G$ with the following properties:

1. Closure: $g * h \in G$ when $g, h \in G$.
2. Associativity: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$.
3. Identity: $\exists e \in G$ such that $\forall g \in G, e * g = g * e = g$.
4. Inverses: $\forall g \in G, \exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A group which also satisfies

5. Commutativity: $\forall g, h \in G, g * h = h * g$

is called an abelian group.

Usually we just refer to G as the group. If we need to specify the group operation, we say "G under [operation]." Usually instead of *, the group operation is just written + or $\cdot$ like addition or multiplication even if it is not those.

This class is being recorded

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ under multiplication? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/ bad question.

Integers $\mathbb{Z}$? Vote. — Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote — Yes.

Integers $\mathbb{Z}$ under multiplication? Vote — No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote — No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote — Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/ bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

Group Examples

For each of the following, vote on whether it is a group: yes/no/ bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

$\mathbb{Z}_N$ under addition? Vote

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.	Bad question. Which group operation?
Integers $\mathbb{Z}$ under addition? Vote	Yes.
Integers $\mathbb{Z}$ under multiplication? Vote	No. No inverses.
Reals $\mathbb{R}$ under multiplication? Vote	No. 0 still has no inverse.
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ under multiplication? Vote	Yes.
$\mathbb{R}^*$ under exponentiation? Vote	No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)
$\mathbb{Z}_N$ under addition? Vote	Yes.

Group Examples

For each of the following, vote on whether it is a group: yes/no/ bad question.

Integers $\mathbb{Z}$? Vote.	Bad question. Which group operation?
Integers $\mathbb{Z}$ under addition? Vote	Yes.
Integers $\mathbb{Z}$ under multiplication? Vote	No. No inverses.
Reals $\mathbb{R}$ under multiplication? Vote	No. 0 still has no inverse.
$\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ under multiplication? Vote	Yes.
$\mathbb{R}^*$ under exponentiation? Vote	No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)
$\mathbb{Z}_N$ under addition? Vote	Yes.
$\mathbb{Z}_N^*$ under multiplication? Vote	

This class is being recorded

Group Examples

For each of the following, vote on whether it is a group: yes/no/bad question.

Integers $\mathbb{Z}$? Vote.

Bad question. Which group operation?

Integers $\mathbb{Z}$ under addition? Vote

Yes.

Integers $\mathbb{Z}$ under multiplication? Vote

No. No inverses.

Reals $\mathbb{R}$ under multiplication? Vote

No. 0 still has no inverse.

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ under multiplication? Vote

Yes.

$\mathbb{R}^*$ under exponentiation? Vote

No. Fails associativity (e.g., $(3^3)^3 \neq 3^{(3^3)}$) and closure (e.g., $(-1)^{0.5}$)

$\mathbb{Z}_N$ under addition? Vote

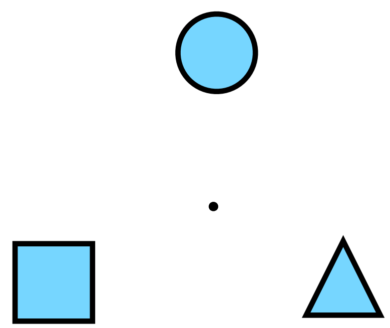
Yes.

$\mathbb{Z}_N^*$ under multiplication? Vote

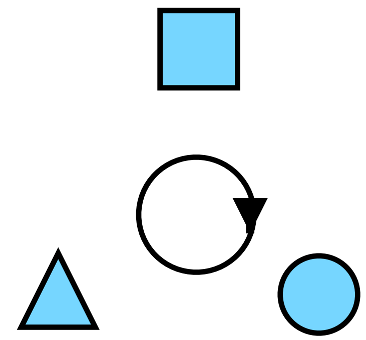
Yes.

Group Theory Example

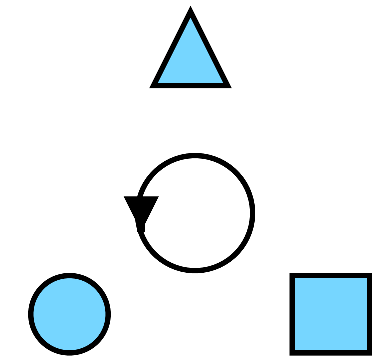
Permutations of 3 elements: Group S_3, $|S_3| = 6$



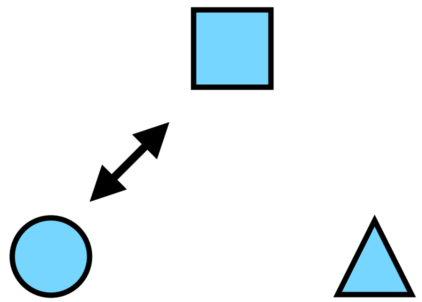
Identity e



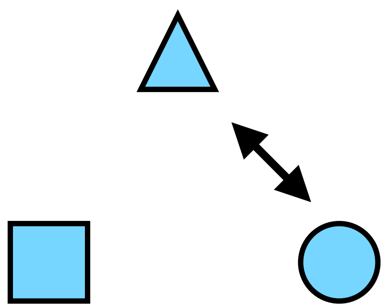
Rotate clockwise R



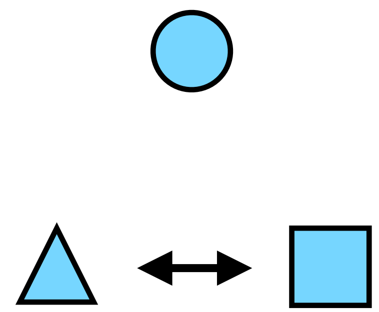
Rotate ccw $R^{-1} = R^2$



Swap left S_L



Swap right S_R



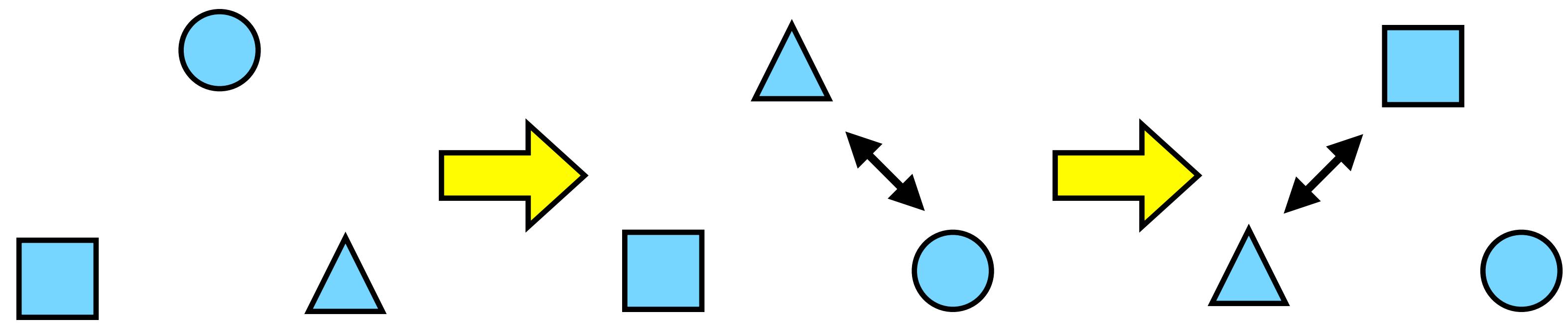
Swap bottom S_B

$S_3 = \{e, R, R^2, S_L, S_R, S_B\}$ with group operation composition.

Group Properties: Closure

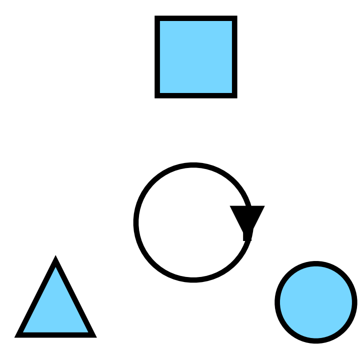
Closure: Product of two permutations is a permutation.

E.g.: $S_L S_R$ (acts from right)



Starting arrangement $\quad S_R \quad S_L$

=



$= R$

This class is being recorded

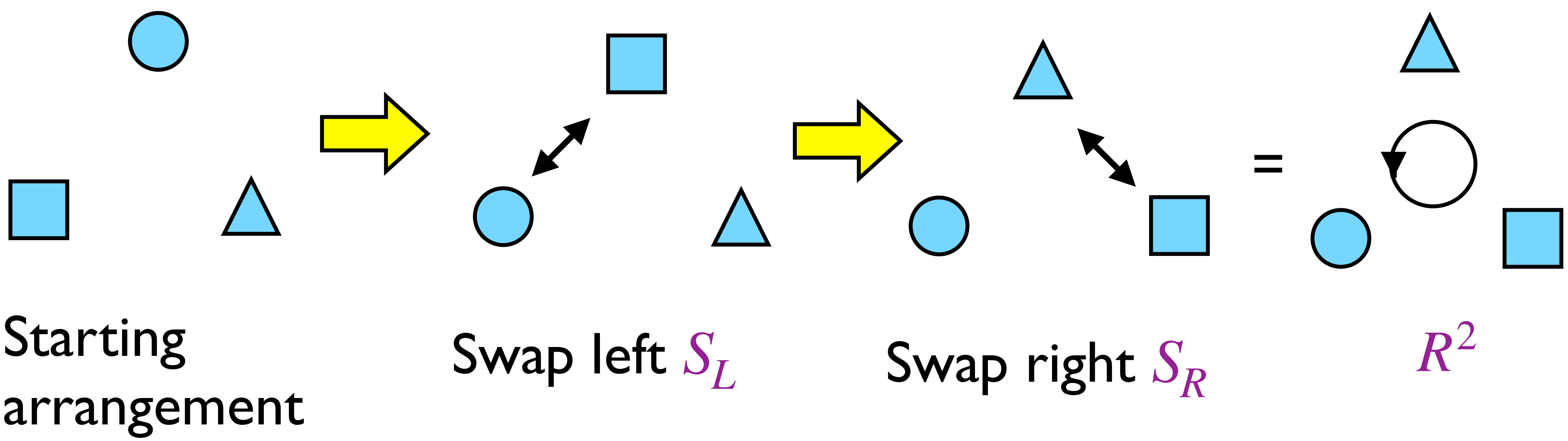
Group Properties: Others

Associativity: Can be checked but is automatic for composition of operations.

Identity: e is the identity element of the group. $e\sigma = \sigma$

Inverses: R and R^2 are inverses of each other. S_L, S_R, and S_B are inverses of themselves.

Non-abelian: $S_R S_L = R^2 \neq R = S_L S_R$



This class is being recorded

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

This class is being recorded

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

Examples:

The set of even integers forms a subgroup of $\mathbb{Z}$ under addition.

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

Examples:

The set of even integers forms a subgroup of $\mathbb{Z}$ under addition.

$\mathbb{Z}_5$ is not a subgroup of $\mathbb{Z}$ under addition: The addition operation is different, since in $\mathbb{Z}_5$, $3 + 3 = 1$, whereas in $\mathbb{Z}$, $3 + 3 = 6$.

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

Examples:

The set of even integers forms a subgroup of $\mathbb{Z}$ under addition.

$\mathbb{Z}_5$ is not a subgroup of $\mathbb{Z}$ under addition: The addition operation is different, since in $\mathbb{Z}_5$, $3 + 3 = 1$, whereas in $\mathbb{Z}$, $3 + 3 = 6$.

$\{0,2,4\}$ is a subgroup of $\mathbb{Z}_6$ under addition: Addition is closed, 0 is the identity, and -2 = 4.

Subgroups

Definition: H is a subgroup of G if $H \subseteq G$ and H is a group with the same group operation as G. We sometimes write $H \leq G$. The trivial subgroups of G are $\{e\}$ and G itself.

Examples:

The set of even integers forms a subgroup of $\mathbb{Z}$ under addition.

$\mathbb{Z}_5$ is not a subgroup of $\mathbb{Z}$ under addition: The addition operation is different, since in $\mathbb{Z}_5$, $3 + 3 = 1$, whereas in $\mathbb{Z}$, $3 + 3 = 6$.

$\{0,2,4\}$ is a subgroup of $\mathbb{Z}_6$ under addition: Addition is closed, 0 is the identity, and -2 = 4.

$\mathbb{Z}_6^*$ under multiplication is not a subgroup of $\mathbb{Z}_6$ under addition because it uses a different group operation.

Order of Groups and Subgroups

Definition: The order of a finite group G is written $|G|$ and is equal to the number of elements in G.

Examples:

$|\mathbb{Z}_5| = 5$ and $|\mathbb{Z}_5^*| = 4$.

$|\mathbb{Z}_6| = 6$

$|\{0,2,4\}| = 3$

$|\mathbb{Z}_6^*| = 2$ since $\mathbb{Z}_6^* = \{1,5\}$

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

This class is being recorded

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

This class is being recorded

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

Let $gH = \{gh \mid h \in H\}$.

(gH is known as a coset.)

This class is being recorded

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

Let $gH = \{gh \mid h \in H\}$.

(gH is known as a coset.)

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \varnothing$

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

Let $gH = \{gh | h \in H\}$.

(gH is known as a coset.)

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$

This means that the cosets don't overlap and that every element is in a coset (shared with other cosets that differ by multiplication by an element of the subgroup): a "partition."

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

Let $gH = \{gh \mid h \in H\}$.

(gH is known as a coset.)

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$

This means that the cosets don't overlap and that every element is in a coset (shared with other cosets that differ by multiplication by an element of the subgroup): a "partition."

Claim 3: $|gH| = |H|$

Lagrange's Theorem Proof

Lagrange's Theorem: If H and G are finite groups with $H \leq G$, then $|H|$ divides $|G|$.

Proof: For this proof, write the group operation as multiplication.

Let $gH = \{gh | h \in H\}$.

(gH is known as a coset.)

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \varnothing$

This means that the cosets don't overlap and that every element is in a coset (shared with other cosets that differ by multiplication by an element of the subgroup): a "partition."

Claim 3: $|gH| = |H|$

G is partitioned into cosets of size $|H|$, so $|H|$ divides $|G|$.

Proof of Claim 1

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$:

Proof of claim 1:

This class is being recorded

Proof of Claim 1

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$:

Proof of claim 1:

$g'H = \{gkh \,|\, h \in H\}$ but $kh \in H$ (by closure of H).

This class is being recorded

Proof of Claim 1

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$:

Proof of claim 1:

$g'H = \{gkh \mid h \in H\}$ but $kh \in H$ (by closure of H).

If $k \in H$, then $k^{-1} \in H$ (by the inverses property of H).

Proof of Claim 1

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$:

Proof of claim 1:

$g'H = \{gkh \,|\, h \in H\}$ but $kh \in H$ (by closure of H).

If $k \in H$, then $k^{-1} \in H$ (by the inverses property of H).

kh can take on *any* value $h' \in H$, when $h = k^{-1}h'$ (the product is in H by closure again). That is, as h runs over H for fixed k, kh runs over H as well.

Proof of Claim 1

Claim 1: If $g' = gk$ for $k \in H$, then $gH = g'H$:

Proof of claim 1:

$g'H = \{gkh \,|\, h \in H\}$ but $kh \in H$ (by closure of H).

If $k \in H$, then $k^{-1} \in H$ (by the inverses property of H).

kh can take on *any* value $h' \in H$, when $h = k^{-1}h'$ (the product is in H by closure again). That is, as h runs over H for fixed k, kh runs over H as well.

But that means that

$$g'H = \{gkh \,|\, h \in H\} = \{gh' \,|\, h' \in H\} = gH$$

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \varnothing$:

Proof of claim 2:

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \varnothing$:

Proof of claim 2:

Suppose $g' \neq gk$ but $gH \cap g'H \neq \varnothing$.
Then $\exists x \in gH \cap g'H$.

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$:

Proof of claim 2:

Suppose $g' \neq gk$ but $gH \cap g'H \neq \emptyset$.
Then $\exists x \in gH \cap g'H$.

But $k \in gH \cap g'H$ means $k = gh$ *and* $k = g'h'$ for some $h, h' \in H$.

This class is being recorded

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$:

Proof of claim 2:

Suppose $g' \neq gk$ but $gH \cap g'H \neq \emptyset$.
Then $\exists x \in gH \cap g'H$.

But $k \in gH \cap g'H$ means $k = gh$ *and* $k = g'h'$ for some $h, h' \in H$.

Thus, $g' = ghh'^{-1}$.

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$:

Proof of claim 2:

Suppose $g' \neq gk$ but $gH \cap g'H \neq \emptyset$.
Then $\exists x \in gH \cap g'H$.

But $k \in gH \cap g'H$ means $k = gh$ *and* $k = g'h'$ for some $h, h' \in H$.

Thus, $g' = ghh'^{-1}$.

But $k = hh'^{-1} \in H$ by the closure and inverses properties of H.

This class is being recorded

Proof of Claim 2

Claim 2: If $g' \neq gk$ for all $k \in H$, then $gH \cap g'H = \emptyset$:

Proof of claim 2:

Suppose $g' \neq gk$ but $gH \cap g'H \neq \emptyset$.
Then $\exists x \in gH \cap g'H$.

But $k \in gH \cap g'H$ means $k = gh$ *and* $k = g'h'$ for some $h, h' \in H$.

Thus, $g' = ghh'^{-1}$.

But $k = hh'^{-1} \in H$ by the closure and inverses properties of H.

This contradicts $g' \neq gk$ for $k \in H$. It must therefore be that $gH \cap g'H = \emptyset$.

Proof of Claim 3

Claim 3: $|gH| = |H|$

Proof of claim 3:

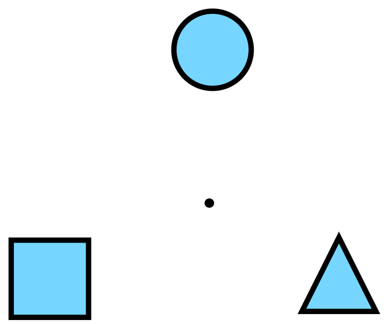
$gh = gh'$ iff $h = h'$ (multiply by g^{-1}).

Thus, $gH = \{gh | h \in H\}$ has exactly as many elements as H.

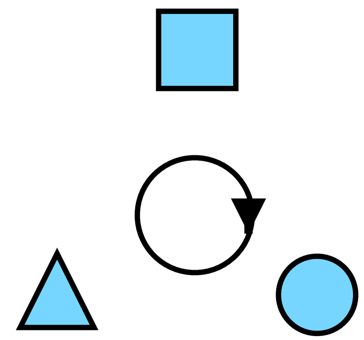
This class is being recorded

Subgroups of Permutation Group

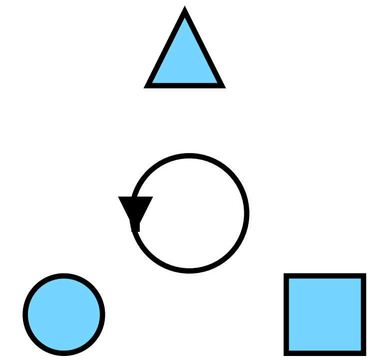
Order 3: Generated by R or by R^2.



Identity e

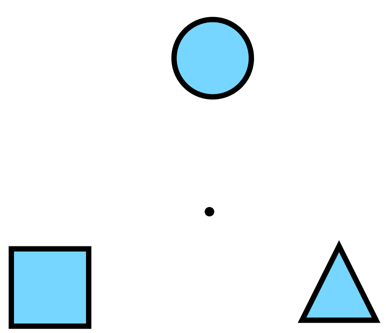


Rotate clockwise R

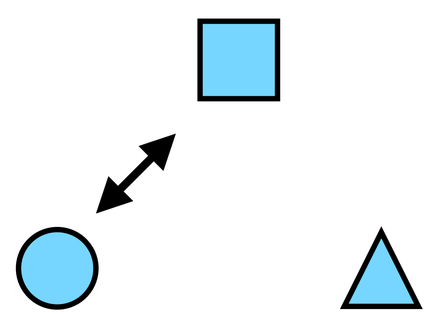


Rotate ccw $R^{-1} = R^2$

3 order 2 subgroups: For instance, generated by S_L.



Identity e



Swap left S_L

Note: Order of subgroups a factor of 6 (Lagrange’s thm.)

Generators and Cyclic Groups

Definition: Let G be a group. A set $S \subseteq G$ is a generating set for G if any element of G can be written as a finite product (under the group operation) of elements of S or inverses of elements of S, with repeats allowed. Note: S is a subset of G. It need not be a subgroup of G.

A group is cyclic if it has a generating set with just a single element.

Examples:

Generators and Cyclic Groups

Definition: Let G be a group. A set $S \subseteq G$ is a generating set for G if any element of G can be written as a finite product (under the group operation) of elements of S or inverses of elements of S, with repeats allowed. Note: S is a subset of G. It need not be a subgroup of G.

A group is cyclic if it has a generating set with just a single element.

Examples:

$\{1\}$ is a generating set for $\mathbb{Z}$, so $\mathbb{Z}$ is cyclic. (Under addition, since otherwise $\mathbb{Z}$ is not a group.)

Generators and Cyclic Groups

Definition: Let G be a group. A set $S \subseteq G$ is a generating set for G if any element of G can be written as a finite product (under the group operation) of elements of S or inverses of elements of S, with repeats allowed. Note: S is a subset of G. It need not be a subgroup of G.

A group is cyclic if it has a generating set with just a single element.

Examples:

$\{1\}$ is a generating set for $\mathbb{Z}$, so $\mathbb{Z}$ is cyclic. (Under addition, since otherwise $\mathbb{Z}$ is not a group.)

$\{2,3\}$ is also a generating set for $\mathbb{Z}$, as is any pair $\{a, b\}$ with gcd(a,b) = 1. Proof: Euclid's algorithm.

Generators and Cyclic Groups

Definition: Let G be a group. A set $S \subseteq G$ is a generating set for G if any element of G can be written as a finite product (under the group operation) of elements of S or inverses of elements of S, with repeats allowed. Note: S is a subset of G. It need not be a subgroup of G.

A group is cyclic if it has a generating set with just a single element.

Examples:

$\{1\}$ is a generating set for $\mathbb{Z}$, so $\mathbb{Z}$ is cyclic. (Under addition, since otherwise $\mathbb{Z}$ is not a group.)

$\{2,3\}$ is also a generating set for $\mathbb{Z}$, as is any pair $\{a, b\}$ with gcd(a,b) = 1. Proof: Euclid's algorithm.

$\{1\}$ is a generating set for $\mathbb{Z}_5$ (under addition), as is $\{a\}$ for any $a \neq 0$.

This class is being recorded

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

- $g^a g^b = g^{a+b}$, so $\langle g \rangle$ is closed under the group operation.

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

- $g^a g^b = g^{a+b}$, so $\langle g \rangle$ is closed under the group operation.
- $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$

This class is being recorded

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

- $g^a g^b = g^{a+b}$, so $\langle g \rangle$ is closed under the group operation.
- $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$
- $(g^a)^{-1} = (g^{-1})^a$, so $\langle g \rangle$ has inverses.

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

- $g^a g^b = g^{a+b}$, so $\langle g \rangle$ is closed under the group operation.
- $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$
- $(g^a)^{-1} = (g^{-1})^a$, so $\langle g \rangle$ has inverses.

By Lagrange's Theorem, $\mathrm{ord}(g) = |\langle g \rangle|$ divides $|\mathbb{Z}_N^*|$. This tells us the possible values of the order of g: the factors of $|\mathbb{Z}_N^*|$.

Cyclic Subgroups of $\mathbb{Z}_N^*$

Now let us consider the question: what are the possible orders of a number under modular exponentiation?

Let $g \in \mathbb{Z}_N^*$ and define $\langle g \rangle = \{g^a \in \mathbb{Z}_N^*\}$. $\langle g \rangle$ is the cyclic subgroup of $\mathbb{Z}_N^*$ generated by g.

Why is $\langle g \rangle$ a subgroup?

- $g^a g^b = g^{a+b}$, so $\langle g \rangle$ is closed under the group operation.
- $g \cdot g^{\mathrm{ord}(g)-1} = 1$, so $g^{-1} = g^{\mathrm{ord}(g)-1} \in \langle g \rangle$
- $(g^a)^{-1} = (g^{-1})^a$, so $\langle g \rangle$ has inverses.

By Lagrange's Theorem, $\mathrm{ord}(g) = |\langle g \rangle|$ divides $|\mathbb{Z}_N^*|$. This tells us the possible values of the order of g: the factors of $|\mathbb{Z}_N^*|$.

What is $|\mathbb{Z}_N^*|$?