21-373

8/31/20

$A \times B = \{ (a,b) \mid a \in A, b \in B \}$

a relation $R \subseteq A \times B$

R is a function from A to B if

(1) $R \subseteq A \times B$

(2) $\forall a \in A, \exists b \in B$ s.t. $(a,b) \in R$

(3) $\forall a \in A, \forall b_1, b_2 \in B$,
if $(a_1,b_1), (a_2,b_2) \in R$ then $b_1 = b_2$.

notation: $R: A \to B$

we can write $b = R(a)$ given $R: A \to B$, instead of $(a,b) \in R$.

Ex. If $R \subseteq A \times B$ satisfies (2), prove "R is well-defined" means to establish (3)

$f: A \to B$, $g: B \to C$. $h := g \circ f$, $h: A \to C$.

$h(a) = g(f(a))$.

Surjective

Injective

Bijective

For $f: A \to B$, $g: B \to C$. If both f and g are injective then $g \circ f$ is also injective.

image $B^* := f(A)$ $\quad B^* \to A$

If $f: A \to B$ is injective, f^{-1} is also a function. bijective → bijective.

$f: A \to A$ bijective → $f^{-1}: A \to A$ bijective.

If $f: A \to B$, $g: B \to C$ bijections, then $g \circ f$ is a bijection.

If f, g are bijections of A onto A then also $f \circ g$ and $g \circ f$ are both bijections.

$f: A \to B$ bijection: Permutation (e.g. $A = \mathbb{R}$, $f(x) := x+1$).

$f(x) = x^2$ is not a permutation of $\mathbb{R}$, not surjective or injective.

(Associativity) $f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$

Conclusion. Given a fixed set A ($\neq \emptyset$),

(1) $f, g \in S(A) \Rightarrow f \circ g \in S(A)$

(2) $f \in S(A) \Rightarrow f^{-1} \in S(A)$

[Let $S(A) = \{ f \mid f$ permutation of $A \}$]

(3) $f_1, f_2, f_3 \in S(A) \Rightarrow (f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$

(4) id_A identity function. $\forall f \in S(A)$, $f \circ id_A = id_A \circ f = f$

(2') $f \circ f^{-1} = id_A = f^{-1} \circ f$

"Group"

Evariste Galois (1811-1832)

(Abel)

motivation. $ax^5 + \dots = 0$

Galois Group { degrees (3, 6, 7 ...) impossible to find precise formula)

Pf idea. Sub-fields, Complex numbers.

Artin, Noether — redefine as "Abstract Algebra"

$X \overset{\text{function}}{\rightarrow} Y$

$X/\sim \rightarrow Y/\sim$

Check that $g(x) \sim g(x')$ whenever $x \sim x'$.

21-373 9/2/20

Let A be a set. $E \subseteq A \times A$ is an equivalence relation, provided

Reflexive $\forall a \in A,\ (a,a) \in E$

Symmetric $\forall a,b \in A,\ (a,b) \in E \Rightarrow (b,a) \in E$

Transitivity $\forall a,b,c \in A\ \ (a,b) \in E \wedge (b,c) \in E \Rightarrow (a,c) \in E$

"Trivial" example: equality

Def. For $x, y \in \mathbb{Z} - \{0\}$, $x \mid y \iff \exists n \in \mathbb{Z}$ s.t. $y = n \cdot x$

Lemma. $x_1 \mid x_2 \wedge x_2 \mid x_3$ (for $x_1, x_2, x_3 \in \mathbb{Z} - \{0\}$) $\Rightarrow x_1 \mid x_3$

If $x \mid y \wedge x \mid z$ then $x \mid (ay + bz)\ \forall a,b \in \mathbb{Z}$

Def (Gauss) $a \equiv b \bmod n \iff n \mid (b-a)$, $n \geq 2$

Given $n \geq 1$, $a \equiv b \bmod n$ is an equivalence relation on $\mathbb{Z}$.

Let A be a set and $F = \{S_i \mid i \in I\}$ family of subsets of A. F is a partition of A provided

Equiv) Partition (1) $A = \bigcup_{i \in I} S_i$

(2) $i \neq j \in I \Rightarrow S_i \cap S_j = \emptyset$

Let E be an equivalence relation on A. For $a \in A$, $[a] := \{y \in A \mid (a,y) \in E\}$

Remark. (1) By reflexivity, $a \in [a]\ \forall a \in A$.

(2) Given $a,b \in A$, $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$ contrapositive

proving double containment

Corollary. If E is an equivalence relation on A, then $\{[a] \mid a \in A\}$ is a partition.

Theorem A If A is a set, E is an eq relation on A, then $\{[a] : a \in A\}$ is a partition of A.

Theorem 13

Suppose $P := \{S_i \mid i \in I\}$ is a partition of A.

Let $E := \{(a,b) \in A \times A \mid \exists\, i \in I \text{ s.t. } a \in S_i \wedge b \in S_i\}$

Then E is an eq relation.

$$E \xrightarrow{A} F_E \xrightarrow{B} E(F_E) \quad \text{if } E = E_{(F_E)}$$

$$F \xrightarrow{B} E_F \xrightarrow{A} F(E_F)$$

Let $A = \mathbb{Z}$, $n \geq 2$, (integer). Consider $E = \{(a,b) \mid a \equiv b \bmod n\}$.

$[k] := \{l \cdot n + k \mid l \in \mathbb{Z}\}$, $0 \leq k < n$.

$\bar{0} = [0] = \{ln \mid l \in \mathbb{Z}\}$

$\bar{1} = [1] = \{ln+1 \mid l \in \mathbb{Z}\}$

call a finite set!

$\overline{n-1}$ $[n-1] = \{ln + (n-1) \mid l \in \mathbb{Z}\}$

↓

Congruent classes of n. $\{[k] : 0 \leq k < n\} = \mathbb{Z}/n\mathbb{Z}$.

Finite v Infinite Groups.

Fact. Suppose $P = \{S_i \mid i \in I\}$ a partition of a finite set A.

Application: Cardinality Then $|A| = \sum_{i \in I} |S_i|$.

(modular multiplication / division) behave nicely in $\mathbb{Z}/n\mathbb{Z}$ (recall 15-251).

$\{F, +, 0\}$ are both groups
$\{F-\{0\}, \cdot, 1\}$

A field is a sequence (tuple) $\langle F, +, \cdot, 0, 1 \rangle$ when

F is non-empty set $\quad 0 \neq 1 \in F$ (two elements of the set)

(a) $\forall a \forall b \forall c \quad [a+(b+c) = (a+b)+c]$ associativity
$[a \cdot (b \cdot c) = (a \cdot b) \cdot c]$

$+ : F \times F \to F$ and $\cdot : F \times F \to F$

addition multiplication

(b) $\forall a, \exists b \; [a+b=0]$

(b') $(\forall a \in F - \{0\}) \exists b$. s.t $[a \cdot b = 1]$

(c) $\forall a \; [a+0=a]$

(c') $\forall a \; [a \cdot 1 = a]$

(d) $\forall a \forall b, \; [a+b = b+a]$, $\wedge [a \cdot b = b \cdot a]$ Commutativity

* (e) $\forall a \forall b \forall c, \; [a \cdot (b+c) = a \cdot b + a \cdot c]$ distributivity

(reason why 2 groups don't automatically make a field)

Example, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (with usual $+, \cdot$) are fields

(2) $\mathbb{Z}$ is not a field. b' fails.

(3) When $n \geq 2$ $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot, \bar{0}, \bar{1})$ is a field $\Leftrightarrow$ n is a prime number else fails b'.

Group $\langle G, \cdot, 1_G \rangle$, $1 \in G$ identity, such that

$\cdot : G \times G \to G$, $\forall^{(iv)}$ a, b $\in G$, $a \cdot b \in G$.

e.g. bijections

(i) associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) $\forall a \; [a \cdot 1 = 1 \cdot a = a]$

(iii) $\forall a \; \exists b \; [a \cdot b = 1 \wedge b \cdot a = 1]$.

gcd of a,b denoted by $d=(a,b)$ or $d=\gcd(a,b)$ is defined such that

(1) $d \mid a \wedge d \mid b$

(2) $\forall\, c \in \mathbb{N}-\{0\}$ if $c \mid a \wedge c \mid b$, then $c \mid d$

Euclidean Algorithm

Fact $\forall\, a,b \in \mathbb{N}-\{0\}$, $\exists\, d \in \mathbb{N}, \exists\, x,y \in \mathbb{Z}$ s.t.
$d = ax+by$, and $d=\gcd(a,b)$

Idea of Proof Using well-ordering principle ($\forall\, S \subseteq \mathbb{N}$ if $S \neq \emptyset$ then $\exists\, m \in S$ minimal)

Consider $S := \{ax+by \mid x,y \in \mathbb{Z}\} \cap \mathbb{N}$

Let $d = \min S$, take $x_0, y_0 \in \mathbb{Z}$ s.t. $d = ax_0+by_0$ is GCD.

Claim: $\forall\, n \in S$, $d \mid n$ (since $a,b \in S$),

Pf: If $d \nmid n$, $n \equiv k \bmod d$, $k < d$. But $k = d - ax' - bx'$, so $k < d$ implies that d is not $\min S$. contradiction.

Then d is the gcd.

Special case: Given $a,b \in \mathbb{N}-\{0\}$, if $(a,b)=1$, we say (a,b) are relatively prime.

Then there exists $x,y \in \mathbb{Z}$ s.t. $ax+by=1$.

Euclid's Lemma: Let $a,b \in \mathbb{N}-\{0\}$, p a prime number.

If $p \mid ab$ then $p \mid a \vee p \mid b$. (contrap. $p \nmid a \wedge p \nmid b \to p \nmid ab$)

Pf. Case 1: $p \mid a$. we are done

2: $p \nmid a$. Since p is prime, we have $(p,a)=1$.

$\exists\, x,y \in \mathbb{Z}$ st $px+ay=1$.

Then $b(px+ay)=b$

$bpx + \underbrace{aby}_{p \mid ab} = b \Rightarrow \therefore$ LHS $\equiv$ RHS $\equiv 0 \bmod p$

$p \mid b$.

Most important example of a group:

$S_1, S_2 \ldots$

For $X \neq \emptyset$ set, $S(X)$ the set of permutations of X,

$(S(X), \circ, id_X)$ is a group.

$\circ$: composition.

$= \{a \in \mathbb{Q} \mid a \neq 0\}$

$(\mathbb{Q}, +, 0), (\mathbb{Q}^\times, \cdot, 1), (F, +, 0), (F^\times, \cdot, 1)$ where F is a field.

$n \geq 1$ $(\mathbb{Z}/n\mathbb{Z}, +, \bar{0})$ is a group.

Def. A group G is called Abelian (commutative) provided $\forall x, y \in G,\ x \cdot y = y \cdot x$.

Abelian Group

* When X is a set with ≥ 3 elements, then $(S(X), \circ, id_X)$ is not commutative.

"symmetric group on X"

When $X = \{1, 2, \ldots n\}$, then $S(X) = S_n$.

Def Subgroups

Suppose $(G, \circ, 1_G)$ is a group. $H \subseteq G$ is a subgroup of G provided $(H, \circ, 1_G)$ is also a group.

Notation: $H \leq G$.

$H \lneq G$: proper subgroup ($H \leq G$ and $H \neq G$)

Examples. (1) $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$

(2) $(\mathbb{Z}/n\mathbb{Z}, \bar{0}, +)$

(3) $n \in \mathbb{Z}$, $(n\mathbb{Z}, +, 0) \leq (\mathbb{Z}, +, 0)$

Proof. → Associativity ✓

→ $x = n \cdot k_x$ $y = n \cdot k_y$

$x \pm y = nk_x \pm nk_y = n(k_x \pm k_y) = nk' \in n\mathbb{Z}$

→ identity. → inverse?

"infinite subgroups"

Cor. $(2^n\mathbb{Z}, +, 0) \leq (4\mathbb{Z}, +, 0) \leq (2\mathbb{Z}, +, 0) \lneq (\mathbb{Z}, +, 0)$

eq. class of 0, under relation $\equiv \bmod 2$

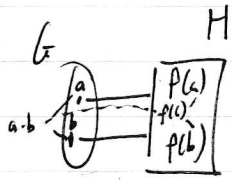
• the set of $n \times n$ invertible matrices together with the operation of matrix operation

Let $(G, \cdot, 1_G)$ and $(H, \circ, 1_H)$ be groups.

$f: G \to H$ is called an isomorphism from G to H provided:

$\forall a, b \in G$, (1) $f(a) \circ f(b) = f(a \cdot b)$

(2) f is a bijection.



~ Graph isomorphism. ? Same adjacency matrix up to permutations of the rows/columns

Notation: When f is an isomorphism from G to H, we write

$f: G \overset{\text{(Isomorphism)}}{\cong} H$ ($G \cong H \Leftrightarrow (\exists f: G \cong H)$)

lemma: $\cong$ an equivalence relation on groups.

(1) $G \cong G$

Isomorphism generates eq. classes

Symmetric (2) $f: G \cong H \Rightarrow f^{-1}: H \cong G$?

Transitivity (3) $f: G_1 \cong G_2$, $h: G_2 \cong G_3$ then $h \circ f: G_1 \cong G_3$

wts $(f^{-1}(A) \cdot f^{-1}(B) = f^{-1}(A \circ B)$

let $A = f(a)$, $B = f(b)$.

LHS $= f^{-1}(A) \cdot f^{-1}(B) = a \cdot b = f^{-1}(f(a \cdot b))$

$= f^{-1}(f(a) \circ f(b))$

wts: $h(f(a)) \circ h(f(b)) = h(f(a \cdot b))$ $f^{-1}(A \circ B) = \text{RHS}$ ✓

: bijection ✓

Allows us to 'translate' problems.

non-isomorphism. G not isomorphic to $H \Leftrightarrow \neg[G \cong H]$

→ if h is a bijection, $\exists a, b \in G$, s.t $f(a \cdot b) \neq f(a) \cdot f(b)$

→ "Some algebraic property is true in G but false in H"

Eg: If G is Abelian and H is not Abelian, $G \ncong H$.

21-373 9/9/2020

Def. Let G, H be groups $(G, *, 1_G)$, $(H, \circ, 1_H)$.

Isomorphism

$f: G \to H$ is an isomorphism provided

(1) f is bijective.

(2) $f(a * b) = f(a) \circ f(b)$, $\forall a, b \in G$. "order of operations doesn't matter"

Denote this by $f: G \cong H$.

Exs.

(1) $G \cong G$ reflexive

(2) $G \cong H \Rightarrow H \cong G$ commutative

(3) $G_1 \cong G_2 \wedge G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ transitive

Suppose $G \cong H$. If G is abelian then H is abelian. ✗

Pf. Given $a, b \in H$, WTS $a \cdot_H b = b \cdot_H a$. Since f is surjective, $\exists\, a_1, b_1 \in G$ s.t.

$f(a_1) = a$ and $f(b_1) = b$. Then $a \cdot_H b = f(a_1) \cdot_H f(b_1)$

$= f(a_1 \cdot_G b_1)$

$= f(b_1 \cdot_G a_1)$ ← know G is abelian

$= f(b_1) \cdot_H f(a_1) = b \cdot_H a$

So $\forall a, b \in H$ we have $a \cdot_H b = b \cdot_H a$.

Homomorphism

$f(a \cdot_G b) = f(a) \cdot_H f(b)$

Homomorphism: Example in Linear Algebra.

GL = General Linear.

$\det: GL(n, \mathbb{R}) \to (\mathbb{R} - \{0\}, \cdot)$ is a homomorphism.

GL, SL

Fact. For A, B $n \times n$ matrices, $\det(A \cdot B) = \det(A) \cdot \det(B)$

$M_n(\mathbb{R}) = \{A \mid A \text{ is } n \times n \text{ matrix}/\mathbb{R}\}$

$GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$

If A is invertible, $\det(A^{-1}) = \det(A)^{-1}$.

$GL(n, \mathbb{R})$, I_n is a group when $I = (1_{ij})$.

But even for $n = 2$, the group is not commutative.

$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

We note that if G, H are groups and $f: G \to H$ surjective homomorphism,
G is abelian $\Rightarrow$ H is abelian. (no need for isomorphism)

Q. Is the converse true? (H abelian $\Rightarrow$ G abelian?)

A. No, the determinant function suffices as counter-example.

Eg. Let $H := \langle \mathbb{R}-\{0\}, \cdot \rangle$ and $G = GL(n, \mathbb{R})$ $(n \geq 2)$.

$\det(A \cdot B) = \det(A) \cdot \det(B)$ is surjective homomorphism.

$\det$ is surjective. for $x \in \mathbb{R}$, $\det \begin{pmatrix} \sqrt[n]{x} & & & \\ & \sqrt[n]{x} & & \\ & & \ddots & \\ & & & \sqrt[n]{x} \end{pmatrix} = x$.

—If we want to show "iff abelian", we need to work with isomorphic groups.

Def. Let G be a group. $a \in G$ is identity, provided $(\forall x \in G)\ x \cdot a = a \cdot x = x$.

$\forall x \exists y \ [x \cdot y = y \cdot x = a]$. This identity is unique. $(a = a \cdot b = b)$

Def. suppose B, C are candidates for inverse of A
$C \cdot A = A \cdot C = B \cdot A = A \cdot B = I$.

$B \cdot (A \cdot C) = B \cdot A \cdot C = I \cdot C = C$

21-373 9/11/2020

Subgroups recap.

Examples: ① $(\mathbb{Z},+,0) \leq (\mathbb{Q},+,0) \leq (\mathbb{R},+,0) \leq (\mathbb{C},+,0)$

② Suppose V is a F-vector space (F a fixed field)

W is a subspace of V (closed under addition and scalar multiplication)

$(W,+) \leq (V,+)$

③ $GL(n,F) := \{A \mid A \text{ is } n\times n \text{ matrix with elements from } F,\ \det A \neq 0\}$ — not abelian!

$SL(n,F) := \{A \in GL(n,F) \mid \det A = 1\}$ — Special Linear

Claim: $SL(n,F) \leq GL(n,F)$.

Clearly $\circ$ is associative.

consider $A, B \in SL(n,F)$.

$\det(A \circ B) \overset{\text{fact}}{=} \det A \cdot \det B = 1 \cdot 1 = 1$. Hence $A \circ B \in SL$.

$I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in SL(n,F)$.

$A \in SL(n,F)$. $\det(A^{-1}) = \frac{1}{\det(A)} = 1^{-1} = 1$, Hence A^{-1} is the inverse of A.

Q. Can we describe the subgroups of $(\mathbb{Z},+,0)$?

('lattice') $(2^{n+1}\mathbb{Z},+) \leq (2^n\mathbb{Z},+) \leq \cdots \leq (\mathbb{Z},+)$

Each subgroup is an equivalence class

Note. $\forall n \in \mathbb{Z}$, $(n\mathbb{Z},+) \cong (\mathbb{Z},+)$, $\forall n \in \mathbb{Z}-\{0\}$ [isomorphism]

Let $f(x) := n \cdot x$.

- Observe $f(x+y) = n(x+y) \overset{\text{distributive}}{=} n\cdot x + n\cdot y = f(x)+f(y)$
- (bijective) $f(x) = f(y)$

injective $\Downarrow$

$nx = ny$, $n(x-y) = 0$, $x = y$.

surjective ✓ $k \in n\mathbb{Z} \Rightarrow \frac{k}{n} \in \mathbb{Z}$.

(aside: $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $\bar{1}+\bar{1}=\bar{0}$.
But $|1|$ (in $\mathbb{Z}$) is $2 \nmid 1$, $2 \mid 0$.)

Q. Is there $H \leq \mathbb{Z}$ s.t. there is no $n \in \mathbb{Z}$ s.t. $H = n\mathbb{Z}$?

If not, we conclude $\forall H \leq \mathbb{Z}$ then $\exists n \in \mathbb{Z}$ s.t. $H = n\mathbb{Z}$.

Pf. H must contain positive numbers.

$0 \circlearrowright 0$ keep having multiples of n!
(and nothing else)

Lemma. Let G be a group, $H \subseteq G$. TFAE:

(Characterization of subgroups)

(1) $H \leq G$

(2) $H \neq \emptyset$ and $x, y \in H \Rightarrow x \cdot y \in H$, $x \in H \Rightarrow x^{-1} \in H$

(3) $H \neq \emptyset$ and $x, y \in H \Rightarrow x \cdot y^{-1} \in H$. [most elegant]

('Subgroup Criterion')

(1) $\Rightarrow$ (2) By definition

(2) $\Rightarrow$ (3) Given $x, y \in H$, using (2) we get $y^{-1} \in H$.

Using (2) again, $x, y^{-1} \in H \Rightarrow x \cdot y^{-1} \in H$

(3) $\Rightarrow$ (1) Associativity ✓

Let $y = x$. Then $x \cdot x^{-1} \in H \Rightarrow 1 \in H$.

Claim: (of inverse) $x \in H \Rightarrow 1 \cdot x^{-1} \in H \Rightarrow x^{-1} \in H$.

(of operation) $x \cdot \underbrace{(y^{-1})^{-1}}_{\text{inverse of } y \text{ exists by the claim}} \in H \Rightarrow x \cdot y \in H$.

21-373

Example. For $n \in \mathbb{Z}$, $H := n\mathbb{Z}$ $(= \{n \cdot k \mid k \in \mathbb{Z}\})$ we have $H \leq (\mathbb{Z}, +, 0)$.

Recall $x \equiv y \bmod n$ is an eq. relation on $\mathbb{Z}$, its eq classes are $[0], \dots [n-1]$, where $[l] = \{nk + l \mid k \in \mathbb{Z}\}$, $0 \leq l < n$.

$[0]$	$[1]$		$[2]$	...	$[n-1]$

where $[0] = n\mathbb{Z}$ $(:= H)$

* H is a subgroup

Def. Suppose G is a group, $H \leq G$. Let $x \sim_H y$ denote $x \cdot y^{-1} \in H$.

For every $x, y \in G$, if G, H as above, then $x \sim_H y$ is an equivalence relation on G.

Subgroups and Equivalence Classes

Reflexivity. Given $x \in G$, $x \cdot x^{-1} = 1 \in H$. (2)

Symmetry. Given $x, y \in G$, suppose $x \sim_H y$, WTS $y \sim_H x$.
From $x \sim_H y$ we have $\underbrace{x \cdot y^{-1}}_{a} \in H$. (3)

Since $a \in H \Rightarrow a^{-1} \in H$ for all $a \in H$, we get $(xy^{-1})^{-1} \in H$

$(xy^{-1})^{-1} = (yx^{-1}) \in H \Rightarrow y \sim_H x$ def.
$(y^{-1})^{-1} = y$, uniqueness of inverse

Transitivity. Suppose $x \sim_H y$ and $y \sim_H z$.

$\underbrace{xy^{-1}}_{a} \in H$ and $\underbrace{yz^{-1}}_{b} \in H \Rightarrow a \cdot b \in H$

$\Rightarrow (xy^{-1})(yz^{-1}) \in H$

$\overset{\text{Assoc.}}{\Rightarrow} x \cdot (y^{-1}y) z^{-1} = xz^{-1} \in H.$

Given $H \leq G$ we proved $\sim_H$ is eq relation on G.
What are the equivalence classes of $\sim_H$? i.e. Find $[x]_H$.

In the example $H = n\mathbb{Z} \leq \mathbb{Z}^{(+)}$, $x \sim_H y \iff x + (-y) \in H \iff x - y \in n\mathbb{Z}$
$\iff x \equiv y \bmod n$.

(Also recall that $SL(2,F) \leq GL(2,F)$)

Suppose $x, y \in G$ and $x \cdot y^{-1} \in H$. ~~There is $h \in H$ s.t $xy^{-1} = h$~~

~~Then $xy^{-1} \cdot y = hy \Rightarrow x = hy$ for some $y \in G$.~~

note that $y \in [x]_H \Rightarrow$ we have $x \sim_H y \Rightarrow x \cdot y^{-1} \in H$

$\Rightarrow \exists\, h \in H$ s.t $x \cdot y^{-1} = h$ mult by x^{-1} from left

Subgroups → cosets

$$x^{-1} x y^{-1} = x^{-1} h \Rightarrow y^{-1} = x^{-1} h$$

$$\Rightarrow (y^{-1})^{-1} = (x^{-1} h)^{-1}$$

$y = h^{-1} x$, there is $h_1 \in H$ s.t $y = h_1 x$.

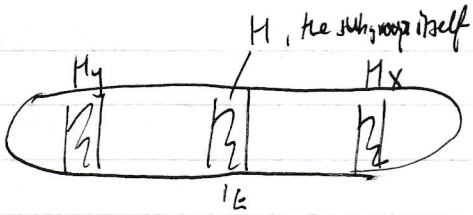
→ exercise: show distinct right cosets have empty intersection

$[x]_{\sim} = \{h_1 x : h_1 \in H\} = Hx$ (the right coset of x) 'attach' to a particular x

Note that $\forall h_2 \in H$ $x \sim_H h_2 x$. $x \cdot (h_2 x)^{-1} \in H$

$\iff x \cdot x^{-1} h_2^{-1} = h_2^{-1} = h_3 \in H$.

Given H



'partition!

$[1_G]_{\sim_H}$. This is $H \cdot 1_G = \{h \cdot 1 \mid h \in H\} = H$.

21-373

Recall. Suppose E is an equivalence relation (Subgroup) on a set S.

$$x \in S \Rightarrow [x]_E := \{y \in S \mid x \sim y\}.$$

(Partitioning) Fact. $\forall x_1, x_2 \in S$, if $[x_1] \cap [x_2] \neq \emptyset$ then $[x_1] = [x_2]$.

As $Hx = [x] \cap H$. If $H \leq G$, $x, y \in G$, $Hx \cap Hy \neq 0 \Rightarrow Hx = Hy$.

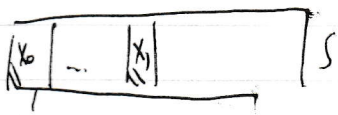
Now, Suppose E is an equivalence relation on S. We have that $S = \bigcup_{x \in S} [x]_E$.

Fact ① $x \in S \underset{\text{reflexivity}}{\Rightarrow} x \in [x]_E$

② We can find $S^* \subseteq S$ s.t.

$$S = \bigcup_{x \in S^*} [x]_E, \text{ and } x_1 \neq x_2 \in S^* \Rightarrow [x_1] \cap [x_2] = \emptyset.$$

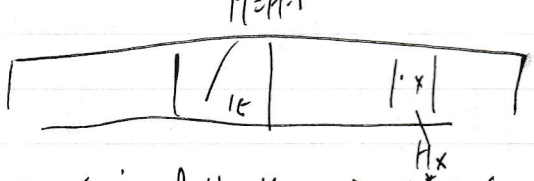
Proof of ②. For S finite: "Algorithm". Pick $x_0 \in S$.



[representative] Pick $x_1 \in S - [x_0]$. Pick $x_2 \in S - ([x_0] \cup [x_1])$

$\vdots$

$S^* = \{x_0, x_1, x_2 \cdots x_n\}$ "one representative each."



When G is finite, there is $G^* \subseteq G$ s.t.

$$G = \bigcup_{x \in G^*} Hx \text{ and } x_1 \neq x_2 \in G^* \Rightarrow Hx_1 \cap Hx_2 = \emptyset$$

$$|G| = \sum_{x \in G^*} |Hx|.$$

mentoring@cmu.edu

(from Fact) Cor 1. $|S| = \sum_{i=1}^{n} |[x_i]|$

Theorem. If $H \leq G$, G is finite group then $\exists\, g_1, g_2 \cdots \in$

s.t. $\in = \bigcup_{i=1}^{n} Hg_i$, $i \neq j \Rightarrow Hg_i \cap Hg_j = \emptyset$.

Pf. Apply Fact when $S \leftarrow \in$, E is $\sim_H$ ㅁ.

Cor 2. $|\in| = \sum_{i=1}^{n} |Hg_i|$. (Thm + Cor 1)

(Theorem + Cor 1)

Cor 3. (Lagrange) Suppose G is a finite group.
If $H \leq \in$ then $|H| \mid |G|$

Pf.

Lemma. If $H \leq G$, $x \in G$ then $|H| = |Hx|$.

Pf. Consider $f: H \to Hx$ given by $f(h) := h \cdot x$.

f is clearly surjective.

$f(h_1) = f(h_2) \Rightarrow h_1 x = h_2 x$

$\Rightarrow h_1 x x^{-1} = h_2 x x^{-1}$

$\Rightarrow h_1 = h_2$. $\therefore$ injective.

Then since $|\in| = \sum_{i=1}^{n} |Hg_i|$, when $i \neq j \Rightarrow Hg_i \cap Hg_j \neq \emptyset$,

$\sum_{i=1}^{n} |Hg_i| = \sum_{i=1}^{n} |H| = n \cdot |H|$

$\Rightarrow |G| = n \cdot |H|$

Suppose $H \leq \in$ the index of H in $\in$ is $[\in : H] = |\{gH : g \in G\}|$.

In other words, if $H \leq \in$ then $|\in| = [G : H] \cdot |H|$

p35: $|LC| = |RC|$

21-373

let $n:=[G:H]$ Pick $g_1 \dots g_n$.

$1 \le i \ne j \le n \Rightarrow Hg_i \ne Hg_j$.

Since $Hg_i = [g_i]_{\sim H}$, being distinct implies being disjoint.

$Hg_i \cap Hg_j = \emptyset$.

Let G be a group. Then the center (element) of G is

$$Z(G) := \{h \in G \mid (\forall g \in G)\ gh = hg\}$$

(1) Always $1_G \in Z(G)$.

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

$$\{1_G\} \subseteq Z(G) \subseteq G$$

Center is subgroup

Thm. $Z(G) \le G$.

Proof. $Z(G)$ is not empty since $1_G \in Z(G)$.

Suppose $x \in Z(G)$, $(\forall g \in G)\ gx = xg$.

right x^{-1} multiply $(\forall g \in G)\ (gx)x^{-1} = (xg)x^{-1}$

$x \in Z(G) \to x^{-1} \in Z(G)$

$g = xgx^{-1}$.

$x^{-1}g = x^{-1}xgx^{-1}$

$x^{-1}g = gx^{-1} \Rightarrow x^{-1} \in Z(G)$

$x, y \in Z(G) \to xy \in Z(G)$

- Suppose $x, y \in Z(G)$. W.T.S $xy \in Z(G)$.

know: $(\forall g \in G)\ gx = xg$. $(\forall h \in G)\ hy = yh$

$x \in Z(G)$

$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$

(assoc; $y \in Z(G)$)

$\therefore xy \in Z(G)$

S_4, S_5: $\{1\} \subsetneq Z(G) \subsetneq G$

Def. Let G be a group, $A \subseteq G$, the centralizer of A is

$$C_G(A) = \{g \in G \mid (\forall h \in A) gh = hg\}$$

→ When $A = G$, $C_G(G) = Z(G)$

→ $A = \{1_G\}$ $C_G(A) = G$.

$A \subseteq B \subseteq G \rightarrow C_G(B) \subseteq C_G(A)$

If it commutes all elements of B, it commutes all elements of A.

21-373 9/18/2020

(centralizer of set ⊆ subgroup)

lemma Let G be a group. If $A \subseteq G$ then $C_G(A) \leq G$.

Proof. show $C_G(A) \neq \emptyset$. Verify that $1_G \in C_G(A)$ ✓

~~Enough to show if $x, y \in C_G(A]$ then $x \cdot y^{-1} \in C_G(A)$.~~

Alternatively

- Let $x, y \in C_G(A)$, $h \in A$ be given

want to show $(xy^{-1})h = h(xy^{-1})$.

directly:
$xh = hx$
$yh = hy$
$h = y^{-1}hy$
$hy^{-1} = y^{-1}h$
$(xy^{-1})h = x(y^{-1}h) = xHy^{-1}$
$= (hx)y^{-1}$
$= h(xy^{-1})$.

(1) Closure under inverse

Since $y \in C_G(A)$, $yh = hy$

$y^{-1}(yh)y^{-1} = y^{-1}(hyy^{-1})$

$(y^{-1}y)hy^{-1} = y^{-1}h(yy^{-1})$

$hy^{-1} = y^{-1}h$

$\rightarrow y^{-1} \in C_G(A)$

(2) Closure under composition

Show $x, y \in C_G(A) \Rightarrow xy \in C_G(A)$. For every $h \in A$,

$(xy)h = h(xy)$.

$(xy)h = x(yh) = x(hy) = xh \cdot y = (hx)y = h(xy)$
($y \in C_G(A)$)

"Non-trivial subgroups": Except $\{1_G\}$ and G.

Claim. If G has 7 elements, then all subgroups of G as trivial.

→ Corollary from Lagrange Theorem. If G is finite, $|G|$ is a prime number, then the subgroups of G are $\{1_G\}$ and G.

Example: $(\mathbb{Z}/p\mathbb{Z}, \oplus)$.

(G is abelian)

Note. if $|G|$ is prime then $G = Z(G)$. Furthermore $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof: We prove that G is cyclic. Take $a \in G$, $a \neq 1_G$. $\langle a \rangle = \{1_G\}$ or $\{G\}$

Let a be such $\varphi(g) = [k]$.
where $|a| = |G|$.

Def. Suppose G is a group. G is a cyclic if there exists $a \in G$, s.t. $G = \{a^n \mid n \in \mathbb{Z}\}$.

Let the generator of G be a. Then $a^0 = 1_G$. $a^{n+1} = a^n a$
$a^{n-1} = (a^n) \cdot a^{-1}$.

cyclic subgroup

Prop. Given G group, $a \in G$, $H = \{a^n \mid n \in \mathbb{Z}\}$, then $H \leq G$.

see also $\langle S \rangle$ later

Proof: $1 \in H$ since $1 = a^0$.

- $x \in H \Rightarrow (\exists\, n \in \mathbb{Z})$ s.t. $x = a^n$. $x^{-1} = a^{-n} = a^m \in H$.
  $(m = -n)$

- Given $x, y \in H$, there are $n, m \in \mathbb{Z}$ s.t. $x = a^n$, $y = a^m$.
  $x \cdot y = a^n \cdot a^m = a^{n+m} \in H$.

Def. Given $a \in G$, $H = \{a^n \mid n \in \mathbb{Z}\}$ is the subgroup of G generated by a.

Ex. $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots [n-1]\}$

21-373

Example. $G = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots [n-1]\}$ $\quad [\ell] := \{nk+\ell \mid k \in \mathbb{Z}\}$.

(1) $H = \{m[1] \mid m \in \mathbb{Z}\} = G$ ('additive') $\quad \mathbb{Z}/n\mathbb{Z}$ is generated by $[1]$.

(2) Consider $G = (\mathbb{Z}, +, 0)$, $n \in G$

$n\mathbb{Z} \leq G$. $n\mathbb{Z}$ is generated by n.

G itself is generated by 1.

Find a non-cyclic group? (1) $(\mathbb{R}, +)$ is not cyclic because it is uncountable.

$H = \{a^n \mid n \in \mathbb{Z}\}$ is always finite or countable.

(2) $(\mathbb{Q}, +)$, the rationals, is not cyclic.

(3) S_3 is not cyclic.

Not abelian $\rightarrow$ not cyclic!

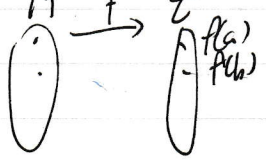
cyclic $\rightarrow$ Abelian

$a^m \cdot a^n = a^{m+n} = a^n \cdot a^m$.

$\rightarrow$ Given A countable (infinite), find $+_A : A \times A \to A$ s.t. $(A, +_A)$ is a cyclic grp.

$f : A \leftrightarrow \mathbb{Z}$. define $a +_A b$:

$a +_A b = f^{-1}(f(a) + f(b))$.



generator is $x \in A$ s.t. $f(x) = 1$.

Can check that $f : (A, +_A) \cong (\mathbb{Z}, +)$.

9/21/2020

Recall G is cyclic iff $\exists\, a \in G$ s.t $G = \{a^n \mid n \in \mathbb{Z}\}$

Examples (1) $(\mathbb{Z}, +)$ ± 1 when $(G, +)$ addition, $G = \{n \cdot a \mid n \in \mathbb{Z}\}$.

(2) $(\mathbb{Z}/n\mathbb{Z}, +)$ $n \geq 0$

Lemma If G is infinite cyclic, then $(\mathbb{Z}, +) \cong G$

Proof. Let $f(n) := a^n$, where a is a generator

Clearly $f: \mathbb{Z} \to G$ onto G since $G = \{a^n \mid n \in \mathbb{Z}\}$

Suppose $f(n_1) = f(n_2) \Rightarrow a^{n_1} = a^{n_2}$. WLOG suppose $n_1 \geq n_2$.

$a^{n_1 - n_2} = a^0 = 1$. $\Rightarrow n_1 = n_2$.

Recall that $\forall\, n \in \mathbb{Z}$, $n\mathbb{Z} \leq (\mathbb{Z}, +)$

Question Given $H \leq (\mathbb{Z}, +)$ $\exists\, n_H \in \mathbb{Z}$ s.t $H = n_H \mathbb{Z}$? Yes.

Subgroup also has generator

Theorem. If G is cyclic and $H \leq G$ then also H is cyclic.

Moreover if a generates G then a^d generates H, where d is the smallest positive integer n s.t $a^n \in H$

$H = \{h^k \mid k \in \mathbb{Z}\}$ where $h = a^d$

Corollary. $H \leq (\mathbb{Z}, +) \Rightarrow (\exists\, n \in \mathbb{Z})\ H = n\mathbb{Z}$

Pf. fix $a \in G$ generator. Consider $S_0 = \{d \in \mathbb{Z} \mid a^d \in H\}$, which is non-empty.

$d \in S_0 \Rightarrow -d \in S_0$. $[\, a^d \in H \Rightarrow a^d (a^{-d}) = 1 \in H\,]$

the inverse is in the set too!

If $H = \{1_G\}$ we are done. $d := 0$ Clearly H is cyclic generated by a^0.

DF Pg 57.

- If $|x| = n < \infty$ then $|x^q| = \frac{n}{(n,q)}$

$x^n = 1$ let $n = db$, $a = dc$, $(c,d) = 1$, $y = x^a$

WTS $|y| = b$. $y^b = x^{ab} = x^{dcb} = (x^{db})^c = 1^c = 1$.

So $|y| \mid b$. Let $|y| = k$, $y^k = 1$. $x^{ak} = 1$.

$n \mid ak \Rightarrow db \mid dk$

$b \mid ck$

$b \mid k$

$\Rightarrow b = k$

21-373

9/21/2020

Otherwise $\{1_G\} \subsetneq H$. Then $\exists\, d \neq 0,\ d \in S_0$.

Hence $-d \in S_0$ (as before)

Chap 2.3

So $S_1 := S_0 \cap \mathbb{Z}^+$ is always not empty.

By the well-ordering principle, there is a minimal $d \in S_1$, $[c \in S_1 \Rightarrow c \geq d]$.

→ Enough to prove that a^d generates H.

Pf. Namely if $a^n \in H$ $(n \neq 0)$, then $d \mid n$.

Let $n \neq 0$ s.t. $a^n \in H$ be given. By the division algorithm, there are $q, r \in \mathbb{N}$ s.t. $n = q \cdot d + r$ where $0 \leq r < d$.

$a^n = a^{q \cdot d + r} = (a^d)^q \cdot a^r \Rightarrow a^{n - dq} = a^r$.

(A) $a^n \in H$ by assumption.

(B) $a^d \in H$ (since $d \in S_0$).

$\Rightarrow (a^d)^q \in H \Rightarrow a^{dq} \in H$.

(A)+(B) $a^{n-dq} \in H \Rightarrow a^r \in H$.

So $r \in S_0$.

But $d > r \geq 0$, if $r > 0$ then $r \in S_1$.

which contradicts the minimality of d. So $r = 0$.

$\therefore d \mid n$

Theorem. Let G be a group, $\{H_i \mid i \in I\}$ subgroups of G. Let $K := \bigcap_{i \in I} H_i$. Then $K \leq G$.

Pf. As $H_i \leq G \ \forall i \in I$, clearly $1_G \in H_i \ \forall i \in I$. So $1_G \in K$.

Given $xy \in K$ as $H_i \leq G$ $xy^{-1} \in H_i \ \forall i \in I$. By definition of intersection, $xy^{-1} \in K$.

Def. Let G be a group, $A \subseteq G$. The subgroup ~~"degenerated"~~ "generated" by A is denoted by $\langle A \rangle$

Subgroup generated by a group

$$\langle A \rangle = \bigcap \{H \mid H \leq G, A \subseteq H\}.$$

If G is cyclic and generated by $a \in G$, then

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

~~let's call this H~~

- Clearly $H \leq G$ [$1 = a^0, a^n, a^m \in H \Rightarrow a^{n-m} \in H$]

If $K \leq G$ containing a then $a^n \in K \ \forall n \in \mathbb{Z}$ (intersection) $K \supseteq H = \{a^n \mid n \in \mathbb{Z}\}$

Hence H is the 'smallest'.

(Remark) G is cyclic $\Leftrightarrow$ $(\exists a \in G)\ G = \langle a \rangle$.

Proposition. Suppose G is a group, $A \subseteq G$, then $\langle A \rangle = \{a_0^{\varepsilon_0} a_1^{\varepsilon_1} \dots a_{n-1}^{\varepsilon_{n-1}} \mid n \in \mathbb{N}, a_i \in A, \varepsilon_i \in \{+1, -1\}\}$

Cyclic → abelian

Not abelian → generating set has more than 1 element

'Special' Types of Groups (DKF Chap 1)

Dihedral groups (D_{2n})

At most $|s| = 2$ reflections and $|r| = n$ rotations

s or 1 $\qquad$ $1, r, r^2, \ldots r^{n-1}$

$|D_n| = 2n$.

- $s \neq r^i$ for any i.
- $sr^i \neq sr^j$.
- $rs = sr^{-1}$
- $r^i s = sr^{-i}$

Quaternions (Q_8)

$1 \cdot a = a \cdot 1 = a$

$-1 \cdot a = a \cdot -1 = -a$

1	-1
i	$-i$
j	-1
k	$-k$

$i \cdot j = k$, $j \cdot i = -k$

$i \cdot -j = -k$, $-i \cdot j = -k$

$i \cdot i = j \cdot j = k \cdot k = -1$

$i \cdot -i =$

Cyclic (S_n)

( ) ( ) ( )

Cycle Decomposition.

$g \cdot I$

(8) $\sigma_1 \cdot \sigma_2^{-1} \in G_I$

$[\sigma_1 \circ \sigma_2^{-1}]$ $\begin{cases} g_1 \cdot I = I \\ g_2 \cdot I = I \end{cases}$

Symmetry $\sigma: A \to A$ $\quad \varphi: S_A \to G$

$\sigma(a) = g \cdot a$

σ_g $\quad \varphi: G \to S_A$

$g \cdot a = \varphi(g)(a)$ $\quad N_S \to N_S$

$g_1 \cdot I = I$

$g_2 \cdot I = I$

$g_1 \cdot g_2^{-1} = I$

(10)

$N_G(H) = \{ g \in G \mid a \cdot h = h \cdot a, h \in H \}$

$C_G(H) = \{ g \in G \mid g \cdot h = h \cdot g \ \forall\ h \in H \}$

Show that $x \in N_G(H) \to x \in C_G(H)$

$\{ g \cdot h_i \cdot g^{-1} \mid h \in A \} = \{ H \}$

$x h_1 x^{-1} = h_2$ $\quad h_1 = h_1 \cdot h_2 = x \cdot h_1 \cdot h_2 \cdot x^{-1} = h_2$?

$= h_1$

$x h_2 x^{-1} = h_1$

$x h_1 = h_2 x$

$h_1 = x^{-1} h_2 x$

$x h_2 x^{-1} = x^{-1} h_2 x.$

E: empty $\quad N_G(H) = G = C_G(H)$ $\quad N_x$

$G =$

$H \trianglelefteq Z(G)$

21-373 9/23/2020

Let G be a group, $A \subseteq G$.

$\langle A \rangle = \bigcap_{H \leq G,\ H \supseteq A} H$, the subgroup generated by A.

Special case $A = \{a\}$, by abuse of notation, we say that $\langle A \rangle$ is generated by a.

So $\langle a \rangle = G \Leftrightarrow G$ is cyclic.

We know $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Theorem. Let G be a group $A \subseteq G$, $A \neq \emptyset$ then

$\langle A \rangle = \bar{A}$, $\bar{A} := \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \mid a_i \in A, n \in \mathbb{N}, \varepsilon_i \in \{+1, -1\}\}$

Proof. — $\bar{A} \subseteq \langle A \rangle$: Given $a_1, \ldots a_n \in A$ and $\varepsilon_i \in \{+1, -1\}$,

let $b := a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \in H$ for any $H \leq G$, $H \supseteq A$.

$b \in \bar{A} \Rightarrow b \in \langle A \rangle$

So $b \in \bigcap_{H \leq G, H \supseteq A} H = \langle A \rangle$

↑ is one of the H's

— $\langle A \rangle \subseteq \bar{A}$: As $\langle A \rangle \subseteq G$, clearly containing A, enough to show that $A \subseteq \langle A \rangle$

(a) $A \subseteq \bar{A}$: Given $a \in A$ as $a = a^1 \in \bar{A}$.

(b) $\bar{A} \leq G$: Enough to show $x, y \in \bar{A} \Rightarrow x \cdot y^{-1} \in \bar{A}$.

Suppose $x = a_1(x)^{\varepsilon_1(x)} \cdots a_n(x)^{\varepsilon_n(x)}$

$y = a_1(y)^{\delta_1(y)} \cdots a_m(y)^{\delta_m(y)}$

$y^{-1} = a_m(y)^{-\delta_m(y)} \cdots a_1(y)^{-\delta_1(y)}$, $xy^{-1} = a_1(x)^{\varepsilon_1(x)} a_n(x)^{\varepsilon_n(x)} a_m(y)^{-\delta_m(y)} \cdots a_1(y)^{-\delta_1(y)}$

Question (before CS!) Suppose we have a group G and a finite $A \subseteq G$ s.t. $G = \langle A \rangle$

Is there an algorithm that takes as input a word, i.e. $W = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ where $a_i \in A$, $\varepsilon_i \in \{+1, -1\}$

Can the algorithm tell us if $W = 1_G$? Ex. $ab \cdot b^{-1}c^{-1}$

Answer No.

Alt. Given W_1, W_2 words in A, does there exist an algorithm such that $W_1 = W_2$?

Back to Homomorphisms: $\varphi: G \to H$, $\varphi(a *_G b) = \varphi(a) *_H \varphi(b)$.

e.g. (1) If V, W are vector spaces over F, then the linear transformation $T: V \to W$, $(V, +_V) \to (W, +_W)$ is homomorphism.

(2) Suppose $(F, +, -, 0, 1)$ is a field.

Fix $a \in F$. $\varphi(x) = a \cdot x$. $\varphi: (F, +) \to (F, +)$ is a homomorphism.

since $\varphi(x+y) = a(x+y) = ax + ay = f(x) + f(y)$

- identity $\varphi(1_G) = \varphi(1_G) \cdot \varphi(1_G)$
- inverse $\varphi(1_G)^{-1} \varphi(1_G) = \varphi(1_G)$
  $1_H = \varphi(1_G)$

  $\varphi(x) \cdot \varphi(x^{-1}) = 1_H$.

  $\varphi(x) \cdot [\varphi(x)]^{-1} = 1_H$.

Kernel Def. Suppose G, H are groups $\varphi: G \to H$ homomorphism.

21-373

9/25/2020

The kernel of φ, $\ker(\varphi) := \{a \in G \mid \varphi(a) = 1_H\}$.

Ex. Let $n \geq 2$, F = field, $G = GL(n,F) = \{A \in M_n(F) \mid \det A \neq 0\}$

general linear matrix; square

$\det: G \to F^*$ [the multiplicative Group of F]

$\det(A \cdot B) = (\det A)(\det B)$

$\ker(\det) = SL(n,F)$

Lemma: If $\varphi: G \to H$ homomorphism then $\ker(\varphi) \leq G$.

[Kernel is subgroup]

transitivity

$\varphi: G_1 \to G_2$, $\psi: G_2 \to G_3$

$\psi \circ \varphi: G_1 \to G_3$ homomorphism.

Suppose $\chi = \psi \circ \varphi$. Given $x, y \in G$, $\chi(x \cdot y) = \psi(\varphi(x \cdot y))$

φ hom $= \psi(\varphi(x)\varphi(y))$

ψ hom $= \psi(\varphi(x)) \cdot \psi(\varphi(y))$

$= \chi(x) \cdot \chi(y)$

If ψ, φ both injective – then $\psi \circ \varphi$ injective

surjective

bijective

isomorphism

Cor 1 If $\varphi: G_1 \cong G_2$, $\psi: G_2 \cong G_3$ then $\psi \circ \varphi: G_1 \cong G_3$.

Def. Let G be a group. If $\varphi: G \cong G$ (injective + surjective) we call φ an automorphism.

$\mathrm{Aut}(G) := \{ \varphi \mid \varphi: G \cong G \}$, the set of all automorphisms

Automorphism ⊂ Isomorphism

Cor 2 $(\mathrm{Aut}(G), \circ)$ is a group

($\circ$: function composition)

Pf. $id \in G \Rightarrow id \in \mathrm{Aut}(G)$, $\varphi, \psi \in \mathrm{Aut}(G) \Rightarrow \psi \circ \varphi \in \mathrm{Aut}(G)$

- inverse $\varphi^{-1} \in \mathrm{Aut}(G)$: Clearly as φ is a bijection, also φ^{-1} is a bijection. Left to show $\forall x, y \in G$, we have $\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$.

Let $x_1 := \varphi^{-1}(x)$, $y_1 := \varphi^{-1}(y)$

$$\varphi(x_1 \cdot y_1) = \varphi(x_1)\,\varphi(y_1) = x \cdot y$$

$$\varphi^{-1}(\varphi(x_1 y_1)) = \varphi^{-1}(x \cdot y)$$

So $\varphi^{-1}(x) \cdot \varphi^{-1}(y) = x_1 \cdot y_1 = \varphi^{-1}(x \cdot y)$

$\mathrm{Aut}(G) \leq \mathrm{Sym}(G) := \{ f: G \to G \mid f \text{ bijection} \}$

21-373 9/25/2020

Def. Let G be a group. Fix $a \in G$, let $f_a(x) = axa^{-1}$.

Want $f_a : G \to G$. If such a exists, $\varphi(x) = f_a(x)$ is inner automorphism of G.

Inner Automorphism

Why it is automorphism?

$$f_a(xy) = axya^{-1} = (ax)(ya^{-1})$$

$$= (ax)(a^{-1}a)(ya^{-1})$$

$$= (axa^{-1})(aya^{-1}) = f_a(x) \cdot f_a(y)$$

f_a is injective: Suppose $f_a(x) = f_a(y) \overset{\text{def}}{\Rightarrow} axa^{-1} = aya^{-1}$

$$\Rightarrow x = y.$$

f_a is surjective: Given $y \in G$ fix x s.t. $f_a(x) = y$.

Then let $x = a^{-1}ya$.

Verify that $f_a(x) = a \cdot x \cdot a^{-1} = a(a^{-1}ya)a^{-1} = y$.

Inner Automorphisms is subgroup of automorphisms

Provided $\exists a \in G$, f_a this is G

Def $\varphi \in \mathrm{Aut}(G)$ is called an inner automorphism of G provided $\exists a \in G$ s.t. $\varphi(x) = f_a(x)$ $\forall x \in G$.

set of functions!

Def. $\mathrm{Inn}(G) = \{\varphi \in \mathrm{Aut}(G) \mid \varphi \text{ is an inner auto}\} \leq \mathrm{Aut}(G)$

identity

① Clearly $\mathrm{id}_G \in \mathrm{Inn}(G)$, taking $a = 1_G$.

② Given $a, b \in G$ need to find $d \in G$ s.t.

$$f_b \circ f_a = f_d.$$

Sketch

$f_b(f_a(x)) = b(axa^{-1})b^{-1} = (ba)x(ba)^{-1}$

Take $d := ba$, then we have $f_b \circ f_a = f_d$.

⑤ Given $f_a \in Inn(G)$, find $b \in G$ s.t. $f_a^{-1} = f_b$. Take $b := a^{-1}$.

$f_a(f_{b(x)}) = f_a(bxb^{-1}) = x$.

Remark. When G is abelian, $Inn(G) = \{id\}$.

$f_a(x) = axa^{-1} = xaa^{-1} = x \cdot 1 = x$.

E.g. $G = \mathbb{C}$, so G can be arbitrarily large!

Quotient Group (p178)

G/K (K is $\ker(\varphi)$, $\varphi: G \to H$ or any normal subgroup; this is right)

- Kernel of a group homomorphism is a normal subgroup

Kernel is normal subgroup

$gkg^{-1} \in K$

21-373

9/28/2020

eg. r^2 is stabilizer of g

$\ker(f_g) = r^2 g r^{-2} = g$

Kernel of Inner Automorphism Group is center

Given $g \in \epsilon$ what is $\ker(f_g)$?

Define $k: \epsilon \to \mathrm{Inn}(\epsilon)$ by $k(a) = k_a$.

$h \in \ker(f_g) \Rightarrow f_g(h) = 1_\epsilon$

$\Leftrightarrow ghg^{-1} = 1_\epsilon$

$\Leftrightarrow$

Then $\ker(k) = z(\epsilon)$

$\hookrightarrow = \{x \in \epsilon : k_x = I_\epsilon\}$

$\hookrightarrow = \{x \in \epsilon : \forall g \in \epsilon : xgx^{-1} = g\}$

$= \{x \in \epsilon : \forall g \in \epsilon : xg = gx\}$

$\ker(f_g)$ is centralizer of g.

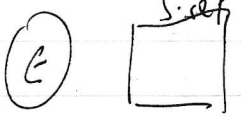
$\forall a \in \epsilon$

$C_\epsilon(\{a\}) = \{g \in \epsilon \mid gag^{-1} = a\} = \{g \in \epsilon \mid f_g(a) = a\}$ stabilize?

$|G| = [\epsilon : H] \cdot |H|$, $H \leq \epsilon$, where $[\epsilon : H] = \#\{Ha \mid a \in \epsilon\}$.

↳ If $|\epsilon| = p$ prime, then ϵ is cyclic. If ϵ finite, $H \leq \epsilon \Rightarrow |H| \mid |\epsilon|$

'keep multiplying'



curve

Group Acting on a Set

Given a finite group with n-many elements.

→ If $m \mid n$ (integer) then $\exists H \leq \epsilon$, $|H| = m$?

Answer: not true in general.

Cauchy's Theorem. If $p \mid |\epsilon|$ and p is prime then $\exists H \leq \epsilon$, $|H| = p$

(1832-1918) Sylow's 1st Theorem If $p^k \mid |G|$ and p is prime then $\exists H \leq \epsilon$, s.t. $|H| = p^k$.

Group Actions

$h: G \times S \to S$ is called an action of G on S provided

(1) $h(1_G, x) = x \quad \forall x \in S$

(2) $\forall g_1, g_2 \in G, x \in S$
$h((g_1 g_2), x) = h(g_1, h(g_2, x))$

injective homomorphism also (isomorphism?)
D6 $\to S_3$

Alt notation $\cdot : G \times S \to S$

$\forall g_1, g_2 \in G, (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

Suppose G acts on S, $x \in S$, then $\text{orbit}(x) := \{g \cdot x \mid g \in G\}$.

Stabilizer $G_x := \{h \in G \mid h \cdot x = x\}$ Pg 51.

Theorems (1) $G_x \leq G$

(2) $|\text{orbit}(x)| = [G : G_x]$

Stabilizer is subgroup

$1_G \in G_x$

$g \in G_x \Rightarrow g \cdot x = x$

g^{-1}? $g^{-1}(g \cdot x) = g^{-1} x$

$x = g^{-1} x$

$\therefore g^{-1} \in G_x$

21-373 9/30/2020

"Coset Calculus"

Def Suppose $H \leq G$, $x \in G$. Then the right coset of x is

$$Hx = \{hx \mid h \in H\}$$

Left coset: $xH = \{xh \mid h \in H\}$.

We have seen: if $H \leq G$, $x, y \in G$, $x \sim_H y \overset{\text{def}}{\iff} xy^{-1} \in H$

$\sim_H$ is an equivalence relation and $[x]_{\sim_H} := Hx$.

Cor. Given $x, y \in G$, either $Hx = Hy$ or $Hx \cap Hy = \emptyset$

[Alt. if $Hx \cap Hy \neq \emptyset \Rightarrow Hx = Hy$]

Proposition. Suppose $H \leq G$, $x, y \in G$. $Hx \cap Hy \neq \emptyset \Rightarrow Hx = Hy$.

Pf. $Hx \cap Hy \neq \emptyset \Rightarrow$ There are $h_1, h_2 \in H$ s.t. $h_1 x = h_2 y$. (A) (start here)

Double containment: Show $Hx \subseteq Hy$: Given $h \in H$, need to find $h^* \in H$ s.t. $hx = h^* y$.

Let $h_3 := h \cdot h_1^{-1}$. Since $H \leq G$, also $h_3 \in H$. Multiply (A) by h_3 from the left.

$$h_3(h_1 x) = h_3(h_2 y)$$

$$(h \cdot h_1^{-1})(h_1 x) = h_3(h_2 y)$$

$$hx = \underbrace{(h_3 h_2)}_{h^*} y \Rightarrow hx = h^* y.$$

Similarly we can show $Hy \subseteq Hx$. Given $h \in H$, find $h^* \in H$ s.t. $hy = h^* x$

Let $h_3 := h \cdot h_2^{-1}$

$$h \underbrace{h_2^{-1} h_1}_{h^*} x = h h_2^{-1} h_2 y$$

For left cosets,

Prop. $H \leq G$, $x, y \in G$. $xH \cap yH \neq \emptyset \Rightarrow xH = yH$

$xH \cap yH \neq \emptyset \Rightarrow \exists\, a \in xH \cap yH$ $a \in xH$, $\exists h_1 \in H$ s.t. $a = xh_1$

$a = yh_2$

$xh_1 = yh_2$ (B)

$xH \subseteq yH$: Given $h \in H$. Taken $h_3 = h^{-1} \cdot h$ mult(B) on the right

$xh_1 \cdot h_3 = yh_2h_3 \Rightarrow xh_1h^{-1} = y \cdot h^* \Rightarrow xh = yh^*$

$yH \subseteq xH$ take yh Find h^* s.t. $yh = xh^*$

know $xh_1 = yh_2$ $xh_1h_2^{-1}h = yh_2h_2^{-1}h = yh$ $\therefore xH \subseteq yH$.

Recall for $H \leq G$, the index of H in G is $[G:H] := |RC|$ (right cosets)

$RC = \{Hx \mid x \in G\}$.

Fact (Lagrange's Theorem) $|G| = |H| \cdot [G:H]$

Recall $|H| = |Hx|$ [use f(a) = ax bijection for H]

$G = \bigcup_{x \in G} Hx$. If $I \subseteq G$ s.t $x \neq y \in I \Rightarrow Hx \neq Hy$,

and $G = \bigcup_{x \in I} Hx$ then $|G| = \sum_{x \in I} |Hx| = |I| \cdot |H|$

Let $LC = \{xH : x \in G\}$. Is there a connection between the no. of left cosets and the number of right cosets?

Remark. (1) If G is commutative, $Hx = xH$.

(2) Is there an element in common between Hx and xH?

Always $x \in Hx$ and $x \in xH$

$(= 1x)$ $(= x \cdot 1)$

WANT TO SHOW: $|RC| = |LC|$

Def $H \leq G$, $x, y \in G$. $x \simeq y \Leftrightarrow x^{-1}y \in H$.
(left coset)

Lemma: $\simeq$ is an equivalence relation.

Proof. Reflexivity. $\because x^{-1} \cdot x \in H \Rightarrow x \simeq x$

Symmetry $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H$
$= y^{-1}x \in H$
$\therefore y^{-1} \simeq x$

Transitivity. $x, y, z \in G$. Given $x^{-1}y \in H \wedge y^{-1}z \in H \Rightarrow$
$x^{-1}y \cdot y^{-1}z \in H \Rightarrow x^{-1}z \in H \Rightarrow x \simeq z$.

Claim. The equivalence class of x with respect to $\simeq_H$ is xH.

Then we show that $|xH| = |H|$. $|G| = |H| \cdot |LC|$

When G is finite $|G| = |H| \cdot |RC| = |H| \cdot |LC|$
$|RC| = |LC|$

Note: cannot 'cancel' if $|G| = \infty$

Fact: $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$, $|\mathbb{Q}| = \aleph_0$, $|\mathbb{R}| = 2^{\aleph_0}$.

$\aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0} \cdot 2^{\aleph_0} \Rightarrow \aleph_0 = 2^{\aleph_0}$??

Need another strategy for $|G| = \infty$.

Th(*) $H \leq G$. $|RC| = |LC|$, without using finiteness of G or Lagrange's Theorem

Pf. Enough to find a bijection $\varphi : RC \to LC$.

Take $\varphi(Hx) := x^{-1}H$.

(1) φ is well-defined.
(2) φ is 1-1.
(3) φ is onto LC.

$H \leq G$, $x \in G$.

$Hx = \{hx \mid h \in H\}$, $xH = \{xh \mid h \in H\}$, $LC = \{xH \mid x \in G\}$

$RC = \{Hx \mid x \in G\}$

Recall $[G:H] = |RC|$

Theorem. $H \leq G$, $|RC| = |LC|$

Fact (1) $H \leq G$, $x, y \in G$ $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

intuition: "same equivalence class" $\Leftrightarrow x \sim y$.

(2) $xH = yH \Leftrightarrow y^{-1}x \in H$

Proof (1) Suppose $Hx = Hy$. Take $h \in H$; $\exists h_1 \in H$ s.t. $hx = h_1 y$.

$\Rightarrow$ (multiply by y^{-1}) $hxy^{-1} = h_1$.

mult by h^{-1} $\Rightarrow xy^{-1} = h^{-1} \cdot h_1$, $h_2 \in H$

$\Leftarrow$ Suppose $xy^{-1} \in H$. There is $h \in H$ s.t. $xy^{-1} = h$ (*)

$hh_1 y = h_1(h^{-1}x)$

Show $Hx \subseteq Hy$. Given $h_1 \in H$ want to find $h_2 \in H$ s.t. $h_1 x = h_2 y$.

$x = h \cdot y$.

$h_1 x = (h_1 \cdot h)y = h_2 \cdot y$, $Hy \subseteq Hx$ similar.

Given $h_1 \in H$, find $h_2 \in H$ s.t. $h_2 x = h_1 y$. $x = hy$

$h_2 x = h_1 hy$

$= h_2 y$ #

(2) Suppose $xH = yH$. Then we $h_1, h_2 \in H$ s.t.

$xh_1 = yh_2 \Rightarrow y^{-1}xh_1 = y^{-1}yh_2 \Rightarrow y^{-1}xh_1 = h_2$ (mult. by h_1^{-1})

$y^{-1}xh_1h_1^{-1} = h_2h_1^{-1}$

$y^{-1}x = h_2 \cdot h_1^{-1} \in H$.

Suppose $y^{-1}x \in H$, show $xH = yH$. Given $h_1 \in H$, WTS $xh_1 \in yH$.

$y^{-1}x = h_2 \Rightarrow yy^{-1}x = yh_2$. $x = yh_2$, $xh_1 = y(h_2h_1)$

Want to find a bijection $\varphi: RC \xrightarrow[\text{onto}]{1-1} LC$ (sets!)

let $\varphi(Hx) := x^{-1}H$

Example. $G = \langle \mathbb{Z}, + \rangle$, $H = 3\mathbb{Z}$

$$RC = \{H+x \mid x \in \mathbb{Z}\} = \{H+3n \mid n \in \mathbb{Z}\} \cup \{H+(3n+1) \mid n \in \mathbb{Z}\}$$
$$\cup \{H+(3n+2) \mid n \in \mathbb{Z}\}$$
$$= 3\mathbb{Z} \cup \{3\mathbb{Z}+1\} \cup \{3\mathbb{Z}+2\}$$

$$RC = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+1\}$$

Since $+$ is commutative $RC = LC$ in this case.

Usually (when $|H| \leq |G|$), for every $x \in G$, $\exists y \in G$ s.t.

$x \neq y$ but $Hx = Hy$.

eg. $(3\mathbb{Z} = 3\mathbb{Z}+0 = 3\mathbb{Z}+6 = 3\mathbb{Z}+9$ etc)

Need to show (1) φ is well-defined. Namely given $x, y \in G$ s.t. $Hx = Hy$ ("style-related")

$Hx = Hy \Rightarrow x^{-1}H = y^{-1}H$

(2) φ is injective

(3) surjective

21-373 10/2/2020

we have shown that

$Hx = Hy \iff x \cdot y^{-1} \in H \iff yx^{-1} \in H \iff (y^{-1})^{-1}(x^{-1}) \in H$

Fact: $a \in H \iff a^{-1} \in H$

(II) $x^{-1}H = y^{-1}H$

(I) $y^{-1}xH = H$

From Fact 2: $x^{-1}H = y^{-1}H \iff yx^{-1} \in H$

Prove well-defined and injective in one step

Hence $Hx = Hy \Rightarrow x^{-1}H = y^{-1}H$

$\varphi(Hx)$ $\varphi(Hy)$

($\Rightarrow$) well-defined

($\Leftarrow$) $\varphi(Hx) = \varphi(Hy) \Rightarrow \dots Hx = Hy$. Thus φ is injective.

opposite direction

Why is φ surjective? Given $x \in G$, find $y \in G$ s.t. $\varphi(Hy) = xH$.

$\varphi(Hy) = y^{-1}H$. Take $y = x^{-1}$.

Eg. $\frac{1}{3} = \frac{2}{6} = \frac{10}{30}$

The argument must be independent of the representative chosen.

Hence we need to prove that it is well-defined.

Review (PSO Prop 4)

- Prove that the set of left cosets of N in G partitions G

  WTS For left cosets uN, vN, either

  $uN = vN$ or $uN \cap vN = \emptyset$

  Suppose $x \in uN \cap vN \rightarrow$ WTS $uN = vN$

  $x = un_1 = vn_2$, $u = vn_2 n_1^{-1}$

  For $y = un_3$, WTS $y \in vN$

  $= v(n_2 n_1^{-1} n_3)$

  n_4 ✓

- P42 Prove $x \sim y \iff x \in \text{orbit}(y)$ is an equivalence class on S

  Reflexive $x \in \text{orbit}(x)$

  Symmetric $x \in \text{orbit}(y) \iff x = g \cdot y$
  $\iff y = g^{-1} \cdot x \iff y \in \text{orbit}(x)$

  Transitive $x \in \text{orbit}(y)$, $y \in \text{orbit}(z)$

  $x = g \cdot y$, $y = h \cdot z$

  $x = (g \cdot h) \cdot z$

  so $x \in \text{orbit}(z)$