Abstract Algebra Proof —— Group

kingno

Properties of Groups

1. If G is a group and $a \in G$ satisfies $a * a = a$, then $a = e$
2. $a * a' = e$ for all $a \in G$
3. $a * e = a$ for all $a \in G$
4. If $e' \in G$ satisfies $e' * a = a$ for all $a \in G$, then $e' = e$.
5. a' that satisfies $a' * a = e$ is unique, called reverse of a, a^{-1}
6. for all $n \geq 2$, $(a_1 * a_2 * \ldots * a_n)^{-1} = a_n^{-1} * \ldots * a_1^{-1}$

2

$(a * a') * (a * a') = a * (a' * a) * a = a * a' = e$

3

$a * e = a * (a' * a) = (a * a') * a = e * a = a$

Exponent of Groups

1. If there's a $k \geq 1$ that makes $a^k = 1(e)$, then the smallest such k is the order of a. Otherwise a has infinite order.
2. Any nonnegative integer n that makes $a^n = 1$ satisfies $n = mk$, where k is the order of a, m is some nonnegative integer.

2

let $n = mk + r, 0 \leq r < k$

$a^n = a^{mk+r} = (a^k)^m * a^r = 1 \quad \Rightarrow a^r = 1$

if $0 < r < k$, then r is smaller than the order of a

$\therefore r = 0, n = mk$

Subgroups

Definition: A subset H of a group G is a subgroup if

1. $1 \in H$
2. closed: if $x, y \in H$, then $x * y \in H$
3. if $x \in H$, then $x^{-1} \in H$

---

1. A subset H of a group G is a subgroup iff H is nonempty and, whenever $x, y \in H, xy^{-1} \in H$
2. A nonempty subset H of a finite group G is a subgroup iff H is closed under the operation of G.

1

Proof $\Leftarrow$.

First, let $y = x$, then $xx^{-1} \in H$

Secondly, let $x = 1$, then $\forall y \in H, 1y^{-1} \in H$

Fianlly, $\forall x, y, x * (y^{-1})^{-1} = xy \in H$

$H \subseteq G$, associativity is already there

Therefore, H is a subgroup.

2

There is some element $a \in H$, because H is nonempty, and $a^n \in H$ for all $n \geq 1$. (closed under $*$)

There must exist some $i, j, 1 \leq i < j$ make $a^i = a^j$ (otherwise H is infinite)

$a^i = a^j, a^{j-i} * a^i = a^j = a^i$, then $a^{j-i} = a^{i-i} = 1$ (identity)

Since $j - i - 1 \geq 0, a^{j-i-1} = a^{i-i-1} = a^{-1} \in H$ (inverse)

Therefore, H is a subgroup.

Cyclic Groups

Definition: If G is a group and $a \in G$, write

$< a >= \{a^n : n \in Z\} = \{\text{all powers of } a\}$;

$< a >$ is called the cyclic subgroup of G generated by a.

A group G is called cyclic if there is some $a \in G$ with $G =< a >$;

---

1. if $< a >$ has order n ($a^n = 1$), a^k is a generator iff $\gcd(k, n) = 1$

1

$a^{tn} = 1$

- If a^k is a generator, $\exists s \in Z^+, a^{sk} = a$, which means $a^{sk} = a^{tn+1}, sk = tn + 1$

  $sk - tn = 1 \quad \Rightarrow \gcd(k, n) = 1$
- If $\gcd(k, n) = 1, sk + tn = 1$. $k, n > 0$, then $st < 0$.

$$\begin{cases} \text{if } s > 0,\ (a^k)^s = a^{-tn+1} = a \quad a^k \text{ is a generator} \\ \text{if } s < 0,\ (a^k)^{-s} = a^{tn+1} = a \\ \text{if } s = 0,\ tn = 1, n = 1 \qquad\qquad \text{which means } a^k = 1 \quad trivial\{1\} \end{cases}$$

Cyclic Subgroups

1. A subgroup of a cyclic group is cyclic.
2. The order of a cyclic group G is the number of the elements $|G|$ in the group.

1

If H is a subgroup of $< a >$, and if $a^m, a^n \in H$.

In the light of closeness, $a^{sm+tn} \in H$, then $a^{\gcd(m,n)} \in H$. It can generate all $\{a^{sm+tn}\}$

If there is other element l not in $\{a^{sm+tn}\}$, then $a^{\gcd(l,\gcd(m,n))} \in H$, It can generate ....

Repeat the above operation

Thus $H =< a^{\text{gcd in the exponent}} >$

2

The order of G is the smallest number k that $a^k = 1$.

- G has most k elements, since any $a^n = a^{n\%k}$
- G has least k elements, since $a^i \neq a^j$ for all $1 \leq i < j \leq k$

Otherwise $a^{j-i} = 1$, contradicts that k is the smallest number makes $a^k = 1$

Cosets

Let H be a subgroup of a group G, and let $a, b \in G$

1. left cosets $aH = bH$ iff $b^{-1}a \in H$. $aH = H$ iff $a \in H$
2. if $aH \cap bH \neq \varnothing$, then $aH = bH$
3. $|aH| = |H|$ for all $a \in G$

1

- if $aH = bH$, then $\forall h_1 \in H, \exists h_2 \in H$, that $ah_1 = bh_2 \Rightarrow b^{-1}a = h_2h_1^{-1} \in H$
- if $b^{-1}a = h_2 \in H$, then $\forall h_1 \in H$,

  $a = bh_2, ah_1 = bh_1h_2$, H is a group, so it's closed under $*$, so $ah_1 = bh_1h_2 \in H, aH \subseteq bH$

  $b = ah_2^{-1}, bh_1 = ah_2^{-1}h_1 \in aH, bH \subseteq aH$

  therefore, $aH = bH$

2

if $aH \cap bH \neq \varnothing$, then there exists $h_1, h_2 \in H$, $ah_1 = bh_2 \Rightarrow b^{-1}a = h_2h_1^{-1} \in H$

3

$ah_1 \neq ah_2$

Lagrange's Theorem

1. If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$.

Proof. Let $\{a_1H, a_2H, \ldots, a_tH\}$ be the family of all the distinct cosets of H in G. Then

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH$$

because each $g \in G$ lies in the coset gH, and $gH = a_iH$ for some i. Moreover, distinct coset a_iH and a_jH are disjoint. It follows that

$$|G| = |a_1H| + |a_2H| + \ldots + |a_tH|$$

But $|a_iH| = |H|$ for all i. So $|G| = t|H|$

Homomorphism

If $(G, *)$ and $(H, \circ)$ are groups, then a function $f : G \to H$ is a homomorphism if

$$f(x * y) = f(x) \circ f(y)$$

Let $f : G \to H$ be a homomorphism.

1. $f(1) = 1$
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x^n) = f(x)^n$ for all $n \in Z$

1

Proof, $f(1_G) = 1_H$

$f(1_G) = f(1_G * 1_G) = f(1_G) \circ f(1_G) = 1_H$

In a group, if $aa = a$, then $a = 1$, thus $f(1_G) = 1_H$

2

$f(x) \circ f(x)^{-1} = 1 = f(1) = f(x * x^{-1}) = f(x) \circ f(x^{-1})$

But the inverse element is unique, therefore, $f(x^{-1}) = f(x)^{-1}$

3

for $n = 0$, $f(1_G) = 1_H$

for $n \in \mathbb{Z}^+$, if $f(x^{n-1}) = f(x)^{n-1}$, then

$f(x^n) = f(x^{n-1} * x) = f(x^{n-1}) \circ f(x) = f(x)^{n-1} f(x) = f(x)^n$

for $-n \in \mathbb{Z}^-$, $f(x^{-n}) = f((x^n)^{-1}) = f(x^n)^{-1} = (f(x)^n)^{-1} = f(x)^{-n}$

Kernels & Images

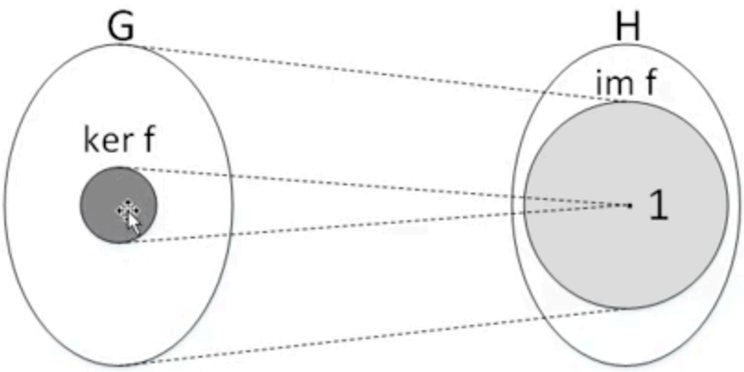
If $f : G \to H$ is a homomorphism, define

$$\ker f = \{x \in G : f(x) = 1\}$$

the kernel of the funciton and

$$\text{im } f = \{h \in H : h = f(x) \text{ for } x \in G\}$$

the image of the function.



1. ker f is a subgroup of G and im f is a subgroup of H.
2. if $x \in \ker f$ and if $a \in G$, then $axa^{-1} \in \ker f$
3. f is an injection iff $\ker f = \{1\}$

1

$f(1) = 1$.

- If $x, y \in \ker f$, then $f(x) = 1 = f(y)$; hence, $f(xy) = f(x)f(y) = 1$, and so $xy \in \ker f$.

  Finally, if $x \in \ker f$, then $f(x) = 1$ and so $f(x^{-1}) = f(x)^{-1} = 1$;

  thus, $x^{-1} \in \ker f$, and $\ker f$ is a subgroup of G.
- First, $1 = f(1) \in \text{im } f$.

  Next, if $h = f(x) \in \text{im } f$, then $h^{-1} = f(x)^{-1} = f(x^{-1}) \in \text{im } f$.

  Finally, if $k = f(y) \in \text{im } f$, then $hk = f(x)f(y) = f(xy) \in \text{im } f$. Hence, $\text{im } f$ is a subgroup of H.

2

$f(axa^{-1}) = f(a)f(x)f(a)^{-1} = 1$

3

If f is an injection, then $x \neq 1$ implies $f(x) \neq f(1) = 1$, and so $x \notin \ker f$. Conversely, assume that ker $f = \{1\}$ and that $f(x) = f(y)$. Then $1 = f(x)f(y)^{-1} = f(xy^{-1})$, so that $xy^{-1} \in \ker f = 1$; therefore, $xy^{-1} = 1, x = y$, and f is an injection.

Conjugate

- A **normal subgroup**(正规子群) $K \lhd G$: for every $k \in K, g \in G, gkg^{-1} \in K$
- A **conjugate** of an element a is of the form:

$$b = gag^{-1}, g \in G$$

- **Conjugation** $\gamma_g : G \to G$

$$\gamma_g(a) = gag^{-1}$$

---

1. conjugation is **isomorphism**
2. conjuage elements have the **same order**

1

- Conjugation $\gamma_g : G \to G$ is a **homomorphism**, because $\forall x, y \in G, gxyg^{-1} = gxg^{-1}gyg^{-1}$
- γ_g is a **serjuection**, because $\forall x \in G, \exists y = g^{-1}xg \in G, x = gyg^{-1}$
- γ_g is a **injection**, because $g^{-1}xg = 1 \Rightarrow x = 1, \ker \gamma_g = \{1\}$

Thus γ_g is an isomophism, and a permutation on G.

Congruence with multiplications

- Function $\mu([a], [b]) = [ab]$ is the multiplication operation on I_m. It is associative and commutative, and [1] is an identity element.
  1. If $(a, m) = 1, [a][x] = [b]$ can be solved for [x] in I_m
  2. If p is a prime, then $I_p^\times$, the set of nonzero elements in I_p, is a multiplicative abelian group of order $p - 1$.

1

$\exists s, t \in \mathbb{Z}, sa + tm = 1$

Let $x = sb, ax = sab = -tbm + b$

$[a][x] = [ax] = [-tbm + b] = [b]$

$[x] = [sb]$ is the solution

2

- Closeness: Since p is a prime, $[s][t] = 0$ implies $[s] = [0]$ or $[t] = [0]$.

Thus, $\forall s, t \in I_p^\times, [s][t] \neq 0, [st]$ is still in $I_p^\times$

- The identity element is [1]: $[1][a] = [a]$

Fermat's Theorem

- If p is a prime and $a \in Z$, then

$$a^p \equiv a \mod p$$
$$a^{p-1} \equiv 1 \mod p \text{ if } a \neq 0 \mod p$$

- If $[a] = 0 \mod p$, it's correct
- Otherwise $[a] \in I_p^\times . < a >= \{[a], [a^2], [a^3], \dots\}$ is a cyclic subgroup of $I_p^\times$.

  Let $d = | < a > |, a^d = [1]$. Note $|I_p^\times| = p - 1$

  According to Lagrange's Subgroup Theorem,

  $d|(p-1), p - 1 = kd, k \in \mathbb{Z}^+$. Thus $a^{p-1} = a^{kd} = [1]$

  Then $a^p \equiv a \mod p$

Quotient groups

1. If $K \lhd G$, then for all $b \in G, bK = Kb$.
2. Let G/K denote the family of all cosets of a subgroup K of G. If K is a normal subgroup, then for all $a, b \in G, (aK)(bK) = (ab)K$.

   And G/K is a group, called **quotient group**, under this operation.

1

$\forall bk \in bK, \exists k' \in K, k' = bkb^{-1}, bk = k'b \in Kb, bK \subseteq Kb$

$\forall kb \in Kb, \exists k' \in K, k' = b^{-1}kb, kb = bk' \in bK, Kb \subseteq bK$

2

If $K \lhd G$, the operation $(aK)(bK) = a(Kb)K = abKK = (ab)K$

Let G/K be the family of all the left cosets.

It is closed under the operation.

- identity: K. Since $(aK)K = aK$
- inverse of aK is $a^{-1}K, (aK)(a^{-1}K) = K$
- the associativity is already there

First Isomorphism Theorem

If $f : G \to H$ is a homomorphism, then

$$\ker f \lhd G \quad \wedge \quad G/\ker f \cong \text{im } f$$

Let $K = \ker f$, and let's consider left cosets:

$$G/K = \{K, aK, bK, \dots\} \quad \text{where } (aK)(bK) = abK$$

The function between G/K and $\text{im } f$ is simply f on a set, a valid function:

$$f(K) = 1_H, f(aK) = f(a), f(bK) = f(b), \dots$$

It is a homomorphism:

$$f(aKbK) = f(abK) = f(aK)f(bK)$$

By definition of $\text{im } f$, it is a surjection;

If $f(aK) = f(bK)$, then

$f(a) = f(b), f(ab^{-1}) = f(a)f(b^{-1}) = 1_H,$

$\exists k \in K, ab^{-1} = k, aK = bkK \subseteq bK, bK = ak^{-1}K \subseteq aK$

Thus $aK = bK$, the f on set is an injection ■

The proof on right cosets is the same.