MATH403: Introduction to Abstract Algebra

Michael Li

Preliminary Theorems

Theorem: $a, c \in Z$ are relatively prime if and only if $\exists x, y \in Z$ such that $ax + cy = 1$

Proof:

- $\implies$ holds by using gcd as a linear combination
- $\impliedby$ if $d \mid a$ and $d \mid c$ then $d \mid ax + cy \implies d \mid 1 \implies d = 1$ so 1 is the only common factor of a, b

Groups

Definition: **Binary Operation** on a set G is a function that assigns each ordered pair of G an element of G

$$f : G \times G \to G$$

Definition: A set G is a **Group** is under a binary operation $\circ$ if the following 3 properties are satisfied

1. **Associativity**: $\circ$ is associative so $(\forall a, b, c \in G)[(ab)c = a(bc)]$
2. **Identity**: there is an element $e \in G$ such that $(\forall a \in G)[ae = ea = a]$
3. **Inverses**: $(\forall a \in G)(\exists a^{-1} \in G)[aa^{-1} = a^{-1}a = e]$

Definition: A group G is said to be **Abelian** if $(\forall a, b \in G)[ab = ba]$

3 Key Properties of Groups

- **Uniqueness of Identity**.

  Proof: Let $(G, \cdot)$ be a group. Suppose by contradiction that e, e' are distinct identities of G then we have

  $$e = ee' = e'$$

  Which is a contradiction thus $e = e'$

- **Cancellation Property**: $(\forall a, b, c \in G)[ba = c\dot{a} \implies b = c]$

  Proof: Note that

  $$(b \cdot a) \cdot a^{-1} = b = c = (c \cdot a) \cdot a^{-1}$$

- **Each Element Has a Unique Inverse**: $(\forall a \in G)(\exists! a^{-1} \in G)[aa^{-1} = e = a^{-1}a]$

  Proof: Let $(G, \cdot)$ be a group. Suppose by contradiction that b, c are distinct inverses of $a \in G$. Then we have

  $$ab = e = ac$$

  However by the cancellation property, $b = c$. Thus we have a contradiction and a has a unique inverse

Shoes-Socks Property: $(ab)^{-1} = b^{-1}a^{-1}$

Proof: Note that $(ab)(b^{-1}a^{-1}) = e$

Theorem: if $a_1, a_2, \dots, a_n \in G$ then

$$(a_1 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$$

Proof by induction:

- Base case $a_1^{-1} = a_1^{-1}$
- IH: Suppose for an arbitrary $n \geq 1, (a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$
- IS: Let $a = a_1 \cdots a_n$ and $b = a_{n+1}$, then, using the shoes-socks property and IH, we have that

$$(a_1 \cdots a_{n+1})^{-1} = (ab)^{-1} = b^{-1} a^{-1} = a_{n+1}^{-1} \cdots a_1$$

Subgroups

Definition: Let $(G, \cdot)$ be a group, then $H \subseteq G$ is a subgroup if it is closed under $\cdot$ and closed under inverse $(h \in H \implies h^{-1} \in H)$

Definition: For any $a \in G$

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

is a subgroup called the **cyclic subgroup generated by** a

- **Note**: $\langle a \rangle = \langle a^{-1} \rangle \quad (a^{-k} \in \langle a^{-1} \rangle \implies (a^{-k})^{-1} = a^k \in \langle a^{-1} \rangle)$
- **Note**: $\langle 2a \rangle \leq \langle a \rangle$

Definition: Let $(G, \cdot)$ be a group. Then

$$Z(G) = \{a \in G \mid (\forall x)[ax = xa]\}$$

is called the **center of** G

- **Note**: If G is Abelian, then $Z(G) = G$

Definition: Let $(G, \cdot)$ be a group. Then for $a \in G$

$$C(a) = \{x \in G \mid ax = xa\}$$

is the **centralizer** for an element $a \in G$

- **Note**: If G is Abeliean, then $C(a) = G$

Theorem: $Z(G)$ is a subgroup of G

Proof:

- Closure: for arbitrary $a_1, a_2 \in Z(G)$ we have that

$$(a_1 a_2)x = a_1 a_2 x = a_1 x a_2 = x a_1 a_2 = x(a_1 a_2)$$

- Inverse: for $a \in Z(G)$ we have that

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \implies xa^{-1} = a^{-1}x$$

Theorem: $H, K \leq G \implies H \cap K \leq G$

Proof: use 2 step subgroup test

- $a, b \in H$ and $a, b \in K \implies ab \in H$ and $ab \in K$ by closure $\implies ab \in H \cap K$
- $a, a^{-1} \in H$ and $a, a^{-1} \in K$ by closure of inverses $\implies a, a^{-1} \in H \cap K$

Cyclic Groups

Definition: A group G is **cyclic** if $\exists a \in G$ such that

$$\langle a \rangle = G$$

so all elements are of the form a^k. Here a is called the **generator** of G

To show that G is cyclic, we need to show

- $G = \langle a \rangle$
- $\langle a \rangle$ has n distinct elements

Definition: The **order** $a \in G$ is the least positive exponent n such that $a^n = e$

Theorem: For $a \in (G, \cdot)$

- if $|a| = \infty, a^i = a^j$ if and only if $i = j$
- if $|a| = n, a^i = a^j$ if and only if $n \mid i - j$

Proof:

For $|a| = \infty$

- If $i = j$ then clearly $a^i = a^j$
- If $a^i = a^j$ where $i > j$ then for $m > 0$, $i = j + m$

$$a^i = a^{j+m} = a^j a^m \implies a^m = e$$

  Meaning that a has finite order, which is a contradiction. Thus $a^i \neq a^j$

For $|a| = n$

- If $n \mid i - j \implies a^i = a^j$

  Note that $a^i = a^{j+nk} = a^j a^{nk} = a^j$

- If $a^i = a^j \implies n \mid i - j$

  We have that $a^{i-j} = e$

  If $i = j \to$ done since $n \mid 0$

  If $i \neq j \to$ WLOG, $i > j$ then we have

  $i = j + m \implies a^{i-j} = a^m$

  Since $a^i = a^j \implies e = a^m$ so we need to show that $n \mid m$

  We can use Division Algorithm: $\exists! q, r \in Z$ such that $m = nq + r$ for $0 \leq r < n$

  Then we have $a^m = a^{nq+r} = a^r = e \implies r = 0$ since $0 \leq r < n$

  Thus we have shown that $n \mid i - j$

Corollary $|a| = |\langle a \rangle|$

Corollary G is cyclic $\implies |G| = |a|$

Corollary $|a| = n$ and $a^k = e \implies n \mid k$

Corollary if $a, b \in G$ have finite order and commute, then $|ab|$ divides $\text{lcm}(|a|, |b|)$

Proof: Let $|a| = n, |b| = m, L = \text{lcm}(m, n)$. Then for $r, s \in Z$

$$(ab)^L = a^L b^L = a^{mr} b^{ns} = e$$

Theorem $|a| = n \implies |a^k| = \frac{n}{\gcd(n,k)}$ and $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

Proof: Let $d = \gcd(n, k)$ and $k = dr$. Then we have

Since $a^k = a^{dr} \implies a^k \in \langle a^d \rangle \implies \langle a^k \rangle \subseteq \langle a^d \rangle$

By gcd as a linear combo, $d = kx + ny$ for $x, y \in Z$. Then

$$a^d = a^{kx+ny} = a^{kx} \implies a^d \in \langle a^k \rangle$$

Thus $\langle a^d \rangle \subseteq \langle a^k \rangle$

Thus $\langle a^d \rangle = \langle a^k \rangle$

Let $d = \gcd(n, k)$. Clearly, $(a^d)^{n/d} = e$ so we have $|a^d| \leq n/d$

On the other hand, suppose we have $i < n/d$ then $(a^d)^i \neq e$ by the definition of $|a| = n$.

Thus we have $|a^k| = |a^{\gcd(n,k)}| = n/\gcd(n, k)$

Corollary if G is cyclic, then the order of any element divides $|G|$

Fundamental Theorem of Cyclic Groups: every subgroup of a cyclic group is cyclic

Proof: Let $H \leq G$

- Case $H = \{e\}$ then H is trivially cyclic
- Case $H \neq \{e\}$ then there is a $b \in H$ such that $b \neq e \implies b = a^k$ for some $k \in Z$

  Furthermore, there must be a $c \in H$ such that $c = a^m$ where m is minimal positive power. Clearly by closure $\langle a^m \rangle \subseteq H$

  Using the division algorithm, we have $k = mq + r \implies a^r = a^{-mq}a^k \in H$ by closure

  However, $0 \leq r < m$, thus $r = 0$ since m is minimal

  Thus $b = a^k = a^{mq} \in \langle a^m \rangle$

  Thus we have $H = \langle a^m \rangle$

Ways of Testing Non-Cyclic Group

Use **Countability**: R is uncountable but $\langle a^k \rangle$ is countable. Thus R is not cyclic

Use **Abelian**: Any cyclic group is Abelian but $GL(2, R)$ is not Abelian. Thus $GL(2, R)$ is not cyclic

Misc Notes

$\langle m \rangle \subseteq \langle d \rangle \implies |m|$ divides $|d|$

$\langle a \rangle \cap \langle b \rangle = \langle lcm(a, b) \rangle$

Smallest subgroup containing $\langle a \rangle$ and $\langle b \rangle$ is $\langle \gcd(a, b) \rangle$

$\langle m, n \rangle = \{mx + ny \mid x, y \in Z\}$ (linear combination of m and n)

Permutations

Let S be an arbitrary set. A **permutation** of S is a bijection $S \to S$.

Then S_n, the group of all permutations of S under composition

Important things to note:

- $|S_n| = n!$
- ϵ is the identity

Theorem: every $\sigma \in S_n$ is a product of disjoint cycles

Proof: take $\sigma \in S_n$.

- If $\sigma = \epsilon = (1) \cdots (n)$ then we are trivially done
- Otherwise start with an arbitrary element c and applying $\sigma(\ldots(\sigma(c)))$ until we get to $\sigma^d(c) = \epsilon$. If this cycles through all possible values, we are done. Otherwise we repeat for the next distinct element
  - **Note**: this works because we know that there are a finite number of values

Theorem: order of an m-cycle is m. Order of a product of multiple disjoint cycles is the lcm of their orders.

- **Note**: in general $gh = hg \implies |gh| \neq lcm(|g|, |b|)$. Take for example $G = Z_{30}$
  - Let $g = 5 = h \implies |g| = 6 = |h|$. Then $g + h = 10$ but $|g + h| = 3 \neq lcm(|g|, |h|) = 6$. Instead, we showed above that $|gh| \mid lcm(|g|, |h|)$

Proof: Let $|c| = m$, $|d| = n$, $l = lcm(|c|, |d|)$, and $k = |cd|$

We have $(cd)^l = e \implies k \mid l$

Note that if c, d are disjoint then so are c^k, d^k.

Thus we have $(cd)^k = e \implies c^k d^k = e \implies c^k = d^{-k}$

- d fixes all elements of c
- d^k fixes all elements of c
- c fixes all elements of d
- c^k fixes all elements of d

Thus $c^k = d^{-k} \implies$ all elements are fixed.

Thus $c^k = d^{-k} = \epsilon \implies n \mid k, m \mid k \implies l \mid k$

Theorem: for $S_n, n > 1$, any $\sigma \in S_n$ is a product of 2 cycles (may not be disjoint)

Proof: We can take any cycle c_i of order k in σ such that $c_i = (abc \ldots k) = (ak)(aj) \ldots (ab)$. We can repeat this for any cycle in σ

Theorem: $\epsilon = c_1 \ldots c_r$ (all 2 cycles) $\implies r$ is even

Proof by induction:

$r = 1 \implies \epsilon \neq (ab)$ so $r \neq 1$

$r = 2 \implies$ trivially true

IH: For $k < r$, we have that $\epsilon = c_1 \ldots c_k \implies k$ is even

IS: show for $\epsilon = c_1 \ldots c_r$. Take the last 2 cycles. Possible cases are

- $(ab)(ab) = \epsilon$
- $(ab)(bc) = (ac)(ab)$
- $(ac)(cb) = (bc)(ab)$

- $(ab)(cd) = (cd)(ab)$

  Either we get the first case and then by Strong Induction $c_1 \dots c_{r-2}$ is even or we recurse downard and get the equation $\epsilon = (a?)c_2' \dots c_r'$. However, the LHS fixes a but the RHS doesn't fix a. Thus we have a contradiction and $\epsilon \neq c_1 \dots c_r$ in the case where r is odd

Theorem: If $\sigma \in S_n, n \geq 2$ and $\sigma = c_1 \dots c_r = f_1 \dots f_s$ (2 cycles), then r and f have the same parity

Proof: Note that $\sigma \cdot \sigma^1 = \epsilon$

Then we have $f_s^{-1} \cdots c_1^{-1} d_1 \cdots d_r = \epsilon \implies s + r$ is even by previous theorem

Thus either f, r are both odd or f, r are both even

Definition: $A_k = \{\sigma \in S_n \mid \sigma \text{ product of even number of 2-cycles}\}$

Theorem: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$

Proof: need to show that $|A_n| = |S_n - A_n|$, or that there is a bijection $f : A_n \to S - A_n$

Take $\sigma \in A_n$ and add a 2-cycle

- $f^{-1}(p) = (12)p$
- $f(f^{-1}(p)) = (12)(12)(p) = p$

Thus there is a bijection and $|A_n| = |S - A_n|$

Misc Notes

How many elements of order 3 are in S_5?

$|\sigma| = lcm(|c_1|, \dots)$

So there is a cycle c_i such that $|c_i| = 3$ but we can only have one 3 cycle for any permutation in S_5

Thus we can select $5 * 4 * 3/3$ unique 3 cycles, so there are 20 elements of order 3 in S_5

Isomorphism

Definition: A function $\phi : G \to G'$ is a **homomorphim** if $\phi(g_1 g_2) = \phi(g_1')\phi(g_2')$. If ϕ is a bijection, then it is an **isomorphism**

Properties of Homomorphisms

- For $e \in G$, $\phi(e) = e' \in G'$. Proof: $\phi(ee) = \phi(e)\phi(e) = \phi(e) \implies e'$ is the identity of G'
- For $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$. Proof: $\phi(gg^{-1}) = \phi(e) = \phi(g)\phi(g^{-1}) \implies \phi(g^{-1} = (\phi(g))^{-1}$

Definition: **Automorphism** of G is an isomorphic $\phi : G \to G$

- Trivial example is the identity mapping $\phi(a) = ea = a$ for all $a \in G$
- Aut(G) is the set of all automorphisms of G

Example: $f : Z_{10} \to Z_{10}$

- Note that 1 is a generator of Z_{10} thus $f(1)$ must also be a generator so $f(1) = \{1, 3, 7, 9\} = U(1)$
- Since we are working with addition, $f_a(n) = an$

Proof: Aut(G) is a group under function composition

- Given Automorphisms ϕ, ψ, $\psi\phi$ is also a bijection thus $(\psi\phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi\phi)(a)(\psi\phi)(b)$ is an automorphism and is closed
- Function composition is associative
- The identity mapping I exists where $\phi I = \psi$
- Inverses exists because ϕ is bijective

Proof: $U(n)$ is isomorphic to Aut(Z_n)

Proof: Isomorphisms $G \approx H$ are an equivalence relation

- Reflexivity: Identity mapping $I_G : G \to G$
- Symmetry: $\phi : G \to H \implies \phi^{-1} : H \to G$ by bijection
- Transitivity: $\phi : G \to H, \psi : H \to K \implies \psi\phi$ is bijective and is an isomoprhism

Note: $\mathrm{Aut}(G)$ is a permutation of G but NOT the converse since $|\mathrm{Aut}(G)|$

Theorem $U(n) \approx \mathrm{Aut}(Z_n)$

Note: $U(p) \approx Z_{p-1}$ where p is a prime since both are cycli of order $p - 1$

Note: $\mathrm{Aut}(Z_9) = (f_1, f_2, f_4, f_5 f_7) \approx U(9)$????????????????????????????

Definition: Inner Automorphism of G is $\phi_a(g) = aga^{-1}$ for $g \in G$

Proof: $\mathrm{Inn}(G)$ is a group:

- $\phi_a(gg') = aga^{-1}ag'a^{-1} = \phi_a(g)\phi_a(g')$ closure
- $\phi_a(e) = a^{-1} = e$ identity
-