MATH403 Introduction to Abstract Algebra

Michael Li

Contents

1 Preliminaries **2**

2 Groups **4**

2.1 Elementary Properties of Groups . . . 5

3 Finite Groups; Subgroups **6**

3.1 Subgroup Tests . . . 6

3.2 Examples of Subgroups . . . 8

4 Cyclic Groups **9**

5 Permutation Group **10**

1 Preliminaries

Well Ordering Principle: every nonempty set of positive integers has a smallest member

Division Algorithm: let $a, b \in Z$ with $b > 0$ then there exist unique $q, r \in Z$ such that $a = bq + r$ where $0 \leq r < b$

Proof: broken down into existence and uniqueness

- Existence: consider the set $S = \{a - bk \mid k \in Z \wedge a - bk \geq 0\}$
  - if $0 \in S$ then $b \mid a \implies q = a/b$ and $r = 0$
  - if $0 \notin S$ then
    - if $a > 0, a - b \cdot 0 \in S$
    - if $a < 0, a - b(2a) = a(1 - 2b) \in S$ (**note**: we are dealing with integers)

    So S is nonempty. Applying Well Ordering Principle, S has a smallest member $r = a - bq$ where $r \geq 0$

    To show that $r < b$, assume by contradiction that $r \geq b$, then $r - b \geq 0 \implies a - bq - b = a - b(q + 1) \in S$.

    However, $a - b(q + 1) < a - bq$ which is a contradiction since $a - bq$ is not the smallest member. Thus $r < b$.
- Uniqueness: suppose $q, q', r, r' \in Z$ such that

  $$a = bq + r,\ 0 \leq r < b \quad \text{and} \quad a = bq' + r',\ 0 \leq r' < b$$

  Without loss of generality, suppose $r' \geq r$, then $bq + r = bq' + r' \implies b(q - q') = r' - r$.

  Note that $0 \leq r' - r < b$ so the only multiple of b that satisfies the inequality above is 0

  Thus $r' = r \implies q' = q$

GCD Is a Linear Combo: for any nonzero $a, b \in Z$, there exists $s, t \in Z$ such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$

Proof: broken down into existence, smallest, and greatest divisor

- Existence: consider $S = \{am + bn \mid m, n \in Z \wedge am + bn > 0\}$

  Since S is nonempty, by the Well Ordering Principle, S has a smallest member, say $d = as + bt$
- Smallest: we claim that $d = \gcd(a, b)$

  Using Division Algorithm, we have $a = dq + r$ where $0 \leq r < d$

  If $r > 0$ then $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq) \in S$ contradicting that d is the smallest member of S

  So $r = 0$ and $d \mid a$

  Analogously, $d \mid b$ so d is a common divisor of a, b
- Greatest Divisor: suppose d' is another common divisor, then $a = d'h \quad \text{and} \quad b = d'k$

  Then $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$ so d' is a divisor of d and d is the greatest divisor

GCD Corollary: if a, b are relatively prime, then $\exists s, t \in Z$ such that $as + bt = 1$

Euclid's Lemma: if p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Proof: Suppose $p \nmid a$, then $\gcd(p, a) = 1 \implies 1 = as + pt$ for $s, t \in Z$ since GCD can be represented as a linear combo

This means that $b = bas + bpt$. Since $p \mid \text{RHS} \implies p \mid \text{LHS}$

Thus $p \mid b$

Fundamental Theorem of Arithmetic: every integer > 1 is a prime or a product of primes. This product is unique.

Proof: broken down into existence of a product of primes and unique product

- Existence: let S be the set of positive integers that cannot be factored as a product of primes

  By the Well Ordering Principle, S has a smallest member n

  Since n is not prime, $n = ab$ where $1 < a, b < n$

  Both $a, b \notin S$ so they are a product of primes

  But $n = ab$ so n is a product of primes, thus a contradiction is reached and S is empty

- Uniqueness: let S be a set of positive integers with non-unique prime factorizations

  By the Well Ordering Principle, S has a smallest member $n = p_1 \dots p_r = q_1 \dots q_s$

  Note that $p_1 \mid n \implies p_1 \mid q_1 \dots q_s$

  By Euclid's Generalized Lemma, $p_1 \mid q_j$ for some $1 \leq j \leq s$

  Since both p_1 and q_j are prime, $p_1 = q_j$

  After reordering the q_k factors, we get $p_2 \dots p_r = q_2 \dots q_s < n$ so $\notin S$

  Thus the remaining factors have a unique factorization and $r = s$ and $p_2 \dots p_r$ are the same as $p_2 \dots q_s$

  Thus S is empty

Multiples of lcm(a,b): let $a, b \in Z$ be nonzero. Then every common multiple of a, b is a multiple of (a, b)

Proof: let $m = (a, b)$ and M be a multiple of a, b.

By definition of lcm, $m \leq M$

By the division algorithm, $M = mq + r$ for $q, r \in Z$ and $0 \leq r < m$

Implies $r = M - mq$ and $ab \mid \text{RHS} \implies ab \mid \text{LHS}$

Since r is restricted to $0 \leq r < m$ and m is the lowest multiple of ab, we have that $r = 0$

Thus $M = qm$ and $m \mid M$

First Principle of Mathematical Induction: let S be a set of integers containing a. Suppose S has the property that for some integers $n \geq a, n \in S$, then $n + 1 \in S$. Then, S contains every integer greater than or equal to a

Proof: let A be an nonempty set consisting of integers $n \geq a$ where $P(n)$ doesn't hold

By the Well Ordering Principle, A has a least element, call it m.

Since $P(a)$ is true, $a \neq m$. Also, since m is the smallest member of A, $P(m - 1)$ is true

But then the property holds for $(m - 1) + 1$ thus a contradiction is reached and A is empty

Thus S contains all integers $\geq a$

Second Principle of Mathematical Induction: let S be a set of integers containing a. Suppose S has the property that $n \in S$ whenever every integer $< n$ and $\geq a$ is in S. Then S contains every integer $\geq a$

Proof: let A be a nonempty set consisting of integers $n \geq a$ where $P(n)$ doesn't hold

By the Well Ordering Principle, A has a smallest element, call it m.

Since $P(a)$ holds, $a \neq m$

This means that $P(a), P(a + 1), \dots, P(m - 2), P(m - 1)$ hold, which implies that $P(m)$ holds and we have a contradiction

Thus A is empty and S contains all integers $\geq a$

Equivalence Relation: an **equivalence relation** on set S is a set R of ordered pairs of elements of S such that

1. **Reflexive Property**: $(a, a) \in R$ for all $a \in S$
2. **Symmetric Property**: $(a, b) \in R \implies (b, a) \in R$
3. **Transitive Property**: $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$

Partition: a **partition** of set S is a collection of nonempty disjoint subsets of S whose union is S

Equivalence Classes Partition: the equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P

Proof: let $\sim$ be an equivalence relation on set S.

- for any $a \in S$, reflexive property shows that $a \in [a]$ so $[a]$ is nonempty and the union of all equivalence classes is S
- suppose $[a]$ and $[b]$ are distinct equivalence classes, need to show that $[a] \wedge [b] = \emptyset$

  By contradiction, assume $c \in [a] \wedge [b]$

  Let $x \in [a]$ then we have $c \sim a, c \sim b, x \sim a$.

  By symmetric property, we also have that $a \sim c$ and by transitivity we have $x \sim c$ and $x \sim b$.

  Thus $[a] \subseteq [b]$. Analogously $[b] \subseteq [a]$.

  Thus $[a] = [b]$ which yields a contradiction that $[a]$ and $[b]$ were distinct equivalence classes

  Thus $[a]$ and $[b]$ are disjoint

To prove the converse, let P be a collection of nonempty disjoint subsets of S whose union is S.

Define $a \sim b$ if a, b belong in the same subset

- Reflexivity: since the union of the subsets form S every $x \in S$ belongs to some subset
- Symmetry: by definition if a, b are in the same subset, then b, a are in the same subset
- Transitivity: if a, b are in the subset and b, c are in the same subset, then these must be the same subset since partitions must be disjoint. Thus a, c are in the same subset

2 Groups

Binary Operation: binary operation on set G is a function that assigns each ordered pair of elements of G an element of G

- this preserves **closure**, meaning that the members of an ordered pair from G yield a member of G

Group: let G be a set together with a binary operation that assigns each ordered pair (a, b) of elements of G an element in G, denoted ab. G is a **group** if all 3 are satisfied:

1. **Associativity**: operation is associative so $(ab)c = a(bc)$ for all $a, b, c \in G$
2. **Identity**: there is an **identity element** $e \in G$ such that $ae = ea = a$ for all $a \in G$
3. **Inverses**: for each element $a \in G$ there is an **inverse element** $b \in G$ such that $ab = ba = e$

Abelian (commutative): a group is Abelian if for every pair of elements a, b we have $ab = ba$. Otherwise it is non-Abelian if there is some pair of elements a, b such that $ab \neq ba$

Examples:

1. set of integers Z, rational numbers Q, and real numbers R are groups under ordinary addition
   - associativity is held

- identity is 0
- inverse of a is $-a$

2. set of integers under ordinary multiplication is NOT a group
   - there is no integer b such that $5b = 1$
3. subset $\{1, -1, i, -i\}$ of complex numbers is a group under complex multiplication
   - associativity is held
   - identity is 1
   - all terms have an inverse that exists in the subset
4. set Q^+ is a group under ordinary multiplication
   - associativity is held
   - identity is 1
   - inverse of any a is $1/a = a^{-1}$
5. set S of positive irrational numbers and 1, although it satisfies the 3 given properties, it is not a group

   $\sqrt{2} \cdot \sqrt{2} = 2 \notin S$ so S is not closed under multiplication.
6. rectangular matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of real entries is a group under componentwise addition
   - associativity is held
   - identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
   - inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$
7. $Z_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a group under addition modulo n
   - associativity is held
   - identity is 0
   - for $j > 0 \in Z_n$, inverse of j is $n - j$

2.1 Elementary Properties of Groups

Theorem 2.1 Uniqueness of the Identity: in a group G, there is only 1 identity element

Proof: suppose e and e' are both identities of G. Then

1. $ae = a$ for all $a \in G$ and
2. $e'a = a$ for all $a \in G$

Then $e'e = e'$ and $e'e = e$ so $e' = e$

Theorem 2.2 Cancellation: in a group G, the right and left cancellation laws hold. That is

$$ba = ca \implies b = c \quad \text{and} \quad ab = ac \implies b = c$$

Proof: suppose $ba = ca$ and let a' be the inverse of a

$$(ba)a' = (ca)a' \implies b(aa') = c(aa') \,\text{by Associativity} \implies b = c$$

Similar proof for left cancellation

Theorem 2.3 Uniqueness of inverses: for each element $a \in G$, there is a unique element $b \in G$ such that $ab = ba = e$

Proof: assume b, c are both inverses of a. Then $ab = e$ and $ac = e$ so $ab = ac$

Cancelling a on both sides gives $b = c$

Additional Notation:

- $g^0 = e$
- typically do not allow noninteger exponents like $g^{1/2}$
- exponent addition and multiplication laws hold: $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$
- exponent expansion of 2 elements typically does not hold: $(ab)^n \neq a^n b^n$
- because of uniqueness of inverse, for a valid group there is only 1 solution to $ax = b$, namely a^{-1}

Theorem 2.4 Socks-Shoes Property: for elements a, b, $(ab)^{-1} = b^{-1}a^{-1}$

Proof: $(ab)(b^{-1}a^{-1}) = a(bb^{-1}a^{-1})$ by Associativity $= aea^{-1} = aa^{-1} = e$.

Thus $(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1}) = e$ and $(ab)^{-1} = b^{-1}a^{-1}$

3 Finite Groups; Subgroups

Order of a Group: number of elements in a group, denoted $|G|$

Order of an Element: smallest positive integer n such that $g^n = e$, denoted $|g|$

- for additive notation, this would be $ng = 0$
- if no such integer exists, element g has **infinite order**

Examples

- let $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under multiplication mod 15.
  - the group has order 8
  - order of element 7, $7^1 \equiv 7, 7^2 \equiv 4, 7^3 \equiv 13, 7^4 \equiv 1$ so $|7| = 4$
- Z under ordinary addition:
  - every nonzero element has infinite order since the sequence $a, 2a, 3a, \ldots$ never includes 0 when $a \neq 0$

Subgroup: a subset H of group G that is a group under the operation of G, denoted $H \leq G$

- **Trivial Subgroup**: $\{e\}$ of G
- **Nontrivial Subgroup**: any subgroup that is not $\{e\}$
- Note: Z_n under addition modulo n is **not** a subgroup of Z under addition since it isn't an operation under Z

3.1 Subgroup Tests

One-Step Subgroup Test: let G be a group and $H \subseteq G$ with $H \neq \emptyset$. If $(\forall a, b \in H)[ab^{-1} \in H]$, then $H \leq G$

- in additive notation, if $a - b \in H$ whenever $a, b \in H$ then $H \leq G$

Proof:

- associativity: H has the same operation as G
- identity: pick any $x \in H$ and let $a = b = x$, then $xx^{-1} = e \in H$

- inverse: pick any $x \in H$ and let $a = e, b = x$, then $ex^{-1} = x^{-1} \in H$
- closure: pick any $x, y \in H$ and let $a = x, b = y^{-1}$, then $xy = x(y^{-1})^{-1} \in H$

Steps to apply One-Step Subgroup Test:

1. identify property P that distinguishes elements of H (defining condition)
2. prove that the identity has property P (verify H is nonempty)
3. assume elements a, b have property P and use assumption to show ab^{-1} has property P

Example: let G be an Abelian group with identity e. Then $H = \{x \in G | x^2 = e\}$ is a subgroup of G

- defining property of H is condititon $x^2 = e$
- $e^2 = e$ so H is nonempty
- assuming $a, b \in H$, we have $a^2 = b^2 = e$
- since G is Abelian, $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$. Therefore $ab^{-1} \in H$
- so by One-Step Subgroup Test, $H \leq G$

Example: let G be an Abelian group under multiplication with identity e, then $H = \{x^2 | x \in G\}$ is a subgroup of G

- since $e^2 = e$, identity has the correct from so H is nonempty
- assuming $a^2, b^2 \in H$ and since G is Abelian, we can write $a^2(b^2)^{-1}$ as $(ab^{-1})^2$ thus $H \leq G$

Two-Step Subgroup Test: let G be a group and $H \subseteq G$ with $H \neq \emptyset$. If $(\forall a, b \in H)[ab \in H \wedge a^{-1} \in H]$ then $H \leq G$

Proof: given $a, b \in H$, since $b^{-1} \in H$, we have $ab^{-1} \in H$ so the One-Step Subgroup Test is satisfied

Example: let G be an Abelian group. Then $H = \{x \in G \mid |x| \text{ is finite }\}$ is a subggroup of G

- $e^1 = e$ so H is non-empty
- assume $a, b \in H$ and let $|a| = m$ and $|b| = n$
- since G is Abelian, we have $(ab)^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$ so ab has finite order
- $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$, so a^{-1} has finite order
- by Two-Step Subgroup Test, $H \leq G$

Example: let G be an Abelian group and H, K be subgroups of G. Then $HK = \{hk | h \in H, k \in K\}$ is a subgroup of G

- $e = ee \in HK$
- suppose $a, b \in HK$. By definition of H there are elements $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$
- to prove that $ab \in HK$, observe that since G is Abelian and $H, K \leq G$, we have $ab = h_1k_1h_2k_2 = (h_1h_2)(k_1k_2) \in HK$
- likewise $a^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}k_1^{-1} \in HK$
- by Two-Step Subgroup Test, $HK \leq G$

To show a subset of a group is not a subgroup show that either

- identity is not in the set
- an element's inverse is not in the set
- 2 elements whose product is not in the set

Example: G be a group of nonzero real numbers under multiplication. $H = \{x \in G | x = 1 \vee x \in I\}$ and $K = \{x \in G | x \geq q\}$.

- H is not a subgroup of G since $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$

- K is not a subgroup of G since $2 \in K$ but $2^{-1} \notin K$

Finite Subgroup Test: let G be a group and $H \subseteq G$ with $|H| < \infty$. If $(\forall a, b \in H)[ab \in H]$ then $H \leq G$

Proof: need to show that $a^{-1} \in H$ for all $a \in H$ then apply Two-Step Subgroup Test

- given $a \in H$, if $a = e$ then $a^{-1} = e$
- if $a \neq e$, consider $S = \{a, a^1, \ldots\} \in H$ by closure. Since H is finite 2 of elements, say $a^j = a^k$ for $1 \leq j < k$ must be identical. Simplifying we get $e = a^{k-j} = aa^{k-j-1}$ so a^{k-j-1} is the inverse of a and is in H

3.2 Examples of Subgroups

$\langle a \rangle$ **is a Subgroup**: let G be a group and let $a \in G$. Then $\langle a \rangle \leq G$

Proof:

- since $a \in \langle a \rangle$, the subset is not empty
- let $a^n, a^m \in \langle a \rangle$. Then $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$
- by One-Step Subgroup test, $\langle a \rangle \leq G$

Note: $\langle a \rangle$ is called the **cyclic subgroup** of G generated by a

- $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$ so every cyclic group is Abelian

Center of a Group: $Z(G)$ the center of group G is the subset of elements in G that commute with every element $\in G$

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

Center is a Subgroup: the center of G is a subgroup of G

Proof: assume $a, b \in Z(G)$ so for all $x \in G$ we have $ax = xa$ and $bx = xb$. Then use Two-Step Subgroup Test:

- since $xa = ax$ we have $a^{-1}xaa^{-1} = a^{-1}axa^{-1}$ so $a^{-1}x = xa^{-1}$ and $a^{-1} \in Z(G)$
- since $abx = axb = xab$, $ab \in Z(G)$
- by Two-Step Subgroup Test, $Z(G) \leq G$

Centralizer: let a be an element of G. The **centralizer** of $a \in G$, denoted $C(a)$, is the set of all elements in G that commute with a

$$C(a) = \{g \in G | ga = ag\}$$

C(a) is a Subgroup: for each $a \in G$, the centralizer of a is a subgroup of G

Proof:

- $ae = a = ea$ so $e \in C(a)$ and is non-empty
- take any $x, y \in C(a)$, then $ax = xa$ and $ay = ya$. Then $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$ so $xy \in C(a)$
- take any $x \in C(a)$, then $ax = xa$. Then $x^{-1}a = x^{-1}ae = x^{-1}a(xx^{-1}) = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = eax^{-1} = ax^{-1}$ so $x^{-1} \in C(a)$
- By Two-Step Subgroup Test, $C(a) \leq G$

4 Cyclic Groups

A group G is **cyclic** if there is an element $a \in G$ such that $G = \{a^n \mid n \in Z\}$

- a is called the **generator** of G
- cyclic group generated by a is denoted $\langle a \rangle$

Examples:

- $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3 \rangle$. Similar for $\langle 7 \rangle$
- $U(8) = \{1, 3, 5, 7\}$ has no cyclic group
  - $\langle 1 \rangle \to \{1\} \neq U(8)$
  - $\langle 3 \rangle \to \{3, 1\} \neq U(8)$
  - $\langle 5 \rangle \to \{5, 1\} \neq U(8)$
  - $\langle 7 \rangle \to \{7, 1\} \neq U(8)$

Criterion for $\mathbf{a^i = a^j}$: let G be a group and $a \in G$

- if a has infinite order, then $a^i = a^j$ if and only if $i = j$
- if a has finite order (n), then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$

Proof:

- if a has infinite order, then there is no $n > 0$ such that $a^n = e$

  Since $a^i = a^j$, we have that $a^{i-j} = e$ and thus $i - j = 0$
- if a has finite order (n), let a^k be an arbitrary member of $\langle a \rangle$

  By division algorithm, $k = qn + r$ for $q, r \in Z$ and $0 \leq r < n$ So $a^k = a^{qn+r} = (a^n)^q a^r = a^r$

  Thus $a^k \in \{e, a, \ldots, a^{n-1}\}$ and $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$

  Next, assume $a^i = a^j$, which implies $a^{i-j} = e$

  By division algorithm, $i - j = qn + r$ for $q, r \in Z$ and $0 \leq r < n$

  Then $a^{i-j} = a^{qn+r}$ and $e = a^r$.

  Since n is the least positive integer such that $a^n = e$, r must be 0

  Thus $n \mid i - j$

  Conversely, if $i - j = nq$, then $a^{i-j} = a^{nq} = e^q = e$ so $a^i = a^j$

Corollary 1: for any $a \in G, |a| = |\langle a \rangle|$

Corollary 2: let $a \in G$ with $|a| = n$. If $a^k = e$, then $n \mid k$

Proof: since $a^k = e = a^0$, by the previous theorem/criterion, we know that $n \mid k - 0$

Corollary 3: if a, b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$

Proof: let $|a| = m$ and $|b| = n$

$(ab)^{mn} = (a^m)^n (b^n)^m = e$ so by the Corollary 2, $|ab|$ divides mn

Theorem 4.2: let $a \in G$ where $|a| = n$ and let k be a positive integer then

- $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

- $|a^k| = n/\gcd(n,k)\rangle$

Proof: let $d = \gcd(n,k)$ and $k = dr$

Since $a^k = (a^d)^r$, we have $\langle a^k\rangle \subseteq \langle a^d\rangle$ by closure

Since gcd can be written as a linear combo, we have $d = ns + kt \implies a^d = a^{ns+kt} = (a^n)^s(a^k)^t = (a^k)^t \in \langle a^k\rangle$ so $\langle a^d\rangle \subseteq \langle a^k\rangle$

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

Order of Elements in a finite Cyclic Group: in a finite cyclic group, the order of elements divides the order of the group

Criterion for $\langle \mathbf{a^i}\rangle = \langle \mathbf{a^j}\rangle$ and $|\mathbf{a^i}| = |\mathbf{a^j}|$: let $|a| = n$ then

- $\langle a^i\rangle = \langle a^j\rangle$ if and only if $\gcd(n,i) = \gcd(n,j)$
- $|a^i| = |a^j|$ if and only if $\gcd(n,i) = \gcd(n,j)$

Generators of Finite Cyclic Groups: let $|a| = n$ then

- $\langle a\rangle = \langle a^j\rangle$ if and only if $\gcd(n,j) = 1$
- $|a| = |\langle a^j\rangle|$ if an only if $\gcd(n,j) = 1$

Generators of Z_n: $k \in Z_n$ is a generator of Z_n if and only if $\gcd(n,k) = 1$

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

- if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n
- for each positive divisor k of n, the group $\langle a\rangle$ has exactly 1 subgroup of order k, namely $\langle a^{n/k}\rangle$

Number of Elements of Each Order in a Cyclic Group: if d is a positive divisor of n, then the number of elements of order d in a cyclic group of order n is $\phi(d)$ (Euler phi function)

5 Permutation Group

Permutation of a set A is a function from A to A that is both 1-1 and onto

Permutation Group of set A is a set of permutations of A that form a group under function composition