division algorith $\exists q, r \in \mathbb{Z}$ s.t. $k = qn + r$ with $0 \le r < n$.

Thm 0.2 (gcd thm): $\exists s, t$ s.t. $\gcd(n,k) = ns + kt$.

301. Brief points for mid-term.

CH2 Groups.

- Binary operations, group (associativity, identity, inverse).
- properties of groups: uniqueness of identity/inverses.
  cancellation ($ba = ca \Rightarrow b = c$), socks-shoes property ($(ab)^{-1} = b^{-1}a^{-1}$)

CH3 Finite groups, subgroups.

- Order of a group/an element, subgroup (subset $H \subseteq G$, also under operation of G; $H \le G$)
- Subgroup tests (1-step ab^{-1}) (2-step ab & a^{-1}) (finite ~~step~~ subgroup test: closed under operation of G)
- $\langle a \rangle$, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$, $C(a) = \{x \in G \mid ax = xa\}$ are subgroups

CH4. Cyclic groups

- $\langle a \rangle$ a cyclic group generated by a.
- properties of cyclic groups

Thm (Criterion for $a^i = a^j$) $a \in G$, if $|a| = \infty$, $a^i = a^j$ iff $i = j$; if $|a| = n < \infty$, $\langle a \rangle = \{e, a, \cdots, a^{n-1}\}$, $a^i = a^j$ iff n divides $i - j$

- Cor 1: $|a| = |\langle a \rangle|$
- Cor 2: $a^k = e \Rightarrow |a|$ divides k

order of elements in f_{cg}.

Thm $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \dfrac{n}{\gcd(n,k)}$

- Cor 1: In a finite cyc. g. $|a| \mid |G|$
- Cor 2: $|a| = n$, $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n,i) = \gcd(n,j)$; $|a^i| = |a^j|$ iff $\gcd(n,i) = \gcd(n,j)$
- Cor 3: generators of finite cyc grps. Let $|a| = n \Rightarrow \langle a \rangle = \langle a^i \rangle$ iff $\gcd(n,i) = 1$
- Cor 4: generators of Z_n. $k \in \mathbb{Z}$, $k \in Z_n$ is a generator of Z_n iff $\gcd(n,k) = 1$.

*

- subgroups of cyclic groups

FT of CG: Every subgp of cg is cyc. if $|\langle a \rangle| = n$, then order of each subgp is a divisor of n, say for each divisor $k > 0$, $\langle a \rangle$ has exactly one subgp of order k, which is $\langle a^{\frac{n}{k}} \rangle$.

Pf: ① show subgp is cyclic (if $H = \{e\}$ or not ...)

② —

③ —

Cor: (Subgp of Z_n) each positive divisor k of n, $\langle n/k \rangle$ is the unique ~~gp~~ subgp of Z_n of order k; these are the only subgps of Z_n.

Z_{30}: $\langle 1 \rangle = \{0, \cdots 29\}$ order 30

$\langle 5 \rangle = \{0, 5, 10, \cdots 25\}$ order 6

Thm: # of elements of each order in a cyclic group: d is a + divisor of n, the # of elements of order d in a cyclic group of order n is $\phi(d)$

Cor: finite grp. # elements of order d is a multiple of $\phi(d)$.

CH5 Permutation groups.

- def: permtt'n of A is a func $A \to A$ bijection, p-group of A is a set of p's of A that forms a group under func. composition
- symmetric group S_n: $A=\{1,\dots,n\}$. the set of all p's of A is called S_n. element of S_n has form of

$$\alpha=\begin{bmatrix}1 & 2 & \cdots & n\\ \alpha(1) & \alpha(2) & \cdots & \alpha(n)\end{bmatrix}$$ cycle-notation.

- properties of p's.

thm
① Products of disj cycles: be written as a cycle/product ... (added up)
② disjoint cycles commute: $\alpha\beta=\beta\alpha$ (no entries in common) (try a_i, b_i, c_i separately)
③ order of a permutation: = lcm of lengths of disj. cycles.
④ Product of 2-cycles. p's can be written as ... ① → ④ say $(12345)=$ ~~$(15)(14)(13)$~~ ~~$(51)(54)(53)(52)(51)$~~

Lemma ↗

⑤ $\varepsilon=\beta_1\cdots\beta_r$, β's → 2cycles, then r is even.
⑥ ⑤ $\alpha=\beta_1\cdots\beta_r=\gamma_1\cdots\gamma_s$, r, & s are both odd/even.
⑦ ⑥ even permutations form a group. (An (alternating group of deg n) is gp of even p's.)
⑦ For $n>1$, $|A_n|=\frac{n!}{2}$

CH6 Isomorphism

- bijection map from $G \to \bar{G}$ that preserves operation $\phi(ab)=\phi(a)\phi(b)$. $\Rightarrow G\cong\bar{G}$.
- cayley's thm: every gp is iso to a group of permutations.

thm properties: thm. (on elements) ① carries (id of G) → ($\bar{G}$'s id)
② $\phi(a^n)=[\phi(a)]^n$
③ $ab=ba$ iff $\phi(a)\phi(b)=\phi(b)\phi(a)$
④ $G=\langle a\rangle$ iff $\bar{G}=\langle\phi(a)\rangle$
⑤ $|a|=|\phi(a)|$
⑥ $x^k=b$, $x^k=\phi(b)$ have same # of solutions
⑦ G & $\bar{G}$ have same # elements of every order.

thm (on groups): ① $\phi^{-1}:\bar{G}\to G$ ② G abelian $\Leftrightarrow$ $\bar{G}$ abelian
③ cyclic ... ④ subgp ⑤ similar ⑥ $\phi(Z(G))=Z(\bar{G})$

- automorphism $G\to G$, inner auto. $\phi_a(x)=axa^{-1}$, $\forall x\in G$.

6.4. Aut(G) & Inn(G) are groups.
6.5 $Aut(Z_n)\cong U(n)$

Chapter 1. Introduction to Groups

- If $ab=ba$ for all $a,b \in G$, then G is ~~##~~ Abelian.

- The Dihedral Groups.
  D_4 : the dihedral group of order 8 (order – the number of elements it contains)
  D_n : the —— of order $2n$.

- The dihedral group of order $2n$ is called the group of symmetries of a regular n-gon.

- notes: In D_n, a reflection followed by a reflection must be a rotation.
  a rotation followed by a rotation must be a rotation.
  a rotation & a reflection in either order must be a reflection.

Chapter 2 Groups

Def (Binary Operation)
Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.
condition: 'closure'

Def (Group)
G is a group under the operation if
① Associativity. $(ab)c=a(bc)$, $\forall a,b,c \in G$.
② Identity. $\exists e \in G$ s.t. $ae=ea=a$ $\forall a \in G$.
③ Inverses. $\forall a \in G$, $\exists b \in G$ s.t. $ab=ba=e$.

- Non Abelian group example : general linear group of 2×2 matrices over $\mathbb{R}$.
  $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{R}, ad-bc \neq 0 \right\}$

- $U(n)$, $n>1$ to be the set of all positive integers less than n and relatively prime to n.

- The set of all 2×2 matrices with det 1 with entries from $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}_p$ is a non-~~Abl~~Abelian group under matrix multiplication.

Special linear group of 2×2 matrices
$SL(2,F)$

- Summary of Group Examples (F ⋯ ; L is a reflection).

Group	Operation	Identity	Form of element	Inverse	Abelian
$\mathbb{Z}$	Addition	0	k	$-k$	Yes
$\mathbb{Q}^+$	Multiplication	1	$\frac{m}{n}, m,n>0$	n/m	Yes
$\mathbb{Z}_n$	Addition mod n	0	k	$n-k$	Yes
$\mathbb{R}^*$	Multiplication	1	x	$\frac{1}{x}$	Yes
$GL(2,F)$	Matrix multiplication	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}a&b\\c&d\end{bmatrix}$ $ad-bc\neq 0$	$\begin{bmatrix}\frac{d}{ad-bc} & \frac{-b}{ad-bc}\\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}\end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k,n)=1$	Solution to $kx \bmod n = 1$	Yes
$\mathbb{R}^n$	Componentwise addition	$(0,0,\cdots,0)$	$(a_1,\cdots,a_n)$	$(-a_1,\cdots,-a_n)$	Yes
$SL(2,F)$	Matrix Multiplication	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}a&b\\c&d\end{bmatrix}$ $ad-bc=1$	$\begin{bmatrix}d&-b\\-c&a\end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360-\alpha}, L$	No

- Elementary properties of groups.

Thm 2.1. Uniqueness of the Identity.
In G, $\exists$ only one identity element.

Pf ① $ae=a$ $\forall a\in G$

② ~~$e'a=a$~~ $\forall a\in G$
$e'a=a$

Pf: No need.

Thm 2.2 Cancellation

In a G, $ba=ca \Rightarrow b=c$ and $ab=ac \Rightarrow b=c$.

Pf: Sps $ba=ca$. Let a' be inverse of a.

$(ba)a'=(ca)a' \xrightarrow{\text{associativity}} b(aa')=c(aa')$

$\Rightarrow be=ce \Rightarrow b=c$.

Similarly ... .

Thm 2.3 Uniqueness of Inverses.

$\forall a\in G, \exists b\in G$ s.t. $ab=ba=e$.

Pf: Sps two inverses $ab=e$ & $ac=e \Rightarrow ab=ac \Rightarrow b=c$.

Thm 2.4 Socks-Shoes property

$\forall a,b\in G.\ (ab)^{-1}=b^{-1}a^{-1}$

Pf. $(ab)(ab)^{-1}=e$ & $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aea^{-1}=aa^{-1}=e$

By 2.3 $(ab)^{-1}=b^{-1}a^{-1}$

Chapter 3. Finite Groups / subgroups

Def (order of a group).

# of elements of a group (finite / infinite) is called its order $|G|$

Def (Order of an Element)

$g\in G$, $|g|=n$ s.t. $g^n=e$, as n is the smallest int. If no such int exists, say g has infinite order.

Def (Subgroup)

If $H\subset G$ is itself a group under the operation of G, we say $H\leq G$.

① if $H<G$, it's called a proper subgroup.

② $\{e\}$ is called the trivial subgroup.

③ not $\{e\}$ is called a nontrivial subgroup.

Subgroup Tests:

Thm 3.1 One-step Subgroup Test

Let G be a group. H a non-empty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.

Proof: Same operation in G & H. then H has associativity.

let $x \in H$, $a = x$, $b = x$

$e = x \cdot x^{-1} = ab^{-1} \in H$.

$a = e$, $b = x$ so $x^{-1} \in H$.

show ($x, y \in H$. $xy \in H$)

already showed $y^{-1} \in H$ whenever $y \in H$

let $a = x$, $b = y^{-1}$, we have $xy = x(y^{-1})^{-1} = ab^{-1} \in H$ ▨

4 steps: ① Identify the property P that distinguishes the elements of H, identify a defining condition.

② Prove that the identity has property P. (verifies H is non-empty).

③ Assume that two elements a & b have P.

④ Use the assumption to show ab^{-1} also has P.

Thm 3.2. Two-step Subgroup Test.

G → group, H → non-empty subset of G. If $ab \in H$, $\forall a, b \in H$. and a^{-1} in H. $\forall a \in H$. Then subgroup.

Proof:

Thm 3.3. Finite ~~step~~ Subgroup Test

H non-empty subset (finite) of G. H is closed ~~up~~ under the operation of G, then H is a subgroup of G.

Pf: By 3.2. need only prove $a^{-1} \in H$ whenever $a \in H$. If $a = e$. then $a^{-1} = a$. done. If $a \neq e$, think of a. a^2. ...

By closure, all those belong to H. Since H is finite, not all of these are distinct. Say $a^i = a^j$, $i > j$. Then $a^{i-j} = e$ since $a \neq e$, $i - j > 1$.

So $aa^{i-j-1} = a^{i-j} = e$ and $a^{i-j-1} = a^{-1}$. But $i - j - 1 \geq 1 \Rightarrow a^{i-j-1} \in H$. done. ▨

Eg of subgroups:

Thm 3.4. $\langle a \rangle$ is a subgroup

Let G be a group, $a \in G$. Then $\langle a \rangle$ is a subgroup of G.

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

Pf: $a \in \langle a \rangle$, $\langle a \rangle \neq \emptyset$, Let $a^n, a^m \in \langle a^n \rangle$ Then

$a^n (a^m)^{-1} = a^{n-m} \in \langle a \rangle$. by thm 3.1. $\langle a \rangle$ is a subgroup of G.

→ Cyclic subgroup.

Def (Centre of a Group)

Center. $Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$

of group G is the subset of elements in G that commute with every element of G.

Thm 3.5. Center of G is a subgroup of G.

Pf: $e \in Z(G)$, $Z(G) \neq \emptyset$.

① Sps $a, b \in Z(G)$, then $(ab)x = a(xb) = (ax)b = (xa)b = x(ab)$ $\forall x \in G$.

So $ab \in Z(G)$

② Assume $a \in Z(G)$, $\Rightarrow xa = ax$.

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

$$(a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})$$

$$exa^{-1} = a^{-1}xe$$

$$xa^{-1} = a^{-1}x$$

By Thm 3.2. ✓

Def (Centralizer) of a in G:

the elements in G that commute with a.

Let a be a fixed element in G. The centralizer is the set of all

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

Thm 3.6. Centralizer of a ($C(a)$) is a subgroup.

Pf: Similar to Thm 3.5. ∎

Chapter 4 Cyclic Groups (The proofs on next two pages)

A group G is cyclic if $\exists\, a \in G$ s.t. $G = \{a^n \mid n \in \mathbb{Z}\}$.
Then a is called the generator of G.
notation: $G = \langle a \rangle$.

Thm 4.1 Criterion for $a^i = a^j$
Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ iff $i = j$. If a has finite order, say n then $\langle a \rangle = \{e, a, \cdots, a^{n-1}\}$ and $a^j = a^i$ iff n divides $i-j$.

Cor 1 $|a| = |\langle a \rangle|$
For any group element a, $|a| = |\langle a \rangle|$.

Cor 2 $a^k = e$ implies that $|a|$ divides k
Let G be a group & let a be an element of order n in G. If $a^k = e$, then n divides k.

Thm 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$
Let a be an element of order n in a group & let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n / \gcd(n,k)$

Cor. 1. Orders of elements in finite cyclic groups.
In a finite cyclic group, the order of an element divides the order of the group.

Cor 2. Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$
Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n,i) = \gcd(n,j)$ and $|a^i| = |a^j|$ iff $\gcd(n,i) = \gcd(n,j)$

Cor 3. Generators of Finite Cyclic Groups

Let $|a|=n$. Then $\langle a\rangle=\langle a^j\rangle$ iff $\gcd(n,j)=1$ and $|a|=|\langle a^j\rangle|$ iff $\gcd(n,j)=1$.

Cor 4. Generators of $\mathbb{Z}_n$.

An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n,k)=1$.

- Classification of subgroups of Cyclic Groups

Thm 4.3 Fundamental Thm 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; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k}\rangle$.

* Special Case: For each positive divisor k of n, the set $\langle n/k\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover these are the only subgroups of $\mathbb{Z}_n$.

Thm 4.4 Number of Elements of Each Order in a Cyclic Group.

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Note: $\phi(n)=|U(n)|$

Cor. Number of Elements of Order d in a Finite Group.

In a finite group, the number of elements of order d is divisible by $\phi(d)$.

~~Chapter 5~~

• Cor. 1 proof:

proof: Thm 4.1

• Cor 2 proof:

Proof: Since $a^k = e = a^0$, by Thm 4.1 that n divides $k-0$.

Thm 4.2 proof:

① let $d = \gcd(n, k)$ and let $k = dr$

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

By Thm 0.2 (gcd thm), there are integers s & t s.t. $d = ns + kt$.

So $a^d = a^{ns+kt} = (a^n)^s \cdot (a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$.

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

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

② first show $|a^d| = \frac{n}{d}$ for any divisor d of n.

Clearly $(a^d)^{\frac{n}{d}} = a^n = e$

So $|a^d| \leq \frac{n}{d}$

On the other hand, if i is positive integer less than $\frac{n}{d}$, then $(a^d)^i \neq e$ by def of $|a|$.

Since $d = \gcd(n, k)$ ~~to obtain~~ $\Rightarrow |a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = |$~~gcd~~$a^{\gcd(n,k)}|$

$$= \frac{n}{\gcd(n,k)}$$

Cor 2:

Proof: Thm 4.2 shows that $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$

so we need to prove $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ iff $\gcd(n,i) = \gcd(n,j)$

Chapter 5 Permutation groups

Definition Permutation of A, Permutation group of A.

A permutation ~~group~~ of a set A is a function from A to A that is both 1-1 & onto.

A permutation group of (a) set A is a set of permutations of A that forms a group under function composition.

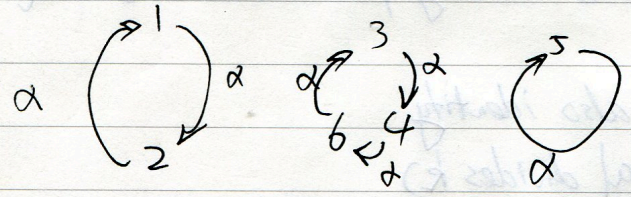
- Elements of S_n have the form $\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}$

~~The~~ S_n is called the symmetric group of degree n

$|S_n| = n!$

Cycle-notation:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$



$\alpha = (1,2)(3,4,6)(5)$

$(a_1, a_2, \cdots, a_m)$ is called a cycle of length m or an m-cycle.

$\alpha = (13)(27)(456)(8)$, $\beta = (1237)(648)(5)$

$\alpha\beta = \cdots$ disjoint cycle.

Properties of permutations.

Thm 5.1 : Products of disjoint cycles.

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Pf: Let α be a permt$\int$ on $A = \{1, \cdots, n\}$.

Say ~~a_1~~, $a_2 = \alpha(a_1)$, $a_3 = \alpha(\alpha(a_2))$ $\cdots$ until ~~$a_1 =$~~ $\alpha^m(a_1)$

then $\alpha = (a_1, \cdots, a_m) \cdots$

then we choose b_1 of A not in $a_1, \cdots, a_m$

$\cdots (b_1, \cdots, b_k)$ $\cdots$ similarly until it's ~~done~~ done

Thm 5.2 Disjoint cycles commute.

If pair of cycles $\alpha = (a_1, a_2, \cdots, a_m)$ and $\beta = (b_1, b_2, \cdots, b_n)$ have no common entries. then $\alpha\beta = \beta\alpha$.

Pf: $S = \{a_1, \cdots, a_m, b_1, \cdots, b_n, c_1, \cdots, c_k\}$

say a_i, $(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$

$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$

Similarly for b_i

then $c_i, \cdots$ = all equal to c_i so done

Thm 5.3 Order of a Permtn

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Pf: • n cycle has order n. (verify it)

• say α and β are disjoint cycles of lengths m & n. ($lcm = k$)

by Thm 4.1 both α^k & β^k are the identity permutation ε and since $\alpha\beta$ commute

$(\alpha\beta)^k = \alpha^k\beta^k$ is also identity.

By Cor 2 in Thm 4.1 ($a^k = e \Rightarrow |a|$ divides k)

say $|\alpha\beta| = t \Rightarrow t$ divides k.

then $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$

so $\alpha^t = \beta^{-t}$

However, it's clear that if α & β have no common symbol, the state is true for α^t & β^{-t}, since raising a cycle to a power does not introduce new symbols.

But if $\alpha^t = \beta^{-t}$ and no symbols $\Rightarrow$ both are identity.

then m & n must divide t.

means that k divides t also $\Rightarrow k = t$

inductively, it works for other cases.

order of $7! = 5040$ elements of S_7.

note that $(1\ 2\ \cdots\ n)$ is an n-cycle.

(7)
$(6)(1)$
$(5)(2)$

orders of the elements of S_7
(find those lcm)
$7, 6, 10, 5, 12, 4, 3, 2, 1$.

5 1 1
4 3
4 2 1
~~4 1 2~~
4 1 1 1
3 3 1
3 2 2
3 2 1 1
3 1 1 1 1
2 2 2 1
2 2 1 1 1
2 1 1 1 1 1 1
1 1 1 1 1 1 1

Thm 5.4. Product of 2-cycles.

Every permutation in S_n, $n>1$ is a product of 2-cycles.

Pf: note identity can be expressed as $(12)(12)$

so identity is a product of 2-cycles.

By Thm 5.1, every permtn can be written as

$$(a_1 \cdots a_k)(b_1 \cdots b_t) \cdots (c_1 \cdots c_s)$$

$$\Rightarrow (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(b_1 b_t)(b_1 b_{t-1}) \cdots (b_1 b_2) \cdots (c_1 c_s) \cdots (c_1 c_2)$$

Lemma If $\varepsilon = \beta_1 \cdots \beta_r$, β's are 2-cycles. then r is even. ∎

Pf. $r \neq 1$, since a 2-cycle is not the identity.

$r=2$, done.

induction.

4 cases for $\beta_{r-1}\beta_1$ (since $(ij) = (ji)$)

$\varepsilon = (ab)(ab)$

$(ab)(bc) = (ac)(ab)$

$(ac)(cb) = (bc)(ab)$

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

?

Thm 5.5 Always even or always odd.
If a p'mt'n α can be expressed as a product of an even(odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even(odd) number of 2-cycles.

If $\alpha = \beta_1\beta_2\cdots\beta_r$ & $\alpha = \gamma_1\gamma_2\cdots\gamma_s$ both
where β's & γ's are 2-cycles, then r, s are even/odd.

Pf: $\beta_1\cdots\beta_r = \gamma_1\cdots\gamma_s$
$\Rightarrow \varepsilon = \gamma_1\cdots\gamma_s\beta_r^{-1}\cdots\beta_2^{-1}\beta_1^{-1}$
$= \gamma_1\cdots\gamma_s\beta_r\cdots\beta_1$
since 2-cycle is its own inverse,
by lemma, s+r is even, $\Rightarrow$ both even/odd. ∎

Def'n: even & odd permutations
A p'm is even: can be expressed as a product of an even number of 2-cycles.
odd ...

Thm 5.6 Even per'ns form a group.
The set of even per'ns in S_n forms a subgroup of S_n.
(Ex 17)

Def: The group of even permutations of n symbols is denoted by A_n and is called the alternating group of degree n.

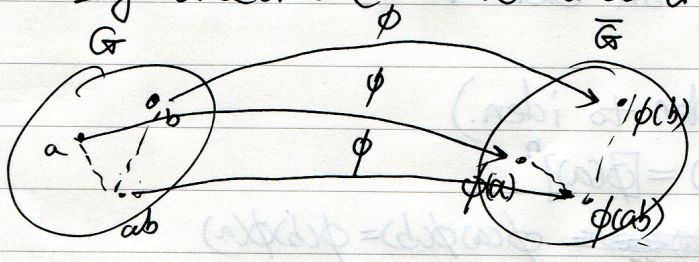
Thm 5.7 For $n>1$, A_n has order $\frac{n!}{2}$
Pf: 2 parts to show odd permutations number = even
For each odd per'n α, $(1\,2)\alpha$ is even
& $(1\,2)\alpha \neq (1\,2)\beta$ when $\alpha \neq \beta$
So at least many even p'n as odd ones.
vice versa.
so half-half.
$|S_n| = n! \Rightarrow |A_n| = \frac{n!}{2}$ ∎

Chapter 6 Isomorphisms

Def: Group Isomorphism
↳ ϕ from $G \to \bar{G}$ is 1-1 and onto map (function) that preserves the group operation.

ie. $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$

Say G & $\bar{G}$ are —ic and $G \approx \bar{G}$



G oper	$\bar{G}$ oper	Operation Preservation
+	+	$\phi(a+b) = \phi(a) + \phi(b)$
·	+	$\phi(a \cdot b) = \phi(a) + \phi(b)$
+	·	$\phi(a+b) = \phi(a) \cdot \phi(b)$
·	·	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

4 steps to verify iso.
① Mapping ② 1-1 ③ onto ④ O.P"

Cayley's thm
Thm 6.1
Every group is iso to a group of permutations

Pf: $\forall g \in G$, define a function T_g from G to G by

$$T_g(x) = gx, \quad \forall x \in G$$

(T_g is just multiple g on the left)

Prove T_g is a permutation on the set of elements of G.

Let $\bar{G} = \{T_g \mid g \in G\}$

it's under function composition.

why? $\forall g, h \in G$. ~~$T_g T_h = T_{gh}$~~

$$T_g T_h(x) = T_g(T_h(x)) = T_g(hx) = ghx = (gh)x = T_{gh}(x)$$

So $T_g T_h = T_{gh}$

So $T_g^{-1} = T_{g^{-1}}$ $\Rightarrow$ associative $\Rightarrow$ $\bar{G}$ is a group

$\forall g \in G$, $\phi(g) = T_g$. if $T_g = T_h \Rightarrow T_g(e) = T_h(e)$ or $ge = he$.
Thus $g = h$. ϕ is 1-1.
By $\overline{G}$ constructed like that, ϕ is onto.
$\phi(ab) = T_{ab} = T_a T_b = \phi(a)\phi(b)$.

Properties of iso.
Thm 6.2. properties acting on elements
ϕ is an iso : $G \to \overline{G}$.
① $\phi(e) = \bar{e}$ in $\overline{G}$ (carries iden to iden.)
② $\forall$ int. n, $\forall a \in G$, $\phi(a^n) = [\phi(a)]^n$.
③ $\forall a, b \in G$, $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$
④ $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$
⑤ $|a| = |\phi(a)|$, $\forall a \in G$ (preserves orders)
⑥ For fixed int k, fixed group element b in G,
$x^k = b$ has the same # of solutions in G
as does
$x^k = \phi(b)$ in $\overline{G}$.
⑦ If G is finite, then G & $\overline{G}$ has the same number of elements of every order.

Thm 6.3 — on groups
① ϕ^{-1} is iso $\overline{G} \to G$
② G is Abelian iff $\overline{G}$ is.
③ G is cyclic iff $\overline{G}$ is.
④ If K is a subgroup of G, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of $\overline{G}$.
⑤ $\overline{K}$ $\overline{G}$ $\phi^{-1}(\overline{K}) = \{g \in G | \phi(g) \in \overline{K}\}$ G
⑥ $\phi(Z(G)) = Z(\overline{G})$

Def: An iso $G \to G$ is automorphism of G.

Def: G be a group. $a \in G$. $\phi_a(x) = axa^{-1}$ $\forall x \in G$. is called the inner auto-- of G induced by a.

Thm 6.4 $Aut(G)$ and $Inn(G)$ are groups. (under function composition).

(Ex. 15)

Thm 6.5 $Aut(Z_n) \approx U(n)$

n: positive int. $Aut(Z_n)$ is iso to $U(n)$

Pf: $T: \alpha \to \alpha(1)$

$\alpha(k) = k\alpha(1)$ Why? For Z_n ... $\alpha(k) = \alpha(1 + \cdots + 1) = \alpha(1) + \alpha(1) \cdots + \alpha(1) = k\alpha(1)$

$\Rightarrow T$ is 1-1.

if $\alpha, \beta \in Aut(Z_n)$ & $\alpha(1) = \beta(1)$

then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$

$\alpha = \beta$

Let $r \in U(n)$ consider $\alpha: Z_n \to Z_n$ defined by

$\alpha(s) = sr \pmod n$ $\forall s \in Z_n$

--- α is in $Aut(Z_n)$ (see Ex 27)

Then since $T(\alpha) = \alpha(1) = r$, T is onto

Finally, OP

$T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(1 + \cdots + 1)$

$= \alpha(1) + \cdots + \alpha(1)$

$= \alpha(1)\beta(1)$

$= T(\alpha)T(\beta)$

■

Process of finding the disjoint cycle form of $\alpha\beta$.

$\alpha = (13)(27)(456)(8)$

$\beta = (1237)(648)(5)$

$\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$ (R to L)

For 1, (5) fixes 1, (648) fixes 1, (1237) sends 1 to 2, (8) fixes 1, (456) fixes 1, (27) sends 2 to 7, (13) fixes 7.

So the net effect of $\alpha\beta$ on 1 is sending 1 to 7.

For 7, $7 \to 7 \to 1 \to 1 \to 1 \to 1 \to 3$

For 3, $3 \to 3 \to 7 \to 7 \to 7 \to 2 \to 2$

For 2, $2 \to 3 \to 1$

So $\alpha\beta = (1732)(\cdots)\cdots$

For 4, $4 \to 8$

For 8, $8 \to 6 \to 4$

So $\alpha\beta = (1732)(48)\cdots$

For 5, $5 \to 6$

For 6, $6 \to 4 \to 5$

So $\alpha\beta = (1732)(48)(56)$ ✓

Review for Quiz 2.

Chapter 7 Cosets & Lagrange's Thm.

Def: G be a group, H is a nonempty subset of G.

$\forall a \in G$, $aH = \{ah \mid h \in H\}$, $Ha = \{ha \mid h \in H\}$, $aHa^{-1} = \{aha^{-1} \mid h \in H\}$

When H is a subgroup of G, we call aH the left coset of H in G containing a, Ha the right coset ...

a is the coset representative of Ha or aH.

2. properties of cosets and the related proofs

Chapter 7 Cosets & Lagrange's Theorem

Def: Coset of H in G.

Let G be a group and let H be a nonempty subset of G. $\forall a \in G$, the set $\{ah \mid h \in H\}$ is denoted ~~as~~ by aH. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a ~~*~~subgroup of G, the set aH is called the left coset of H in G containing a, whereas Ha is called ~~the right coset representative of aH (or Ha)~~ right coset of H in G containing a. In this case, the element a is called the coset representative of aH or (Ha). We use $|aH|$ to ~~dent~~ denote the number of elements in the set aH, and $|Ha|$ to denote the # of elements in the set Ha.

Lemma (Properties of Cosets)

Let H be a subgroup of G, and let a and b belong to G. Then,

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$
4. $aH = bH$ iff $a \in bH$
5. $aH = bH$ or $aH \cap bH = \emptyset$
6. $aH = bH$ iff $a^{-1}b \in H$.
7. $|aH| = |bH|$
8. $aH = Ha$ iff $H = aHa^{-1}$
9. aH is a subgroup of G iff $a \in H$.

~~Proof: 1. $a = ae \in aH$~~

~~2. Suppose $aH = H$. Then $a = ae \in aH = H$~~

~~3.~~

Lagrange's thm & Consequences.

Thm 7.1 Lagrange's Thm: $|H|$ divides $|G|$

Finite $H \leq G$, $|H|$ divides $|G|$

& $|G:H| = |G|/|H|$ # of ~~left cosets~~ or distinct (left)/(right) cosets.

Proof:

Cor 1: $|G:H| = |G|/|H|$

Cor 2: $|a|$ divides $|G|$

↳ order of each element of the finite group.

~~Cor 3~~: Pf: $|a| = |\langle a \rangle|$, by 7.1 $|\langle a \rangle|$ divides $|G|$.

Cor 3: A group of prime order is cyclic.

Pf: Sps $|G|$ is a prime, Let $a \in G$, $a \neq e$, $|\langle a \rangle|$ divides $|G|$ and $|\langle a \rangle| \neq 1$. Thus $|\langle a \rangle| = |G|$.

Cor 4: $a^{|G|} = e$

By Cor 2: $|G| = |a|k$, $\exists k \in \mathbb{Z}^+$. Thus

$$a^{|G|} = a^{|a|k} = e^k = e.$$

Cor 5: (Fermat's Little Thm): $\forall a \in \mathbb{Z}$, $\forall p$ is prime, $a^p \bmod p = a \bmod p$

Pf: If $a \equiv 0 \bmod p$, LHS $= 0^p = 0$, RHS $= 0$. True

If $a \not\equiv 0 \bmod p$, $a \in U(p)$, but $|U(p)| = p-1$, so by previous Cor. $a^{p-1} \equiv 1 \bmod p$

$$a^p \equiv a \bmod p.$$

Thm 7.2. Two finite subgroups H and K of a group, $HK = \{hk \mid h \in H, k \in K\}$ (set).

Then ~~$|HK| = |HK|$~~ $= \frac{|H||K|}{|H \cap K|}$

Pf: Let $t \in H \cap K$, $\forall t$, $hk = (ht)(t^{-1}k)$

So each group element in HK is represented by at least $|H \cap K|$ products in HK.

But $hk = h'k' \Rightarrow t = h^{-1}h' = kk'^{-1} \in H \cap K$, thus $h' = ht$, $k' = t^{-1}k$.

Thus each element in HK is represented by exactly $|H \cap K|$ products.

$\therefore |HK| = |H||K|/|H \cap K|$

Classification of groups of order $2p$,

Thm: for $p > 2$. G is a group of order $2p$, so G either $\simeq \mathbb{Z}_{2p}$ or $G \simeq D_p$.

proof

Chapter 8 External Direct products.

Def: $G_1, \cdots, G_n$ a finite collection of groups. The EDP of $G_1, \cdots, G_n$ is $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, \cdots, g_n) \mid g_i \in G_i\}$$

rule: $(g_1, \cdots, g_n)(g_1', \cdots, g_n') = (g_1 g_1', \cdots, g_n g_n')$

$U(8) \oplus U(10)$: $(3,7)(7,9) = (21 \bmod 8, 63 \bmod 10) = (5,3)$

- $|G_1 \oplus \cdots \oplus G_n| = |G_1| \cdots |G_n|$

Prop: $|G| = 4$, either $G \cong Z_4$ or $G \cong Z_2 \oplus Z_2$

↙ $g \in G$, $|g| = 4$, cyclic!

↘ $|g| = |\langle g \rangle|$, $\langle g \rangle \mid |G|$ so g has order 1 or 2

$G = \{e, a, b, ab\}$

$\phi(e) = (0,0)$

$\phi(a) = (1,0)$

$\phi(b) = (0,1)$

$\phi(ab) = (1,1)$

Thm 8.1. Order of an element in a Direct Product

Sps $G_1, \cdots, G_n$ are finite groups, then

$$|(g_1, \cdots, g_n)| = \operatorname{lcm}(|g_1|, \cdots, |g_n|)$$

Pf: Let $s = \operatorname{lcm}(|g_1|, \cdots, |g_n|)$, $t = |(g_1, \cdots, g_n)|$

$(g_1, \cdots, g_n)^s = (e_1, \cdots, e_n)$, $t \le s$

& $(g_1^t, \cdots, g_n^t) = (g_1, \cdots, g_n)^t = (e_1, \cdots, e_n)$, $s \le t$.

so $s = t$.

Thm 8.2 Criterion for $G \oplus H$ to be cyclic:

G, H, finite cyclic groups, $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime

Pf: ($\Leftarrow$). r.p. let $g \in G$, $h \in H$. Then $|(g,h)| = \operatorname{lcm}(|g|, |h|)$

$$= \operatorname{lcm}(|G|, |H|)$$

$$= \frac{|G||H|}{\gcd(|H|, |G|)}$$

$$= |G| \cdot |H|$$

($\Rightarrow$)

Cor. 1. Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to be cyclic.

$|G_i|$ & $|G_j|$ r.p.

Cor 2. Criterion for $Z_{n_1 \cdot n_2 \cdots n_k} \approx Z_{n_1} \oplus \cdots \oplus Z_{n_k}$

Let $m = n_1 \cdots n_k$, Z_m is iso to $Z_{n_1} \oplus \cdots \oplus Z_{n_k}$ iff n_i and n_j are r.p. when $i \neq j$.

Thm 8.3 $U(n)$ as an EDP.

Sps s & t are r.p. Then $U(st) \approx U(s) \oplus U(t)$

moreover $U_s(st) \approx U(t)$

$U_t(st) \approx U(s)$

Cor: if $m = n_1 \cdot n_2 \cdots n_k$, $\gcd(n_i, n_j) = 1$, for $i \neq j$. Then

$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$

Gauss thm:

$U(2) \approx \mathbb{Z}$

$U(4) \approx \mathbb{Z}_2 + \mathbb{Z}_2$

$U(2^n) \approx \mathbb{Z}_2 + \mathbb{Z}_{2^{n-1}}$

$U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$ where p is an odd prime

Chapter 9 Normal Subgroups & Factor Groups

Def: G, $H \leq G$, H is a normal subgroup of G if $aH = Ha \ \forall a \in G$. $H \lhd G$.

Thm §9.1. Normal subgroup test.
A subgroup H of G is normal in G iff $xHx^{-1} \subseteq H$ for $x \in G$.

Prop: Sps $H \lhd G$, $K \leq G$, Let $HK = \{hk \mid h \in H, k \in K\}$ Then $HK \leq G$.

Factorgroups: Let $H \lhd G$, set $G/H = \{aH \mid a \in G\}$ is a group
under the operation $= \{Ha \mid a \in G\}$ when H is normal.
$(aH)\cdot(bH) = abH$
$\forall a, b \in G$.
Converse is true.

Prop: Let $H \lhd G$, $a, a' \in G$, $b, b' \in G$ s.t. $aH = a'H$, $bH = b'H$. Then $abH = a'b'H$

For G/H
eH is identity: $aH \cdot eH = aeH = aH$
$(aH)^{-1} = a^{-1}H$ $(a^{-1}H \cdot aH = a^{-1}aH = eH = H)$
multiplication in assaociativity as well.

$H \lhd G \iff$ the G/H is well-defined.

Prop: let $n \geq 0$, then $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}_n$

Fact: If $H \leq G$, $|G:H| = 2$ then $H \lhd G$.

Thm: If $G/Z(G)$ is cyclic, the G is abelian.

Thm (Cauchy's Thm for Abelian group).
G, finite abelian group & let p be a prime # dvrging $|G|$,
$\exists\, g \in G$ s.t. $|g| = p$.