MATCO1 NOTES

BINARY OPERATION

Let G be a set. A binary operation is defined to be a function $*: G\times G \mapsto G$ that maps/assigns each ordered pair of elements in G to another element in G.

GROUP

A group is a pair $(G,*)$ consisting of a set $G\neq\emptyset$ and a binary operation $*$ on G ~~st~~ satisfying:

1. $*$ must be associative for each $g\in G$. $\Rightarrow \forall g_1,g_2,g_3\in G, (g_1*g_2)*g_3 = g_1*(g_2*g_3)$
2. the existence of an identity element in G. $\Rightarrow \forall g\in G, \exists e\in G$ s.t. $e*g=g=g*e$
3. for each $g\in G$, the exists a 2-sided inverse $\Rightarrow \forall g\in G, \exists g^{-1}\in G$, s.t. $g^{-1}*g=e=g*g^{-1}$

CAYLEY TABLE (OPERATION TABLE)

$*$	g_1 g_2 $\cdots$ g_n
g_1	g_1*g_2 g_2*g_1 $\cdots$
g_2	$\vdots$. g_2*g_n
g_n	

where $G=\{g_1,g_2,\cdots,g_n\}$, $*$ is the binary operator of G.
g_i is identity of G if $g_i*g_j=g_j*g_i=g_j$
$g_i\in Z(G)$ if $g_i*g_j=g_j*g_i$

EXAMPLE OF GROUPS

GROUP	OPERATION	IDENTITY	FORM OF ELEMENT	INVERSE	ABELIAN
$\mathbb{Z}$ - integers	Addition	0	k	$-k$	yes
$\mathbb{Q}^+$ - positive rationals	Multiplication	1	$\frac{m}{n}$ $m,n>0$	$\frac{n}{m}$	yes
$\mathbb{Z}_n$ - integers modulo n	Addition mod n	0	k	$n-k$	yes
$\mathbb{R}^*$ - reals w/o 0	Multiplication	1	x	$\frac{1}{x}$	yes
$\mathbb{C}^*$ - complex w/o 0	Multiplication	1	$a+bi$	$\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i$	yes
$GL(2, \mathbb{Q}/\mathbb{R}/\mathbb{C}/\mathbb{Z}^+)$ - general lin group	Matrix Multiplication	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}a&b\\c&d\end{bmatrix}$	$\frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix}$	no
$U(n)$ - ~~multiplication~~ units modulo n	multiplication mod n	1	k, $\gcd(k,n)=1$	solution to $kx \bmod n=1$	yes
$\mathbb{R}^n$	componentwise addition	$(0,0,\cdots,0)$	$(a_1,a_2,\cdots,a_n)$	$(-a_1,-a_2,\cdots,-a_n)$	yes
$SL(2,\mathbb{Q}/\mathbb{R}/\mathbb{C}/\mathbb{Z}^+)$ - special lin group	Matrix Multiplication	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}a&b\\c&d\end{bmatrix}$	$\begin{bmatrix}d&-b\\-c&a\end{bmatrix}$	no
D_n - dihedral group	Composition	R_0	R_α, L reflection	$R_{360-\alpha}$, L	no
S_n - symmetric group	Composition	(1)	$(a\ b \cdots d)$		no
A_n - alternating group	Composition	(1)	$\alpha\in S_n$ s.t. α even		no

DIHEDRAL GROUPS D_n

The set of ~~sv~~ plane symmetries of a regular n-gon with composition.

ORDER

Let G be a group. The order of G ($|G|$) is the size of G. The order of an element $g\in G$ ($|g|$) is the smallest positive number n s.t. $g^n=e$. If no such n, then g has infinite order.

PERMUTATION

Bijection from non-empty set X to X. Is a group under $\circ$ composition

5 CONDITIONS TO VERIFY FOR GROUP

1. Set $S \neq \emptyset$
2. Closure under operation $*$
3. Associativity
4. Existence of identity $e \in S$
5. Existence of inverse $a^{-1} \in S \ \forall a \in S$

CHECK CAYLEY TABLE

- identity: same row and col # ~~have co~~ is a copy of row/col header

CYCLE / K-CYCLE

Let $X = \{1, 2, \cdots, n\}$ Let $n \in \mathbb{Z}^+$, $a_1, a_2, \cdots, a_n \in X$ distinct. $(a_1\ a_2 \cdots a_k)$ is a cycle or k-cycle representing the permutation $\begin{matrix} a_1 \mapsto a_2 \\ a_2 \mapsto a_3 \\ \vdots \\ a_k \mapsto a_1 \end{matrix}$ and fixes everything else.

SYMMETRIC GROUP OF DEG n S_n

Group of permutations on set $X = \{1, 2, \dots, n\}$

MODULAR ARITHMETIC

Let $a, n \in \mathbb{Z}$, $n > 0$. $\exists q, r \in \mathbb{Z}$ s.t. $a = nq + r$ where $0 \leq r < n$

- addition modulo n = $(a+b) \bmod n$
- multiplication modulo n = $(ab) \bmod n$

INTEGERS MODULO N

Let $n \in \mathbb{Z}^+$. $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$. ~~is called~~

GROUP: $(\mathbb{Z}_n, + \bmod n)$

UNITS MODULO N

Let $n \in \mathbb{Z}^+$. $U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

GROUP: $(\mathbb{Z}_n, \cdot \bmod n)$

UNIQUENESS OF IDENTITY

If G is a group then the identity element e is unique.

CANCELLATION

If G is a group then
1. $\forall a, b, c \in G$, $ac = bc \Rightarrow a = b$ (right cancellation law)
2. $\forall a, b, c \in G$, $ca = cb \Rightarrow a = b$ (left cancellation law)

UNIQUENESS OF INVERSE

Let G be a group. $\forall g \in G$ $\exists$ a unique $g^{-1} \in G$ s.t. $g^{-1}g = e = gg^{-1}$

SOCKS-SHOES PROPERTY

For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

ABELIAN

Let G be a group. G is abelian if $gh = hg$, $\forall g, h \in G$. If a group is not abelian, we call G non-abelian.

SUBGROUP

Let G be a group. If $H \subseteq G$ and $H \neq \emptyset$ is itself a group under the same group operation as G, then H is a subgroup of G ($H \leq G$). $H < G$ = proper subgroup

ONE-STEP SUBGROUP TEST

Let G be a group and $H \subseteq G$ and $H \neq \phi$. If $h_1 h_2^{-1} \in H$ $\forall h_1, h_2 \in H$. Then $H \leq G$.

TWO-STEP SUBGROUP TEST

Let G be a group. Let $H \subseteq G$ and $H \neq \phi$. If

1. $h_1 h_2 \in H$, $\forall h_1, h_2 \in H$ closure
2. $h^{-1} \in H$, $\forall h \in H$ inverses Then $H \leq G$

CYCLIC GROUP

Let G be a group. Let $a \in G$. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is called the cyclic subgroup of G generated ~~by~~ by a.

If $\langle a \rangle = G$, we say G is a cyclic group generated by a.

CENTER

Let G be a group. $Z(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$ i.e. all elements in G that commute with every elements of G.

CENTER IS A SUBGROUP

The center of a group is a subgroup of G.

CENTRALIZER

Let a be a fixed element of a ~~gr~~ group G. The centralizer of a in G, $C(a)$, is the set of all elements in G that commute with a. $C(a) = \{g \in G \mid ga = ag\}$

For each a in a group G. the centralizer of a is a subgroup of G.

CRITERION FOR $a^i = a^j$

Let G be a group, let $a \in G$. If a has infinite order, then $a^i = a^j \iff i = j$

If a has finite order s.t. $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ $\iff n \mid i-j$

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

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

$a^k = e \Rightarrow |a| \mid k$

Let G be a group, $a \in G$, $|a| = n$. If $a^k = e$, then n divides k $\quad n \mid k$

$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$ $\quad a \in G$, $|a| = n$, $k \in \mathbb{Z}^+$

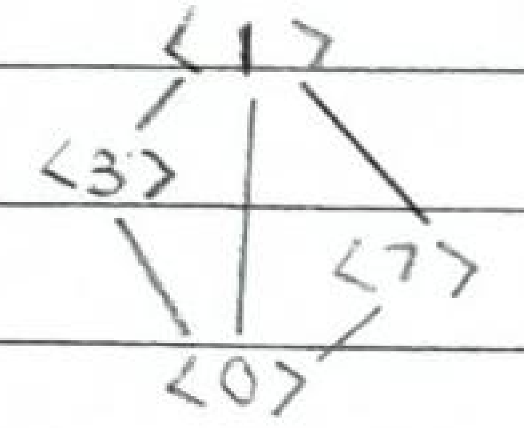
THE FUNDAMENTAL THM OF CYCLIC GROUPS (FTOCG)

1. Every subgroup of a cyclic group is cyclic.
2. If $|\langle a \rangle| = n$ and H is ~~any~~ any subgroup of $\langle a \rangle$, then $|H| \mid n$
3. Suppose $|\langle a \rangle| = n$. For each positive divisor k of n. $\langle a \rangle$ has exactly one subgroup of order k. $\langle a^{\frac{n}{k}} \rangle$

Subgroups Of $\mathbb{Z}_n$

For each positive divisor k of n, the set $\langle \frac{n}{k} \rangle$ is a unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$

LATTICE DIAGRAM



LARGEST ORDER

SMALLEST ORDER

$|\mathbb{Z}_{21}| = 21 = n$

$\langle \frac{21}{1} \rangle = \langle 21 \rangle = \{0\}$

$\langle \frac{21}{3} \rangle = \langle 7 \rangle = \{0, 7, 14\}$

$\langle \frac{21}{7} \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18\}$

$\langle \frac{21}{21} \rangle = \langle 1 \rangle = \mathbb{Z}_{21}$

Disjoint Cycles

A pair of ~~any~~ cycles $\alpha = (a_1 a_2 \cdots a_k)$, $\beta = (b_1 b_2 \cdots b_l)$ that have no common entries i.e. $a_i \neq b_j \ \forall i, j$

Product Of Disjoint Cycles

Every element of S_n is either a cycle or can be written uniquely (up to order) as a product of disjoint cycles.

Disjoint Cycles Commute

Disjoint cycles commute. If α and β are ~~dy~~ disjoint, then $\alpha\beta = \beta\alpha$

Order Of A Permutation

Let $\alpha \in S_n$. If α is written as a product of disjoint cycles $\alpha = \alpha_1 \alpha_2 \cdots \alpha_n$ then $|\alpha| = \text{lcm}\{l_1, l_2, \cdots, l_m\}$ where l_i is the length of cycle α_i

Cycle Type Of $\alpha \in S_n$

Let $\alpha \in S_n$. Let $\alpha = \alpha_1 \alpha_2 \cdots \alpha_m$ be a decomposition of α into disjoint cycles. Let l_i be the length of α_i for each i. The cycle type of α is a list in decreasing order of the l_i's.

Product Of 2-Cycles (Tranpositions)

Every permutation in S_n $(n>1)$ can be written as a product of 2-cycles

Odd And Even Permutations

Even: a permutation can be expressed as an even number of transpositions

Odd: a permutation can be expressed as an ~~d~~ odd number of transpositions

Alternating Group Of Degree N

$A_n = \{\alpha \in S_n \mid \alpha \text{ is even}\}$ is called the alternating group of degree n, and is a subgroup of S_n

For $n > 1$, A_n has order $\frac{n!}{2}$

Number Of Permutations Of Certain Cycle Type

$$\frac{n!}{k_1! \cdots k_s! \, n_1^{k_1} \cdots n_s^{k_s}}$$

where k_i = # cycles with length n_i

n_i = length of a cycle (distinct)

HOMOMORPHISM

Let $G, \bar{G}$ be groups. A homomorphism is a map $\phi: G \to \bar{G}$ s.t. $\underset{\text{operation in } G}{\phi(ab)} = \underset{\text{operation in } \bar{G}}{\phi(a)\phi(b)}$ $\forall a, b \in G$

ISOMORPHISM

An isomorphism is a homomorphism that is bijective $G \cong \bar{G}$ or $G \simeq \bar{G}$

EXAMPLES

$\phi: G \to \bar{G}$ $\phi(g) = \bar{e}$ $\forall g \in G$ trivial homomorphism

$\phi: G \to G$ $\phi(g) = g$ $\forall g \in G$ identity homomorphism / trivial isomorphism

if $H \leq G$, then $\phi: H \to G$ $\phi(h) = h$ $\forall h \in H$ inclusion homomorphism

KERNEL

Let $G, \bar{G}$ be groups. Let $\phi: G \to \bar{G}$ is a homomorphism. The set $\ker(\phi) = \{g \in G \mid \phi(g) = \bar{e}\} \subseteq$ is called kernel of ϕ.

KER$(\phi) \leq G$

Let $G, \bar{G}$ be groups. Let $\phi: G \to \bar{G}$ be a homomorphism. Then $\ker(\phi) \leq G$

PROPERTIES OF HOMOMORPHISMS

Let $G, \bar{G}$ be groups. Let $\phi: G \to \bar{G}$ be a homomorphism. Then

1. $\phi(e) = \bar{e}$
2. $\phi(g^n) = (\phi(g))^n$, $\forall g \in G, n \in \mathbb{Z}$
3. If $|g| < \infty$ then $|\phi(g)| \mid |g|$
4. ϕ is injective $\Leftrightarrow \ker(\phi) = \{e\}$

IMAGE OF H UNDER ϕ

Let $H, \bar{H}$ be a group. Let $\phi: H \to \bar{H}$ be a homomorphism. $\phi(H) = \{\phi(h) \in \bar{H} \mid h \in H\}$ is the image of H under ϕ.

PROPERTIES OF SUBGROUPS UNDER HOMOMORPHISM

Let $G, \bar{G}$ be groups. Let $\phi: G \to \bar{G}$ be a homomorphism. Let $H \leq G$. Let $\phi(H)$ be the image of H under ϕ. Then

1. $\phi(H) \leq \bar{G}$
2. If H is cyclic then $\phi(H)$ is cyclic
3. If H is abelian then $\phi(H)$ is abelian

$\Big\}$ iff for ϕ isomorphism.

CAYLEY'S THM

Let G be a group. If $|G| < \infty$ then G is isomorphic to a subgroup of S_n for some $n \in \mathbb{Z}^+$.

EQUAL NUMBER OF ORDER N ELEMENTS

Let $G, \bar{G}$ be groups. Suppose $|G| < \infty$. Let $\phi: G \to \bar{G}$ be an isomorphism. Then for any $n \in \mathbb{Z}^+$, the number of elements in G of order n is equal to the number of elements in $\bar{G}$ of order n.

AUTOMORPHISM

Let G be a group. An automorphism ϕ is an isomorphism $\phi: G \to G$. $Aut(G)$

AUTOMORPHISM AS A GROUP

Let G be a group. The set $Aut(G) = \{\phi : G \to G \mid \phi$ is automorphism$\}$ with the operation of composition is a group.

$\forall n \in \mathbb{Z}^+, Aut(\mathbb{Z}_n) \cong U(n)$

LEFT / RIGHT - COSET OF H IN G CONTAINING a

Let G be a group. Let $H \leq G$ and $a \in G$. The set $\{ah \mid h \in H\} = aH$ is a left-coset of H in G containing a. $\{ha \mid h \in H\} = Ha$ is a right-coset of H in G containing a. a is the coset representative of aH or Ha.

COSET PROPERTIES

Let G be a group. Let $H \leq G$. Let $a, b \in G$. Then

1. $a \in aH$
2. $aH = H \iff a \in H$
3. $aH = bH \iff a \in bH$
4. $aH = bH \iff a^{-1}b \in H$
5. $aH = bH$ or $aH \cap bH = \phi$
6. $|aH| = |bH|$
7. $aH = Ha \iff H = a^{-1}Ha^{-1}$
8. aH is subgroup of $G \iff a \in H$

LAGRANGE'S THM

Let G be a group. Let $H \leq G$. If $|G| < \infty$, then

1. $|H| \mid |G|$
2. the distinct left / right cosets of H in G equals $\frac{|G|}{|H|} = |G:H|$

INDEX OF H IN G

Let G be a group. Let $H \leq G$. The index of H in G is the number of distinct left cosets of H in G. $|G:H|$

|a| DIVIDES |G|, $a^{|G|} = e$

Let G be a finite group and $a \in G$. $|a| \mid |G|$ and $a^{|G|} = e$

FERMAT'S LITTLE THM

Let G be a finite group. if $a \in \mathbb{Z}$ and $p \geq 2$ and is prime then $a^{p-1} \equiv 1 \bmod p$

NORMAL SUBGROUP

Let G be a group. Let $H \leq G$. H is normal $\iff aH = Ha \ \forall a \in G$. $H \trianglelefteq G$

NORMAL SUBGROUP TEST

~~Suppose~~ Let G be a group. Let $H \leq G$, $H \trianglelefteq G \iff aHa^{-1} \subseteq H, \forall a \in G$, where $aHa^{-1} = \{aha^{-1} \mid h \in H\}$

QUOTIENT GROUP (FACTOR GROUP)

Let G be a group. Let $H \trianglelefteq G$, the set $\frac{G}{H} = \{aH \mid a \in G\}$ is a group with operation

* $(aH) * (bH) = (ab)H$. $\frac{G}{H}$ is called quotient group.

1st ISOMORPHISM THM

Let $G, \bar{G}$ be groups. Let $\phi: G \to \bar{G}$ be a homomorphism

Then i. $Ker(\phi) \trianglelefteq G$

ii. $\frac{G}{Ker(\phi)} \cong \phi(G)$ (Image of G)

COROLLARY OF 1st ISO THM

If ϕ is a homomorphism ~~from~~ s.t. $\phi: G \to \bar{G}$ ~~or~~, where $G, \bar{G}$ are finite groups, then $|\phi(G)|$ divides both $|G|$ and $|\bar{G}|$. $|\bar{G}|, |G| < \infty$ and $\phi: G \to \bar{G} \Rightarrow |\phi(G)| \mid |G|$ and $|\phi(G)| \mid |\bar{G}|$