GROUP THEORY 32001

OUTLINE OF COURSE:-

§1 REVISION OF SUBGROUPS, COSETS

§2 MORE EXAMPLES OF GROUPS

§3 SUBGROUPS

§4 CONJUGACY, CLASS EQUATION

§5 GROUP ACTIONS

§6 FINITELY GENERATED ABELIAN GROUPS

§7 NORMAL SUBGROUPS, FACTOR GROUPS

§8 SIMPLE GROUPS, JORDAN HÖLDER THEOREM

§9 SYLOW'S THEOREMS, APPLICATIONS

<u>BOOKS</u> 1) A FIRST COURSE IN ABSTRACT ALGEBRA by J. FALEIGH (Addison Wesley)

2) CONTEMPORARY ABSTRACT ALGEBRA by J. GALLIAN (Houghton Mifflin)

§1 REVISION OF SUBGROUPS, COSETS

Definition 1.1 $(G, *)$ is a group if G is a non-empty set such that

(G1) $\forall\, a, b \in G$, $a * b \in G$ ($*$ is a binary operation on G — now write ab for $a*b$)

(G2) $(ab)c = a(bc)$ $\forall\, a, b, c \in G$

(G3) $\exists\, 1_G \in G$ s.t. $1_G a = a = a 1_G$ $\forall\, a \in G$

(G4) $\forall\, a \in G$ $\exists\, a^{-1} \in G$ s.t. $aa^{-1} = 1_G = a^{-1}a$.

Note: usually write G for $(G, *)$, $*$ being understood, hopefully, from context. Similarly usually write 1 for 1_G (1 is the identity element of G). 1_G is unique. For each $a \in G$, a^{-1} is unique.

Definition 1.2 Let G be a group. A non-empty subset ~~of~~ H of G is a subgroup (of G), and we write $H \leq G$, if H forms a group under the restriction of $*$ to H ($*$ being the binary operation of G).

<u>Remarks</u> (i) If $H \leq G$, then $1_G \in H$ (so $1_G = 1_H$).
(ii) If $H \leq G$ and $K \leq G$ and $K \subseteq H$, then $K \leq H$.

<u>Lemma 1.3</u> (Subgroup criterion) Suppose G is a group and $H \subseteq G$. Then $H \leq G \Longleftrightarrow H \neq \phi$ and $\forall\, a, b \in H$ we have $ab^{-1} \in H$.

<u>Definition 1.4</u> Suppose G is a group and $H \leq G$. For $a \in G$ we define the <u>right coset</u> Ha by

$$Ha = \{ha \mid h \in H\} \quad (\subseteq G)$$

All you need to know about right cosets:-

Theorem 1.5 Suppose G is a group and $H \leq G$.

(i) If $g \in G$, then $g \in Hg$.

(ii) Let $a, b \in G$. Then $Ha = Hb \iff ab^{-1} \in H$.

(iii) Let $a, b \in G$. Then either $Ha = Hb$ or $Ha \cap Hb =$

(iv) G is the disjoint union of the right cosets of H.

(v) If $g \in G$, then $|H| = |Hg|$ (meaning H and Hg have the same cardinality).

Proof (i) $H \leq G \Rightarrow 1 \in H$. So $g = 1g \in \{hg \mid h \in H\} = Hg$.

(ii) Suppose $Ha = Hb$. Then, by (i), $a \in Ha = Hb$. Hence $a = hb$ for some $h \in H$. $\therefore ab^{-1} = h \in H$.

Now suppose $ab^{-1} \in H$. So $ab^{-1} = h_1 \in H \Rightarrow a = h_1 b$.

$\therefore Ha = \{ha \mid h \in H\} = \{hh_1 b \mid h \in H\} \subseteq Hb$, and $Hb = \{hb \mid h \in H\} = \{hh_1^{-1}h_1 b \mid h \in H\} = \{hh_1^{-1}a \mid h \in H\}$ $\subseteq Ha$. Hence $Ha = Hb$.

(iii) If $Ha \cap Hb \neq \emptyset$, then $h_1 a = h_2 b$ for some $h_1, h_2 \in H$. $\therefore$ $ab^{-1} = h_1^{-1} h_2 \in H \Rightarrow Ha = Hb$ by (ii). So (iii) holds.

(iv) follows from (i) and (iii).

(v) the map $\varphi : H \to Hg$ defined by $\varphi : h \mapsto hg$ $(h \in H)$ is (1-1) and onto.

In the situation of ~~the~~ Definition 1.4 a left coset aH is defined by

$$aH = \{ah \mid h \in H\} \quad (\subseteq G).$$

Have results for left cosets analogous to Theorem 1.5 ((ii) is: $aH = bH \Leftrightarrow b^{-1}a \in H$)

For G a group and $H \leq G$, $[G : H]$ denotes the number (cardinality) of the set of right cosets of H — called the index of H in G.

<u>Theorem 1.6</u> Suppose G is a finite group and $H \leq G$.

(i) (Lagrange's theorem) $|G| = [G:H]|H|$ (in particular, the order of H divides the order of G).

(ii) If $K \leq G$ and $K \subseteq H$, then $[G:K] = [G:H][H:K]$.

Proof Thm 1.5 (iv), (v) $\Rightarrow$ (i). Use (i) twice to get (ii).

<u>Symmetric groups</u> Let $\Omega = \{1, 2, \ldots, n\}$. A (1-1), onto map from Ω to Ω is called a <u>permutation of Ω</u>. Let S_Ω (or S_n) denote the set of all permutations of Ω. For $f, g \in S_n$ define $f * g$ by

$$\alpha(f*g) = (\alpha f)g \quad , \ \alpha \in \Omega.$$

($*$ is just composition of maps)

NOTE maps are written on the RIGHT (of elements of Ω) – will ALWAYS do this for permutations (REASON? – a little later).

Theorem 1.7 (i) $(S_n, *)$ is a group.
(ii) $|S_n| = n!$

Cycle notation $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are distinct elements of Ω denotes the following permutation in S_n:

$$\begin{aligned} \alpha_1 &\mapsto \alpha_2 \\ \alpha_2 &\mapsto \alpha_3 \\ &\vdots \\ \alpha_{r-1} &\mapsto \alpha_r \\ \alpha_r &\mapsto \alpha_1 \end{aligned} \qquad \alpha \mapsto \alpha \ \forall \alpha \in \Omega \setminus \{\alpha_1, \ldots, \alpha_r\}$$

cycle of length r

Cycles $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ and $(\beta_1, \beta_2, \ldots, \beta_s)$ are disjoint cycles $\iff$

$$\{\alpha_1, \ldots, \alpha_r\} \cap \{\beta_1, \ldots, \beta_s\} = \phi.$$

<u>Theorem 1.8</u> Any permutation in S_n can be written as a product of (pairwise) disjoint cycles.

<u>EXAMPLE</u> S_9 (so $n=9$ and $\Omega=\{1,2,\ldots,9\}$)

(i) α:

$1 \mapsto 3$	$4 \mapsto 6$	$7 \mapsto 1$
$2 \mapsto 9$	$5 \mapsto 7$	$8 \mapsto 4$
$3 \mapsto 5$	$6 \mapsto 8$	$9 \mapsto 2$

Another notation: $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 5 & 6 & 7 & 8 & 1 & 4 & 2 \end{pmatrix}$

As a product of disjoint cycles: $\alpha = (1\,3\,5\,7)(2\,9)(4\,6\,8)$.

(ii) Multiplying permutations – this is why we write permutations on the right of elements of Ω.

Let $\beta = (9\,8\,7\,6\,5)(1\,2)(3)(4) \in S_9$. Then

$\alpha\beta = (1\,3\,5\,7)(2\,9)(4\,6\,8)(9\,8\,7\,6\,5)(1\,2)(3)(4)$

[NOTE: RHS <u>not</u> expressed as a product of disjoint cycles – YET]

$= (1\,3\,9)(2\,8\,4\,5\,6\,7)$.

What is $\beta\alpha$?