§2. Subgroups, Cosets and Indices, Quotient Groups.

(A). If a non-empty subset H of a group G is closed with respect to the inversion and multiplication in G, it forms a group in its own right. For the group laws I, II and III hold in G and therefore certainly hold also in H. Such a subset is called a <u>subgroup</u> of G. The study of particular groups is largely bound up with the discovery and study of the subgroups they contain.

Let H be a subgroup of G and let $\alpha \in H$. Then $\alpha^{-1} \in H$ and so $\alpha\alpha^{-1} = 1 \in H$. Every subgroup H of G contains the unit element of G and this is at the same time the unit element of H. Since $1^{-1} = 1.1 = 1$, the unit element taken by itself is a subgroup, the <u>unit subgroup</u> of G. We do not need to make a pedantic distinction between the unit element 1 of G and the unit subgroup which has 1 as its sole element.

<u>Lemma 2·1</u> Let $(H_\lambda)_{\lambda\in\Lambda}$ be any family of subgroups of a group G. Then their intersection

$$H = \bigcap_{\lambda\in\Lambda} H_\lambda$$

is also a subgroup of G.

For H contains 1 and so it is not empty. And it inherits the requisite closure properties from the subgroups H_λ.

Note that the intersection of two sets X and Y is usually written $X \cap Y$.

(B). Let X be any subset of G. The intersection of all the subgroups of G which contain X is called the subgroup _generated_ by X and written $\{X\}$. It is the smallest subgroup of G which contains X.

Lemma 2.2 If X is not empty, $\{X\}$ consists of all elements of G which are expressible in at least one way as a product of elements of the set $X \cup X^{-1}$.

Here $X \cup Y$ is the _union_ of the sets X and Y and consists of all elements which belong to ~~both~~ at least one of these two sets. Obviously $\{X\}$ must contain all products of elements of $X \cup X^{-1}$. But the set of all such products is closed with respect to multiplication, and also by 1.5 with respect to inversion. Hence it is a subgroup containing X, and contained in $\{X\}$. Therefore it coincides with $\{X\}$ by definition.

If $H, K, L, \ldots$ are subgroups of G, then $\{H \cup K \cup L \cup \cdots\}$ is usually written $\{H, K, L, \ldots\}$. It is the _join_ of $H, K, L, \ldots$; the smallest subgroup which contains them all.

If $P(\xi, \eta, \cdots)$ is a proposition involving certain elements $\xi, \eta, \cdots$ of a group, then $\{\xi, \eta, \cdots ; P(\xi, \eta, \cdots)\}$ denotes the subgroup generated by all $\xi, \eta, \cdots$ for which $P(\xi, \eta, \cdots)$ is true.

A subset X of a group G such that $\{X\} = G$ is called a _set of generators_ of G. Such a set can usually be chosen in many different ways. $X = G$ is always a possible choice.

A group which can be generated by a single element is called _cyclic_. Every element ξ of a group G generates a cyclic subgroup $\{\xi\}$ and 1.3 shows that this consists of all the powers ξ^m of ξ. $m = 0, \pm 1, \pm 2, \cdots$; it shows also that all cyclic groups are Abelian.

(C). If G is a group, $|G|$ is called the <u>order</u> of G. Unless the contrary is stated, all groups considered will be finite. If $\xi \in G$, the order of $\{\xi\}$ is also called the order of ξ.

Let H be a subgroup of G. The sets $H\xi$ with $\xi \in G$ are called the <u>cosets</u> of H in G. If X is any subset of G, the set HX is the union of a certain number of cosets of G and this number is denoted by $|HX : H|$. This notation is justified by

<u>Lemma 2.3</u> Distinct cosets of H in G have no common element. $|HX| = |HX : H| . |H|$ for any subset X of G.

Proof: Let $\zeta \in H\xi$. Then $\zeta = \eta\xi$ with $\eta \in H$. Hence $\xi = \eta^{-1}\zeta \in H\zeta$ since $\eta^{-1} \in H$. But H contains 1 and is closed with respect to multiplicati[on]. Hence $HH = H$ and so $H\xi = H\zeta$. Therefore if two cosets $H\xi$ and $H\xi'$ have an element ζ in common, they both coincide with $H\zeta$. By 1.6, $|H\xi| = |H|$ for all $\xi \in G$ and so $|HX| = |HX : H| . |H|$ by definition of $|HX|$.

Obviously $G = HG$. The number $|G : H|$ is the total number of cosets of H in G. It is called the <u>index</u> of H in G. An immediate corollary of 2.3 is

<u>Theorem 2.4</u> Let H be a subgroup of G. Then $|G| = |G : H| . |H|$. The order of H and also its index in G divides the order of G. ~~The~~ In particular, the order of every element of G divides $|G|$.

(D). This theorem is usually attributed to J.L. Lagrange 1736-1813. For <u>cyclic groups</u>, a much more precise result holds good. This is

<u>Theorem 2.5</u> Let $G = \{\xi\}$ be a cyclic group of order n. Then the n elements of G are $1, \xi, \xi^2, \ldots, \xi^{n-1}$; and $\xi^n = 1$. For each divisor d of n, G has one and only one subgroup of order d viz. $\{\xi^{n/d}\}$ with elements $1, \xi^{n/d}, \xi^{2n/d}, \ldots, \xi^{(d-1)n/d}$. All subgroups of a cyclic group are cyclic.

Note that ξ^n is the first positive power of ξ which is equal to 1. $\xi^N = 1$ if and only if N is a multiple of n. $\xi^l = \xi^m$ if and only if

$l \equiv m \mod n$. For this reason, the order n of a cyclic group $\{\xi\}$ is often called the period of ξ.

Suppose $\xi \in \Sigma(X)$, and let $x \in X$. If r is the least positive integer such that $x\xi^r = x$, then the elements $x, x\xi, x\xi^2, \ldots, x\xi^{r-1}$ are all distinct. They form a cycle of ξ of order r. If $y = x\xi^k$, the cycle $y, y\xi, \ldots, y\xi^{r-1}$ differs from this only ~~supp~~ superficially; they contain the same r elements of X in the same cyclic order. As cycles, they are to be considered the same. On this understanding, distinct cycles of ξ contain no common term. The n elements of X fall into a certain number of cycles of ξ which are mutually disjoint. If the orders of these cycles are $r_1, r_2, \ldots, r_k$ then $n = \sum r_i$. The numbers $r_1, \ldots, r_k$ are the parts of a partition of n and this partition is called the cycle-type of the permutation ξ. Obviously the order or period of ξ is the least common multiple of the orders of its cycles. Note that this l.c.m. divides $n!$ the order of $\Sigma(X)$.

If a partition contain m_1 parts equal to 1, m_2 parts equal to 2 and so on, it is usually denoted by the symbol $(1^{m_1}2^{m_2}\ldots)$. It is a partition of the number $m_1 + 2m_2 + 3m_3 + \cdots$

(E). Transversals. Let K be a subgroup of the group G. A subset T of G which contains exactly one element from each coset of K in G is called a transversal to K in G. Now ξ and η lie in the same coset of K if and only if $\xi\eta^{-1} \in K$. For T to be transversal to K in G it is therefore necessary and sufficient that

$$G = KT \quad \text{and} \quad K \cap TT^{-1} = 1.$$

Now let

$$H = H_0 \leq H_1 \leq \cdots \leq H_r = G$$

be a chain of subgroups of G each contained in the next. (Here $X < Y$ means that the set X is a proper part of the set Y; $X \leq Y$ that X is contained in Y.) Then we have the product law of indices:

Lemma 2.6 $\quad |G:H| = \prod_{i=1}^{r} |H_i : H_{i-1}|.$

Proof: By induction we may assume $r=2$. Suppose then that K is a subgroup of G containing H. Let T be a transversal to K in G and let S be a transversal to H in K. Then $G = KT$ and $K = HS$ so that $G = HST$. Hence $|G:H| \leq |ST| \leq |S|\cdot|T|$.

Suppose that $\sigma_1\tau_1$ and $\sigma_2\tau_2$ lie in the same coset of H, where $\sigma_i \in S$, $\tau_i \in T$, $i=1,2$. Then $\sigma_1\tau_1\tau_2^{-1}\sigma_2^{-1} \in H$ and so $\tau_1\tau_2^{-1} \in \sigma_1^{-1}H\sigma_2$ which is contained in K since $S \leq K$, $H \leq K$. Hence $\tau_1\tau_2^{-1} \in K$ and so $\tau_1 = \tau_2$ since T is transversal to K. It follows that $\sigma_1\sigma_2^{-1} \in H$ and so $\sigma_1 = \sigma_2$ since S is transversal to H. Thus we obtain $|G:H| = |ST| = |S|\cdot|T|$. Since $|S| = |K:H|$ and $|T| = |G:K|$, the result follows. Note that ST is a transversal to H in G.

The word transversal will sometimes be used in a more general sense. If $\mathfrak{q}$ is an equivalence relation defined on a set X, then X splits up into the union of a number of disjoint non-empty subsets, the $\mathfrak{q}$-classes, each of which consists of all $x \in X$ equivalent under $\mathfrak{q}$ to some fixed element of X. A transversal to the $\mathfrak{q}$-classes is any subset of X which contains just one member from each $\mathfrak{q}$-class.

(F) The product HK of two subgroups H and K is contained in but usually distinct from their join $\{H, K\}$. This is one of the more awkward facts of group theory. Since H and K both contain 1, HK contains both H and K. Hence $HK = \{H, K\}$ if and only if HK is a subgroup. For this there is a simple criterion:

<u>Lemma 2.7</u> HK is a subgroup if and only if $HK = KH$.

Proof: Suppose HK is a subgroup. Then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Conversely, let $HK = KH$. Then $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$ and $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$. So HK is closed with respect to inversion and multiplication: it is a subgroup.

Two subgroups H and K for which $HK = KH$ are called <u>permutable</u>. This does not imply that their elements commute. We also call two subsets X and Y of a group permutable if $XY = YX$.

The most important subgroups of a group are usually those which are permutable with every subset. These are called <u>normal subgroups</u>. In order that a subgroup H of the group G shall be a normal subgroup of G it is necessary and sufficient that

$$H\xi = \xi H$$

for all $\xi \in G$. Now $(H\eta)^{-1} = \eta^{-1}H^{-1} = \eta^{-1}H$. Sets of the form ξH with $\xi \in G$ may therefore be called <u>inverse cosets</u> of H in G. Two distinct inverse cosets of H have no common element. The condition for H to be normal in G is the cosets of H in G shall be the same as the inverse cosets. The normality relation is denoted by

$$H \triangleleft G.$$

~~A fundamental consequence of normality is~~

~~<u>Theorem 2.8</u>. If $H \triangleleft G$, then the cosets of H in G form a group G/H called the <u>quotient group</u> of G by H~~

~~Since $H \triangleleft G$, we have $(H\xi)^{-1} = \xi^{-1}H = H\xi^{-1}$ and $(H\xi)(H\eta) = H(\xi H)\eta = H(H\xi)\eta = (HH)\xi\eta = H\xi\eta$ for all ξ, η in G. The set G/H whose elements are the $|G:H|$ distinct cosets of H in G is therefore closed with respect~~

It should be read "H is a normal subgroup of G" or "H is normal in G".
A fundamental fact is stated in

<u>Theorem 2·8</u>. Let $H \triangleleft G$. Then
$$(H\xi)^{-1} = H\xi^{-1} \quad \text{and} \quad (H\xi)(H\eta) = H\xi\eta$$
for all ξ and η in G. The set G/H whose elements are the cosets of H in G is a group. It is called the <u>quotient group</u> of G by H.

For $(H\xi)^{-1} = \xi^{-1}H = H\xi^{-1}$ and $H\xi H\eta = HH\xi\eta = H\xi\eta$. These equations show that G/H is closed with respect to inversion and multiplication. Laws I and II hold for arbitrary subsets of G. As for law III, we need only note that $(H\xi)(H\xi)^{-1} = H\xi H\xi^{-1} = H\xi\xi^{-1} = H$ for all $\xi \in G$ and $H(H\eta) = H\eta = (H\eta)H$ for all $\eta \in G$. Thus III also holds in G/H. So G/H is a group whose unit element is the subgroup H itself. The unit subgroup of G/H is more appropriately denoted by H/H.

The unit subgroup 1 of G is normal in G and $G/1$ need not be distinguished from G itself. We also have $G \triangleleft G$ and G/G is a unit group with only one element.

If $G \neq 1$ and has no normal subgroups other than 1 and G it is called <u>simple</u>. For example, if $|G| = p$ is a prime, then $G = \{\xi\}$ for every $\xi \neq 1$ in G by 2·4. So G is cyclic and has no subgroups at all other than 1 and G. The discovery and study of simple groups of composite order is one of the most interesting but also one of the most difficult parts of group theory.

By way of contrast, in an Abelian group every subgroup is normal.

Quotient groups H/K, where H is a subgroup of G and $K \triangleleft H$, are called <u>sections</u> of G, following Wielandt. Their study is an essential adjunct to the investigation of the subgroups of G.