E. Spitznagel
Math. Dept.

LECTURE NOTES ON GROUP THEORY

BY

PHILIP HALL

I. Elements of Group Theory.

§1. The laws of group theory. The symmetric groups.

(A). The theory of groups originated in the study of the permutations of a finite set of objects: for example, the roots of an algebraic equation; or the faces, edges and vertices of a regular solid. From this beginning the concept of a group was derived by abstraction, that is to say by the elimination of inessentials, in the following way.

A <u>permutation</u> α of a set X (which need not be finite) is by definition any mapping

$$x \to x\alpha \qquad\qquad (x \in X)$$

of X into itself with these two properties: (i) $x\alpha = y\alpha$ implies $x = y$; and (ii) every y in X has the form $x\alpha$ for some $x \in X$. (i) states that the mapping α is <u>one-to-one</u> and implies that the solution x of the equation $y = x\alpha$ in (ii) is for given y unique. Therefore with every permutation α of X there is associated another permutation α^{-1}, the <u>inverse</u> of α, defined by the rule that $y\alpha^{-1} = x$ whenever $x\alpha = y$.

The number of elements in a set X is denoted by $|X|$. If this number is finite, the two properties (i) and (ii) are equivalent: each implies the other.

The set of all ~~possible~~ permutations of X is denoted by $\Sigma(X)$ and is called the <u>symmetric group</u> on X. If $|X| = n$ is finite, then $|\Sigma(X)| = n!$

Let α and β be in $\Sigma(X)$. Their <u>product</u> $\alpha\beta$ is the mapping of X defined by

$$x(\alpha\beta) = (x\alpha)\beta \qquad\qquad (x \in X).$$

It is the result of applying first α, then β; and it is also a permutation of X. Thus the set $\Sigma(X)$ is closed with respect to two operations: (i) inversion, which is a singulary operation; and

(ii) multiplication, a binary operation.

These two operations satisfy the following laws:

I. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$, the associative law of multiplication;

II. $(\alpha^{-1})^{-1} = \alpha$;

III. $(\alpha\alpha^{-1})\beta = \beta = \beta(\alpha\alpha^{-1})$, the law of cancellation.

Note that the product $\alpha\alpha^{-1}$ is the <u>identity</u> mapping of X which maps each element of X into itself. In these laws, α, β and γ are arbitrary permutations of X.

(B). Now let G be any non-empty set in which "inverses" and "products" have been defined. Provided the laws I, II and III hold for all α, β and γ in G, then G is called a <u>group</u>.

The notations α^{-1}, $\alpha\beta$ are the conventional ones used in the general theory of groups. They are not necessarily the most appropriate in every particular instance. For example, in the set Q of all rational integers, "negatives" and "sums" are defined, and the laws

I$^+$. $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$;

II$^+$. $-(-\alpha) = \alpha$;

III$^+$. $(\alpha+(-\alpha))+\beta = \beta = \beta+(\alpha+(-\alpha))$

hold for all α, β and γ in Q. We express this by calling Q an <u>additive group</u>. The distinction between additive groups like Q and multiplicative groups like $\Sigma(X)$ is not one of principle, but merely of notation.

(C). Some easy consequences of the group-laws I, II and III are to be noted.

<u>Lemma 1·1</u> In any group G, the element $\xi\xi^{-1}$ is independent of the choice of ξ in G. It is called the <u>unit element</u> of G and usually denoted by 1.

The unit element of $\Sigma(X)$ is the identity mapping of X. In an additive group like Q, one speaks of the <u>zero element</u> rather than the unit element, and the notation is 0, not 1. Thus

$\xi + (-\xi) = 0$ for all $\xi \in Q$.

<u>Lemma 1·2</u>. Given elements $\xi_1, \xi_2, \dots, \xi_n$ in a group G, not necessarily distinct, their product in the given order is a uniquely determined element $\xi_1 \xi_2 \cdots \xi_n$ of G and does not depend on the precise way in which the multiplication is carried out.

For example, when $n = 4$, there are five ways of calculating $\xi_1 \xi_2 \xi_3 \xi_4$ viz. $((\xi_1 \xi_2)\xi_3)\xi_4$, $(\xi_1\xi_2)(\xi_3\xi_4)$, $(\xi_1(\xi_2\xi_3))\xi_4$, $\xi_1((\xi_2\xi_3)\xi_4)$ and $\xi_1(\xi_2(\xi_3\xi_4))$. The associative law I ensures that all five give the same answer. Thus, in writing products of three or more elements of a group, brackets may be dispensed with.

However, the ordering of the factors is usually important. In general $\xi\eta \neq \eta\xi$. If it should happen that $\xi\eta = \eta\xi$, then the elements ξ and η are said to <u>commute</u>. Groups in which every pair of elements commute form a very special class called <u>Abelian groups</u> after N.H. Abel 1802-29. Groups, like Q above, which are written in additive notation are nearly always Abelian.

The <u>powers</u> of an element α of a group are defined inductively by the equations

$$\alpha^0 = 1, \quad \alpha^1 = \alpha, \quad \alpha^{n+1} = \alpha^n . \alpha, \quad \alpha^{-n-1} = \alpha^{-n} . \alpha^{-1}$$

for $n = 1, 2, 3, \dots$

<u>Lemma 1·3</u>. For all m, n in Q, we have
$\alpha^m \alpha^n = \alpha^{m+n} = \alpha^n \alpha^m$; $(\alpha^m)^n = \alpha^{mn}$.

If α and β commute, we also have $(\alpha\beta)^m = \alpha^m \beta^m$.

(D). The most significant deduction from the group laws is

<u>Theorem 1·4</u>. Let α be an element of the group G. Then the mapping $r(\alpha)$ of G defined by

$$r(\alpha) \;:\; \xi \to \xi\alpha \qquad (\xi \in G)$$

is a permutation of G, i.e. $r(\alpha) \in \Sigma(G)$. Also, $r(\alpha\beta) = r(\alpha)r(\beta)$ and $r(\alpha^{-1}) = r(\alpha)^{-1}$. Finally, $r(\alpha) = r(\beta)$ only if $\alpha = \beta$.

This theorem brings us back to permutations from which we started. The statement that $r(\alpha) \in \Sigma(G)$ means that, ~~[illegible]~~ for given α and β in G, the equation $\xi\alpha = \beta$ has always a unique solution ξ in G. This unique ξ is $\beta\alpha^{-1}$. For $\xi\alpha = \beta$ implies that $\beta\alpha^{-1} = (\xi\alpha)\alpha^{-1} = \xi(\alpha\alpha^{-1})$ by I, $= \xi$ by III; while $(\beta\alpha^{-1})\alpha = \beta(\alpha^{-1}\alpha)$ by I, $= \beta$ by III, since $\alpha = (\alpha^{-1})^{-1}$ by II.

$r(\alpha)$ is the operation of multiplying the elements of G on the right by α. The operation $l(\alpha)$ of multiplying the elements of G on the left by α is also a permutation of G, because for given α and β in G, the equation $\alpha\eta = \beta$ always has the unique solution $\eta = \alpha^{-1}\beta \in G$. However $l(\alpha\beta) = l(\beta)\,l(\alpha)$ which is different from $l(\alpha)\,l(\beta)$ unless α and β commute. If G is Abelian, $l(\alpha) = r(\alpha)$ for all $\alpha \in G$.

The permutations $r(\alpha)$ and $l(\alpha)$ with $\alpha \in G$ are called the <u>right</u> and <u>left translations</u> of G. Obviously $r(1) = l(1)$ is the identity mapping of G. The word "translation" is a reminder that, if $\alpha \neq 1$, $r(\alpha)$ and $l(\alpha)$ leave no element of G invariant. For example, $\xi\alpha = \xi$ implies $\alpha = \xi^{-1}\xi = 1$.

The law of inversion for products of group elements

<u>Lemma 1·5</u> $(\xi_1\xi_2\cdots\xi_n)^{-1} = \xi_n^{-1}\cdots\xi_2^{-1}\xi_1^{-1}$.

(E) Inverses and products can be defined in a natural way for arbitrary subsets $A, B, X_1, X_2, \dots$ of a group G.

A^{-1} is the set of all inverses α^{-1} of the elements $\alpha \in A$; while AB is the set of all elements ξ of G which are expressible (in at least one way) in the form $\xi = \alpha\beta$ with $\alpha \in A$, $\beta \in B$.

The laws I, II and 1·5 extend at once to these operations on subsets:

$$(AB)C = A(BC) \ ; \ (A^{-1})^{-1} = A \ ; \ (X_1 X_2 \dots X_n)^{-1} = X_n^{-1} \dots X_2^{-1} X_1^{-1}.$$

But law III applies to subsets only in exceptional cases.

The inversion $\alpha \to \alpha^{-1}$ $(\alpha \in G)$ is a permutation of G whose square is the identity. Since it is a permutation, we have $|A^{-1}| = |A|$. By 1·4 we also have

<u>Lemma 1·6</u> For all subsets A, B and all elements ξ, η of a group we have $|A\xi| = |A|$, $|\eta B| = |B|$.

Obviously $|AB| \leq |A| \cdot |B|$.