§4. Automorphisms, Representations, Conjugates

(A) An *automorphism* of a group G is an isomorphic mapping of G onto itself: it is a permutation of G which leaves the group-structure of G invariant.

More generally, let X be any set, and let X^n be the set of all *ordered multiplets*

$$x = (x_1, x_2, \cdots, x_n)$$

with n coordinates $x_i \in X$. The word "multiplet" reminds us that these coordinates need not be distinct. Thus $|X^n| = |X|^n$. Only when $x_1, \cdots, x_n$ are all different shall we call x an *ordered set*. An *n-ary relation* connecting the elements of X determines the set R of all $x \in X^n$ for which the given relation holds. Mostly, we can identify the relation with this subset R of X^n. A *structured set* X can be specified by a certain number of relations $R, R_1, R_2, \cdots$, not necessarily all with the same n. For example we can think of the structure of a group G as specified by a single ternary relation, consisting of all triplets $(\xi, \eta, \zeta) \in G^3$ for which $\xi\eta = \zeta$.

Any $\alpha \in \Sigma(X)$ induces a mapping $x \to x\alpha$ of X^n into itself, defined by the equations $(x\alpha)_i = x_i\alpha$, $i = 1, 2, \cdots, n$. For any relation R, let $R\alpha$ be the set of all $x\alpha$ with $x \in R$. The set of all $\alpha \in \Sigma(X)$ such that $R\alpha = R$, $R_1\alpha = R_1$, $\cdots$ is clearly a subgroup of $\Sigma(X)$: it is called the *group of automorphisms* of X with respect to the structure defined by the relations $R, R_1, \cdots$. An automorphism is a structure preserving permutation.

For example, let X consist of n real numbers and let R consist of all $x \in X^n$ such that

$$\prod_{i>j} (x_i - x_j) > 0.$$

As group of automorphisms of X with respect to R we obtain the *alternating group* $\Sigma^+(X)$ of order $\frac{1}{2}n!$ consisting of all even permutations of X. A permutation of cycle-type $(1^{m_1}2^{m_2}\dots)$ is even or odd according as the number $m_2+m_4+\cdots$ of cycles of even order is even or odd.

The group of automorphisms of a group G will be denoted by Aut G.

(B). Let α, β, ξ, η be elements of a group G. We write

$$\alpha^{-1}\xi\alpha = \xi^{\alpha}.$$

The element ξ^α is called the *transform* of ξ by α. Clearly $(\xi\eta)^\alpha = \xi^\alpha\eta^\alpha$. Hence the mapping $t(\alpha) = l(\alpha^{-1})r(\alpha) \in \Sigma(G)$ defined by

$$t(\alpha): \quad \xi \to \xi^\alpha \qquad (\xi \in G)$$

is an automorphism of G. Those automorphisms of G which have the form $t(\alpha)$ for some $\alpha \in G$ are called *inner automorphisms* of G. We also have $\xi^{\alpha\beta} = (\xi^\alpha)^\beta$ and so $t(\alpha\beta) = t(\alpha)t(\beta)$. Hence the mapping

$$\alpha \to t(\alpha) \qquad (\alpha \in G)$$

is homomorphic: it is an epimorphism of G onto the group $t(G)$ of all inner automorphisms of G. Now $\xi = \xi^\alpha$ if and only if $\alpha\xi = \xi\alpha$. Hence the kernel of this epimorphism consists of all $\alpha \in G$ which commute with every element of G. This kernel is called the *centre* of G and denoted by $\mathfrak{z}G$. By 3.3, $\mathfrak{z}G \lhd G$ and $t(G) \cong G/\mathfrak{z}G$. G is Abelian if and only if $G = \mathfrak{z}G$. The only inner automorphism of an Abelian group is the identity.

Now let τ be any automorphism of G, and let $\xi \in G$. It is usual to denote the image of ξ under τ by ξ^τ. Calculating the transform $\tau^{-1}t(\alpha)\tau$ of the inner automorphism $t(\alpha)$ by τ, we have the scheme

$$\xi^\tau \xrightarrow[\tau^{-1}]{} \xi \xrightarrow[t(\alpha)]{} \alpha^{-1}\xi\alpha \xrightarrow[\tau]{} (\alpha^\tau)^{-1}\xi^\tau\alpha^\tau$$

since $(\alpha^{-1})^\tau = (\alpha^\tau)^{-1}$. But $\tau \in \Sigma(G)$ and so ξ^τ is an arbitrary element of G if ξ is chosen suitably. Hence we obtain the formula

$$t(\alpha)^\tau = t(\alpha^\tau).$$

Summing up, we have

Theorem 4·1 For any group G, with centre $\mathfrak{z}G$, we have
$$G/\mathfrak{z}G \cong t(G) \lhd \operatorname{Aut} G.$$

The quotient group $\operatorname{Aut} G / t(G)$ is sometimes called the group of <u>outer automorphisms</u> of G. But it is more natural to call any automorphism outer if it is not inner.

emote to
we
en
ttled

(C). If X is any subset of the group G and $\alpha \in G$, then we write $\alpha^{-1} X \alpha = X^{\alpha}$. Thus X is invariant under $t(\alpha)$ if and only if $X\alpha = \alpha X$. Hence a normal subgroup of G is precisely one which is invariant under every inner automorphism of G:
$$K \lhd G \Leftrightarrow K^{\alpha} = K \text{ for all } \alpha \in G.$$
If a subgroup of G is invariant under every automorphism of G both outer and inner, it is called a <u>characteristic subgroup</u> of G. By 2·5, in a cyclic group every subgroup is characteristic. We express that K is a characteristic subgroup of G by writing
$$K \text{ char } G.$$
If K ~~char~~ $\lhd G$ and $\alpha \in G$, then the restriction $t_K(\alpha)$ of $t(\alpha)$ to K is an automorphism of K, but in general $t_K(\alpha)$ is not an inner automorphism of K. However we have

Lemma 4·2 If H char K and $K \lhd G$, then $H \lhd G$. If H char K and K char G, then H char G.

But $H \lhd K$ and $K \lhd G$ do not in general imply that $H \lhd G$.

(D). A homomorphism f of a group G into a permutation group $\Sigma(X)$ is called a <u>representation</u> of G by permutations of X. The number $|X|$ is called the <u>degree</u> of the representation f. We have already noted two such representations: the regular representation r of G, and the representation t of G by inner automorphisms. If the kernel of a representation f is 1, it is called <u>faithful</u>, for then

$f(G) \cong G$. r is always faithful by 1·4; but t is faithful only if $G = 1$, by 4·1.

If we are studying one particular representation f of G, it is often convenient to eliminate the symbol f by writing $x\alpha$ instead of $x\,f(\alpha)$, where $\alpha \in G$, $x \in X$ and $f \in \mathrm{Hom}(G, \Sigma(X))$. We are then left with the set X, the group G and a multiplication $XG \to X$ such that

$$\mathrm{I}^* \qquad x(\alpha\beta) = (x\alpha)\beta\ ;$$

$$\mathrm{II}^* \qquad x1 = x\,,$$

for all $x \in X$ and all α, β in G. Here 1 is the unit element of G. The laws I^* and II^* ensure that the mapping

$$f(\alpha) : \quad x \to x\alpha \qquad\qquad (x \in X)$$

is a permutation of X and that $f(\alpha\beta) = f(\alpha)f(\beta)$ for all α, β in G. In this way the representation f is recovered.

Two elements x, y in X are <u>related</u> under G if $x\alpha = y$ for some $\alpha \in G$. If $x\alpha = y$ and $y\beta = z$ then $x(\alpha\beta) = z$; also $y\alpha^{-1} = x$. So this is an equivalence relation. If every pair of elements of X are related under G, f is called a <u>transitive</u> representation. In this case, we say that G permutes X <u>transitively</u>. In general, however, X will split up into a number of <u>transitivity classes</u> X_i:

$$X = X_1 \cup X_2 \cup \cdots \cup X_r$$

each of which is permuted transitively by G. Each X_i consists of all $x \in X$ which are related under G to any given element of X_i. And, of course, $X_i \cap X_j$ is empty if $i \neq j$. If $f_i(\alpha)$ is the permutation of X_i induced by $f(\alpha)$, then f_i is a transitive representation of G. $f_1, f_2, \ldots, f_r$ are called the <u>transitive components</u> of f. Since they determine f uniquely, we express this decomposition by writing

$$f = f_1 \oplus f_2 \oplus \cdots \oplus f_r\,.$$

If K_i is the kernel of f_i, then the kernel of f is $K = \bigcap_{i=1}^{r} K_i$.

(E). Two elements ξ and η of G are called <u>conjugate</u> in G if and only if $\xi^{\alpha} = \eta$ for some $\alpha \in G$. Thus conjugate elements are simply elements related under G in the representation t. Therefore G splits into a certain number of mutually disjoint <u>classes of conjugates</u> G_i:

$$G = G_1 \cup G_2 \cup \dots \cup G_h .$$

The unit element of G is conjugate only to itself, so we may take $G_1 = 1$. The number h is an important numerical invariant of G. We call it the <u>class number</u> of G. If G is Abelian, each G_i consists of a single element of G and so in this case $h = |G|$.

<u>Lemma 4·3</u> In $\Sigma(X)$, two elements ξ and η are conjugate if and only if they have the same cycle-type. If $|X| = n$, the class number of $\Sigma(X)$ is equal to the number of partitions of n.

Proof: Suppose that $\eta = \xi^{\tau}$ with $\tau \in \Sigma(X)$ and let $(x_1, x_2, \dots, x_r)$ be any cycle of ξ. Writing $x_{r+1} = x_1$, we have

$$x_i\tau \xrightarrow[\tau^{-1}]{} x_i \xrightarrow[\xi]{} x_{i+1} \rightarrow x_{i+1}\tau$$

so that $(x_1\tau, x_2\tau, \dots, x_r\tau)$ is a cycle of η of the same order r. Thus ξ and η have the same cycle-type. Conversely, if ξ and η have the same cycle-type, we can find a permutation τ of X which maps each cycle of ξ into a corresponding cycle of η. If the cycle-type of ξ and η is $(1^{m_1} 2^{m_2} \dots)$, this τ can be chosen in precisely

$$\prod_{k=1}^{\infty} (k^{m_k} \cdot m_k!)$$

distinct ways. Taking $\xi = \eta$ gives the first part of

<u>Lemma 4·4</u> The number of elements τ of $\Sigma(X)$ which commute with a given element ξ of type $(1^{m_1} 2^{m_2} \dots)$ is $\prod_k k^{m_k} \cdot m_k!$. There is always an odd τ which commutes with ξ excepting only when the different cycles of ξ have different odd orders i.e. when $m_{2i} = 0$ and $m_{2i-1} \leq 1$ for all $i = 1, 2, \dots$

For if ξ has two cycles $(x_1\, x_2 \dots x_r)$ and $(y_1\, y_2 \dots y_r)$ of odd order r, then $\tau = (x_1 y_1)(x_2 y_2) \cdots (x_r y_r)$ commutes with ξ and is odd. If ξ has an ~~...~~ cycle of even order, we can take τ to be this cycle. Again τ is odd and commutes with ξ. If $\xi = \tau_1 \tau_2 \cdots \tau$ where the τ_i are the cycles of ξ and if these cycles are all of differe[nt] orders, then the only elements of $\Sigma(X)$ which commute with ξ are those of the form $\tau_1^{m_1} \tau_2^{m_2} \cdots \tau_s^{m_s}$. If the τ_i are all of odd order, these products are all even permutations.

(F) Let $f \in \mathrm{Hom}(G, \Sigma(X))$ and let $x \in X$. The set of all $\alpha \in G$ such that $x\alpha = x$ is a subgroup of G called the <u>stabilizer</u> of x in G. We denote it by $S_G(x)$. Let $\xi \in G$ and suppose that $x\xi = y$. Then every element of the coset $S_G(x)\xi$ maps x into y. Conversely, if $x\eta = y$ then $\xi\eta^{-1} \in S_G(x)$ and $\eta \in S_G(x)\xi$. The cosets of $S_G(x)$ in G correspond one-to-one with the elements $y \in X$ which are related to x under G. In particular, we have

<u>Lemma 4·5</u> If G permutes X transitively, then for all $x \in X$ $|G : S_G(x)| = |X|$. The degree of a transitive representation of G divides the order of G.

Let $\xi \in G$. Then the set of all $\alpha \in G$ which commute with ξ is a subgroup $C_G(\xi)$ called the <u>centralizer</u> of ξ in G. Applying 4·5 to the t-representation of G, we have the

<u>Corollary 1</u>. If $\xi \in G$, then $|G : C_G(\xi)|$ is equal to the number of conjugates of ξ in G. This number always divides $|G|$.

Each $t(\alpha)$, $\alpha \in G$, is an automorphism of G and maps subgroups into subgroups. Two subgroups H and K of G are called <u>conjugate</u> in G if and only if $H^\alpha = K$ for some $\alpha \in G$. If $t^*(\alpha)$ is the permutation induced by $t(\alpha)$ on the subgroups of G, then t^* is a representation of G; the transitivity classes of t^* are the <u>classes of conjugate subgroups</u> of G. Each of these classes consists of all the subgroups of G which are conjugate in G to any particular subgroup

H of the class in question. The set of all $\alpha \in G$ such that $H^\alpha = H$ is a subgroup $N_G(H)$ of G which contains H. It is called the normalizer of H in G. Since $H^\alpha = H$ is equivalent to $\alpha H = H\alpha$, the normalizer of H is the largest subgroup N of G such that $H \triangleleft N$. Applying 4·5 to the representation t^* of G, we obtain

Corollary 2. If H is any subgroup of G, then $|G : N_G(H)|$ is equal to the number of subgroups conjugate to H in G.

Note that a subgroup is always conjugate to itself. $H \triangleleft G$ if and only if $N_G(H) = G$. A normal subgroup is conjugate only to itself.

(G) Let G permute X transitively. Then, for given x and y in X, we have $x\alpha = y$. Then $x\xi = x$ if and only if $y\alpha^{-1}\xi\alpha = y$. Hence $S_G(y) = \alpha^{-1} S_G(x)\alpha$. In a transitive representation, the stabilizers form a class of conjugate subgroups. Suppose we have a second representation in which G permutes X' transitively. These two representations are called equivalent if and only if there is a one-to-one mapping θ of X onto X' such that $x\theta\alpha = x\alpha\theta$ for all $\alpha \in G$. If this is the case, then $|X| = |X'|$ and $S_G(x\theta) = S_G(x)$ for all $x \in X$. So equivalent representations have the same stabilizers, and of course the same degree.

Conversely, suppose that for some $x \in X$ and $x' \in X'$ we have $S_G(x) = S_G(x') = H$. Let T be a transversal to H in G. Then each element of X is expressible uniquely in the form $x\tau$ with $\tau \in T$. Similarly each element of X' is expressible uniquely in the form $x'\tau$ with $\tau \in T$. Hence we have a one-to-one mapping θ of X onto X' defined by $(x\tau)\theta = x'\tau$. Given $\alpha \in G$, $\tau \in T$ there is a unique $\tau_1 \in T$ such that $H\tau\alpha = H\tau_1$. We then have

$$(x\tau)\theta\alpha = x'\tau\alpha = x'\tau_1 = (x\tau_1)\theta = (x\tau\alpha)\theta$$

and so the two representations are equivalent.

Given any subgroup H of G, the regular representation τ of G induces a representation τ_H of G by permutations of the cosets of H. For $\alpha \in G$, $\tau_H(\alpha)$ is by definition the mapping

$$\tau_H(\alpha): \quad H\xi \to H\xi\alpha \qquad (\xi \in G).$$

For any ξ, η in G, $\tau_H(\xi^{-1}\eta)$ maps $H\xi$ into $H\eta$. Thus τ_H is a transitive representation of G. The stabilizer of the coset H in this representation is precisely H itself. Summing up, we have

Theorem 4·6 In any transitive representation f of a group G, the stabilizers form a class of conjugate subgroups of G. Two transitive representations are equivalent if and only if they have the same stabilizers. If H is one of the stabilizers for f, then f is equivalent to τ_H.

In any representation of G, the kernel is the intersection of the stabilizers. In the representation τ_H, the stabilizers are the conjugates of H in G. Hence the kernel of τ_H is the group

$$K = \bigcap_{\xi \in G} H^{\xi} = K_G(H).$$

If $L \triangleleft G$ and $L \leq H$, then $L = L^{\xi} \leq H^{\xi}$ for all $\xi \in G$. Hence $L \leq K$. Thus $K_G(H)$ <u>is the largest normal subgroup of G contained in H.</u>

Note that $\tau_1 = \tau$ is precisely the regular representation itself.

(H) If H is any subgroup of G and $N = N_G(H)$, we have a representation t_H of N by automorphisms of H. Here $t_H(\alpha)$ is for any $\alpha \in N$ the restriction of $t(\alpha)$ to H. The kernel of this representation t_H is called the <u>centralizer</u> of H in G and denoted by $C_G(H)$. It consists of all elements of G which commute with every element of H. Hence $t_H(N) \cong N_G(H)/C_G(H)$. This group $t_H(N)$ will be called the <u>automizer</u> of H in G and denoted for preference by $A_G(H)$. It consists of all automorphisms of H which can be induced by transforming H by some element of G. Hence

…fusion
…ne

$$A_G(H) \cong N_G(H)/C_G(H).$$

Note that $C_G(G) = z(G)$ is the centre of G and $A_G(G) = t(G)$ is the group of inner automorphisms of G.

If we are given a representation f of a group Γ by automorphisms of another group G, we shall say that G <u>admits</u> Γ as <u>group of operators</u>. If G is a multiplicative group, it is usually convenient to use the notation

$$\xi \to \xi^\alpha \qquad (\xi \in G)$$

for the automorphism $f(\alpha)$ of G. Here $\alpha \in \Gamma$. If G is an additive group, as often happens, we write $\xi\alpha$ instead of ξ^α. The laws which apply are

$$(\xi\eta)^\alpha = \xi^\alpha\eta^\alpha \;;\quad \xi^1 = \xi \;;\quad \xi^{\alpha\beta} = (\xi^\alpha)^\beta$$

or $$(\xi+\eta)\alpha = \xi\alpha + \eta\alpha \;;\quad \xi 1 = \xi \;;\quad \xi(\alpha\beta) = (\xi\alpha)\beta$$

according to the case. Here $\xi, \eta \in G$ and $\alpha, \beta \in \Gamma$, while 1 is the unit element of Γ.

A subgroup H of G is Γ-<u>admissible</u> if $H^\alpha = H$ for all $\alpha \in \Gamma$. Joins and intersections of admissible subgroups are admissible. A section H/K of G is admissible if both H and K are admissible. If this is the case, then the mapping

$$K\xi \to K\xi^\alpha \qquad (\xi \in H)$$

is ~~[illegible]~~ an automorphism of H/K for all $\alpha \in \Gamma$. If we denote it by $f_{H/K}(\alpha)$, then $f_{H/K}$ is a representation of Γ, and H/K admits Γ as group of operators.

If G_1 is any other group admitting Γ as group of operators, then we say that G and G_1 are <u>operator-isomorphic</u>, or more precisely Γ-isomorphic if there is an isomorphism $\xi \to \xi_1$ of G onto G_1 such that $(\xi^{\alpha})_1 = (\xi_1)^{\alpha}$ for all $\xi \in G$ and all $\alpha \in \Gamma$. This notion of <u>Γ-isomorphism</u> is analogous to that of equivalent representations. It is clear that if two admissible sections of G are incident, they are necessarily Γ-isomorphic. Hence we may state as a corollary of 3·7 and 3·8

<u>Theorem 4·7</u> Let the group G admit ~~the~~ Γ as group of operators. Then any two Γ-admissible series of G have refinements whose factors are Γ-isomorphic in pairs. In ~~any~~ any two Γ-composition series of G, the factors are Γ-isomorphic in pairs.

Here, a <u>Γ-composition series</u> is a proper series whose terms are all Γ-admissible but which cannot be refined any further without losing this property. In other words, each factor group H/K of a Γ-composition series is <u>Γ-simple</u>, in the sense that no admissible subgroup L exists such that ~~[illegible]~~ $K < L < H$ and $L \triangleleft H$. This implies that H/K has no characteristic subgroup L/K other than the two obvious ones with $L = K$ and $L = H$. A group G which has exactly two characteristic subgroups is sometimes called <u>characteristically-simple</u>; but this does not mean that G is simple, for G may have normal subgroups M with $1 < M < G$ which are not characteristic.

The most important special case of 4·7, apart from the one already covered in 3·8, is the case $\Gamma = G$. A G-composition series of G is called a <u>chief series</u> of G and its factors are called <u>chief factors</u> of G. H/K is a chief factor of G if and only if $K \triangleleft G$ and H/K is a <u>minimal normal subgroup</u> of G/K. (M is a minimal normal subgroup of G if $M \neq 1$, $M \triangleleft G$ and M contains no normal subgroup L of G such that $1 < L < M$.)