COMPOSITIO MATHEMATICA

A. M. TURING The extensions of a group

Compositio Mathematica, tome 5 (1938), p. 357-367 <http://www.numdam.org/item?id=CM_1938_5_357_0>

© Foundation Compositio Mathematica, 1938, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http: //http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

$\mathcal N$ umdam

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques http://www.numdam.org/

The extensions of a group

by

A. M. Turing

Cambridge, England

A group \mathfrak{G} is said to be an extension of \mathfrak{R} by \mathfrak{G}' if \mathfrak{R} is a self conjugate subgroup of \mathfrak{G} and $\mathfrak{G}/\mathfrak{R} \mathfrak{D} \mathfrak{G}'$. The problem of finding the extensions of \mathfrak{R} by \mathfrak{G}' has been investigated by Schreier ¹) and by Baer ²).

Let \mathfrak{A} be the automorphism group of \mathfrak{N} and \mathfrak{F} the subgroup of inner automorphisms. Then to each coset γ of \mathfrak{N} in \mathfrak{G} there corresponds a coset $X(\gamma)$ of \mathfrak{F} in \mathfrak{A} , such that if $c \in \gamma$ then the automorphism induced by c in \mathfrak{N} belongs to $X(\gamma)$. $X(\gamma)$ is a homomorphism of \mathfrak{G}' in $\mathfrak{A}/\mathfrak{F}$. Baer's investigations are concerned with finding all possible groups \mathfrak{G} when \mathfrak{N} , \mathfrak{G}' and the homomorphism $X(\gamma)$ are given. As a first step towards the solution of this problem the possible structures of $\mathfrak{G}/\mathfrak{F}(\mathfrak{N})$ are found, where $\mathfrak{F}(\mathfrak{N})$ denotes the centre of \mathfrak{N} ; it then only remains to solve the original problem in the case where \mathfrak{N} is Abelian. This case is treated entirely differently. In the present paper it is proposed to shew how Baer's method for the case when \mathfrak{N} is Abelian can be used for any group \mathfrak{N} .

In a practical determination of all extensions with given characteristics it is necessary to find the structure of the relation group of the factor group \mathfrak{G}' . This is so even when \mathfrak{R} is Abelian. The problem is considered in the second half of the paper.

As an illustration the theory is applied to the case of extensions of an arbitrary group by a cyclic group.

§ 1. Extensions with given automorphisms.

The problem of finding extensions of a group by a given group inducing given classes of automorphisms is best treated

¹) O. SCHREIER, Über die Erweiterung von Gruppen [Monats. f. Math. u. Phys. 34 (1926), 165-180].

²) R. BAER, Erweiterung von Gruppen und ihren Isomorphismen [Math. Zeitschr. 38 (1934), 375-416].

by reducing it to another problem which is both described and solved in the following

THEOREM 1.

 \mathfrak{N} , \mathfrak{F} are given groups ³) and \mathfrak{R} is a self conjugate subgroup of \mathfrak{F} ; χ_a is a homomorphism of \mathfrak{F} into the group of automorphisms of \mathfrak{N} (i.e. $\chi_a(\mathfrak{b})$ as a function of \mathfrak{b} is an automorphism of \mathfrak{N} and satisfies

$$\chi_{ab}(\mathfrak{b}) = \chi_b(\chi_a(\mathfrak{b}))$$
 (1, b, a, \mathfrak{b})

for all b, a of \mathcal{F} and \mathfrak{b} of \mathfrak{N}) and $\mathfrak{a}(r)$ is a homomorphism of \mathfrak{R} into \mathfrak{N} . Then there is a group ³) \mathfrak{G} in which \mathfrak{N} is a self conjugate subgroup, and a homomorphism $\mathfrak{w}(r)$ of \mathcal{F} into \mathfrak{G} which satisfies:

$$\begin{array}{c} a) \qquad \qquad \chi_a(\mathfrak{b}) = (\mathfrak{w}(a))^{-1}\mathfrak{b}\mathfrak{w}(a) \quad (\mathbf{I}, \ a, \ \mathfrak{b}) \\ \\ \mathfrak{w}(r) = \mathfrak{a}(r) \qquad \qquad (\mathbf{II}, \ r) \end{array} \right\}$$

(for all a in \mathfrak{F} , r in \mathfrak{R} and b in \mathfrak{R}),

- b) every coset of \mathfrak{N} in \mathfrak{G} contains an element of $\mathfrak{w}(\mathfrak{F})$,
- c) $\mathfrak{w}(\mathfrak{R}) = \mathfrak{N} \cap \mathfrak{w}(\mathfrak{F})$

if and only if

$$\chi_{a}(\mathfrak{a}(r)) = \mathfrak{a}(a^{-1}ra) \quad (\mathbf{I}, a, r)$$

$$\chi_{r}(\mathfrak{b}) = (\mathfrak{a}(r))^{-1}\mathfrak{b}\mathfrak{a}(r) \quad (\mathbf{II}, r, \mathfrak{b})$$
(3)

(for all a in \mathfrak{F} , r in \mathfrak{R} and b in \mathfrak{N}).

The relevance of this theorem to the original extension problem can be seen from the

COROLLARY:

F is a free ⁴) group with a self conjugate subgroup $\Re(\mathfrak{F}/\Re \subseteq \mathfrak{G}', say)$ and $X(\gamma)$ is a homomorphism of $\mathfrak{F}/\mathfrak{R}$ into the classes of automorphisms of a given group \mathfrak{R} . Let χ_a be any homomorphism of \mathfrak{F} into the automorphisms of \mathfrak{R} for which χ_a belongs to the class $X(\alpha)$ whenever a belongs to the coset α of \mathfrak{R} in \mathfrak{F} . Then an extension

³) Elements of \mathfrak{F} are denoted by italic letters, elements of \mathfrak{N} and (§ by German letters, and elements of $\mathfrak{F}/\mathfrak{R}$ by Greek letters. e, e, e are the identities of these groups and E is the identity of Φ in § 2.

⁴) It is essential that \mathfrak{F} should be free if the conditions are to be necessary. A trivial example shows that at least \mathfrak{F} cannot be arbitrary if we require $\mathfrak{a}(r)$ to be related to a function $\mathfrak{w}(a)$ as in the theorem. Let \mathfrak{G} be the cyclic group $\{\mathfrak{b}\}$ of order 4, \mathfrak{F} the cyclic group $\{g\}$ of order 2, and let \mathfrak{N} be $\{\mathfrak{b}^2\}$ and $\chi_g(\mathfrak{b}^2) = \mathfrak{b}^2$. Then we should have to have $\mathfrak{a}(e) = \mathfrak{e}$. But $\mathfrak{a}(e) = \mathfrak{a}(g^2) = \mathfrak{b}^2$.

 \mathfrak{G} of \mathfrak{N} by \mathfrak{G}' in which the coset α of \mathfrak{N} induces the class $X(\alpha)$ can be found if and only if there is a homomorphism $\alpha(r)$ of \mathfrak{R} in \mathfrak{N} satisfying (3).

Proof of the theorem. The necessity of the conditions is trivial. (3, I, a, r) follows from (2, I, a, a(r)), (2, II, r), (2, II, $a^{-1}ra$) and the fact that w is a homomorphism: (3, II, r, b) follows immediately from (2, I, r, b) and (2, II, r).

For the sufficiency we have to construct the group \mathfrak{G} . The elements of this group are to be all classes of equivalent pairs (a, \mathfrak{a}) $(a \text{ in } \mathfrak{F}, \mathfrak{a} \text{ in } \mathfrak{N})$, (a', \mathfrak{a}') being equivalent to (a, \mathfrak{a}) if and only if $a^{-1}a'$ belongs to \mathfrak{R} and $\mathfrak{a}(a^{-1}a') = \mathfrak{a} \mathfrak{a}'^{-1}$. This is an equivalence relation, for

1) If $a^{-1}a' \in \Re$ and $\mathfrak{a}(a^{-1}a') = \mathfrak{a} \mathfrak{a'}^{-1}$

then

 $a'^{-1}a \in \Re$ and $\mathfrak{a}(a'^{-1}a) = \mathfrak{a}'\mathfrak{a}^{-1}$,

i.e. the relation is symmetric.

2) $a^{-1}a = e \in \Re$, $\mathfrak{a}(a^{-1}a) = \mathfrak{e} = \mathfrak{a} \mathfrak{a}^{-1}$,

i.e. the relation is reflexive.

3) If $a^{-1}a' \in \Re$, $a'^{-1}a'' \in \Re$,

$$\mathfrak{a}(a^{-1}a') = \mathfrak{a} \mathfrak{a'}^{-1}$$
 and $\mathfrak{a}(a'^{-1}a'') = \mathfrak{a'} \mathfrak{a''}^{-1}$

then

$$a^{-1}a^{\prime\prime} = (a^{-1}a^{\prime})(a^{\prime^{-1}}a^{\prime\prime}) \epsilon \Re$$

$$\mathfrak{a}(a^{-1}a^{\prime\prime}) = \mathfrak{a}(a^{-1}a^{\prime}) \mathfrak{a}(a^{\prime^{-1}}a^{\prime\prime}) = \mathfrak{a} \mathfrak{a}^{\prime^{-1}}\mathfrak{a}^{\prime} \mathfrak{a}^{\prime\prime^{-1}} = \mathfrak{a} \mathfrak{a}^{\prime\prime^{-1}},$$

i.e. the relation is transitive.

The product of two pairs is defined by

$$(a, \mathfrak{a})(b, \mathfrak{b}) = (ab, \chi_b(\mathfrak{a})\mathfrak{b}).$$

This will be a valid definition of a product of classes of pairs if we can shew that if (a', a') is equivalent to (a, a) and (b', b')is equivalent to (b, b) then (a', a')(b', b') is equivalent to (a', a)(b, b) i.e. that if

$$\left. \begin{array}{l} a^{-1}a' \,\epsilon \, \Re, \ b^{-1}b' \,\epsilon \, \Re \\ \mathfrak{a}(a^{-1}a') = \mathfrak{a} \, \mathfrak{a'}^{-1} \text{ and } \mathfrak{a}(b^{-1}b') = \mathfrak{b}\mathfrak{b'}^{-1} \end{array} \right\}$$
(4)

then

$$(ab)^{-1}(a'b') \in \mathfrak{R} ext{ and } \mathfrak{a}ig((ab)^{-1}(a'b')ig) = ig(\chi_{b'}(\mathfrak{a})\mathfrak{b}ig)ig(\chi_b(\mathfrak{a}'),\mathfrak{b}'ig)^{-1}.$$

Now

$$(ab)^{-1}(a'b') = b^{-1}(a^{-1}a')b \cdot b^{-1}b' \in \mathfrak{R}$$

and
 $\mathfrak{a}((ab)^{-1}(a'b')) = \chi_b(\mathfrak{a} \mathfrak{a}'^{-1})\mathfrak{b}\mathfrak{b}'^{-1}$
 $= \chi_b(\mathfrak{a})\mathfrak{b} \cdot \mathfrak{b}'^{-1} \cdot (\mathfrak{b}\mathfrak{b}'^{-1})^{-1}\chi_b(\mathfrak{a}'^{-1})\mathfrak{b}\mathfrak{b}'^{-1}$
 $= (\chi_b(\mathfrak{a})\mathfrak{b}) \cdot (\chi_{b'}(\mathfrak{a}')\mathfrak{b}')^{-1}$

by (4), (3, II, $b^{-1}b'$, $\chi_b(\mathfrak{a}')$) and (1). The product is also associative, for

$$((a, a)(b, b))(c, c) = (ab, \chi_b(a)b)(c, c)$$
$$= (abc, \chi_c(\chi_b(a)b)c)$$
$$(a, a)((b, b)(c, c)) = (a, a)(bc, \chi_c(b)c)$$
$$= (abc, \chi_{bc}(a)\chi_c(b)c)$$

and these two expressions are equal on account of (1) and the fact that χ_e is an automorphism.

(e, e) is an identity and $(a^{-1}, \chi_{a^{-1}}(a^{-1}))$ is an inverse to (a, a). Consequently with this product our classes of pairs form a group.

 $\mathfrak{w}(a)$ is defined by

$$\mathfrak{w}(a) = (a, e)$$

and is clearly a homomorphism. To show that (2, II) is satisfied it is only necessary to verify that (r, e) is equivalent to (e, a(r)). As regards (2, I) we have

$$(\mathfrak{w}(a))^{-1}\mathfrak{b}\mathfrak{w}(a) = (a^{-1}, \mathfrak{e})\mathfrak{b}(a, \mathfrak{e})$$

= $(a^{-1}, \mathfrak{e})(a, \chi_a(\mathfrak{b}))$
= $(e, \chi_a(\mathfrak{b})) = \chi_a(\mathfrak{b}).$

Since

$$(g, b) = (g, e)(e, b)$$

= $\mathfrak{w}(g)\mathfrak{b}$

condition b is satisfied.

The condition that an element b of \mathfrak{N} should also lie in $\mathfrak{w}(\mathfrak{F})$ is that (e, b) be equivalent to some pair (a, e). This means that a is in \mathfrak{R} and $\mathfrak{a}(a) = \mathfrak{b}$. Hence $\mathfrak{N} \cap \mathfrak{w}(\mathfrak{F}) \subseteq \mathfrak{w}(\mathfrak{R})$. This is satisfied since $\mathfrak{w}(r) = \mathfrak{a}(r)$ so that $\mathfrak{w}(\mathfrak{R}) \subseteq \mathfrak{N}$.

Proof of the corollary. Suppose \mathfrak{G} is a group with the required properties, e_1, e_2, \ldots, e_n a set of free generators of \mathfrak{F} and ω the function determining the homomorphism of \mathfrak{F} on \mathfrak{G}' . Let e_1 ,

 e_2, \ldots, e_n be elements of \mathfrak{G} with the property that e_i is in the coset $\omega(e_i)$ of \mathfrak{R} and that

$$\chi_{e_i}(\mathfrak{b}) = e_i^{-1}\mathfrak{b}e_i$$
 for all \mathfrak{b} in \mathfrak{N} .

Then if w be a homomorphism of \mathfrak{F} into \mathfrak{G} satisfying $\mathfrak{w}(e_i) = e_i$ for all *i*, we shall have

$$\chi_a(\mathfrak{b}) = (\mathfrak{w}(a))^{-1}\mathfrak{b}\mathfrak{w}(a)$$
 for all \mathfrak{b} in \mathfrak{N} .

If we put w(r) = a(r) for elements r of \Re then by the first half of theorem 1 (whose proof makes no use of b, c) the conditions (3) must hold.

If on the other hand we have a function a(r) satisfying (3) we can form the group \mathfrak{G} of theorem 1 which is easily seen to have the required properties.

For specific applications the corollary to theorem 1 is more useful in the form of

THEOREM 2.

 \Re is a given group. F is a free group with the generators $e_1, e_2, ..., e_n$. \Re is the least self conjugate subgroup of F containing $r_1, r_2, ..., r_l$. ω maps F homomorphically on S', the elements mapped on the identity being those of \Re . χ_a is a homomorphism of F into the automorphisms of \Re , and $X(\omega(a))$ is the class of automorphisms containing χ_a . \mathfrak{r}_1^* , \mathfrak{r}_2^* , ..., \mathfrak{r}_l^* are elements of \Re such that

$$\chi_{r_i}(\mathfrak{b}) = \mathfrak{r}_i^{*-1}\mathfrak{b}\mathfrak{r}_i^* \text{ for all } \mathfrak{b} \text{ of } \mathfrak{N}. \tag{5}$$

Then there is an extension \mathfrak{G} of \mathfrak{N} by \mathfrak{G}' realising the classes $X(\alpha)$ of automorphisms if and only if 5) there are elements $\mathfrak{z}_1, \mathfrak{z}_2, \ldots, \mathfrak{z}_k$ of the centre of \mathfrak{N} for which the equation

$$\prod_{i=1}^{N} \chi_{a_i} \left(\delta_{t_i}^{\tau_i} \right) = \prod_{i=1}^{N} \chi_{a_i} \left(\mathfrak{r}_{t_i}^{*\tau_i} \right) \tag{6}$$

holds whenever the corresponding equation

$$\prod_{i=1}^{N} a_{i}^{-1} r_{l_{i}}^{\tau_{i}} a_{i} = e \tag{7}$$

holds in F.

If the extension $(\emptyset$ exists, then by the corollary to theorem 1 there is a homomorphism $\mathfrak{a}(r)$ of \mathfrak{R} into \mathfrak{R} , satisfying (3). This homomorphism is completely determined by its 'values for

⁵) That the elements z_i do not always exist can be seen from an example given by Baer (loc. cit., 415). Another example will be given in § 3.

 r_1, r_2, \ldots, r_l . Let us put $\mathfrak{a}(r_i) = \mathfrak{r}_i$ and $\mathfrak{z}_i = \mathfrak{r}_i^{-1}\mathfrak{r}_i^*$. \mathfrak{z}_i is certainly in the centre, for \mathfrak{r}_i and \mathfrak{r}_i^* induce the same automorphism. Denoting the expression on the left hand side of (7) by p we must have $\mathfrak{a}(p) = \mathfrak{a}(e) = \mathfrak{e}$. But if we make use of (3, I) and the fact that $\mathfrak{a}(r)$ is a homomorphism we obtain

$$\prod_{i=1}^{N} \chi_{a_i} \left(\mathfrak{r}_{t_i}^{\tau_i} \right) = \mathfrak{e} \tag{8}$$

which is equivalent to (6).

Now suppose that we are given the elements \mathfrak{z}_i i.e. that we are given \mathfrak{r}_i inducing the automorphisms χ_{r_i} and satisfying (8). Then if we put

$$\mathfrak{a}\left(\prod_{i=1}^{N}b_{i}^{-1}r_{s_{i}}^{\tau_{i}}b_{i}\right)=\prod_{i=1}^{N}\chi_{b_{i}}\left(r_{s_{i}}^{\sigma_{i}}\right),$$

we have a definition of a(r) which can be seen to be unique on account of (8), and to be a homomorphism of \Re in \Re .

If

$$r = \prod_{i=1}^N b_i^{-1} r_{s_i}^{\sigma_i} b_i$$

 \mathbf{then}

$$\mathfrak{a}(a^{-1}ra) = \mathfrak{a}\left(\prod_{i=1}^{N} (b_{i}a)^{-1} r_{s_{i}}^{\sigma_{i}} b_{i}a\right)$$

 $= \prod_{i=1}^{N} \chi_{b_{i}a}(\mathfrak{r}_{s_{i}}^{\sigma_{i}}) = \chi_{a}(\mathfrak{a}(r)),$

i.e. (3, I) is satisfied. Also

$$egin{aligned} \chi_{a^{-1}r_ia}\left(\mathfrak{b}
ight) &= \chi_aig(\chi_{r_i}ig(\chi_{a^{-1}}\left(\mathfrak{b}
ight)ig))\ &= \chi_a(\mathfrak{r}_i^{-1})\,\mathfrak{b}\,\chi_a\left(\mathfrak{r}_iig) \end{aligned}$$

so that (3, II, $a^{-1}r_i a, b$) is satisfied. But if (3, II, r, b) and (3, II, s, b) are satisfied for all b then (3, II, rs, b) is satisfied for all b. Consequently (3, II) is satisfied and the corollary to theorem 1 applies.

In the cases when the centre of \mathfrak{N} consists either of the identity alone or of the whole group there is always a solution of the equations (6). The expressions on the right hand sides of these equations always represent centre elements, so that in the case where the centre consists of the identity alone, there is a solution by putting $\mathfrak{z}_i = \mathfrak{e}$ for each *i*. If \mathfrak{N} is Abelian we put $\mathfrak{z}_i = \mathfrak{r}_i^*$. For the general case we have to be able to find all the relations (7).

§ 2. The relations between the relations of a group.

Suppose \mathfrak{F} is a free group with the generators e_1, \ldots, e_n and \mathfrak{R} is the least self conjugate subgroup containing certain elements r_1, r_2, \ldots, r_l . The factor group will be called \mathfrak{G}' . As has been shewn it is important in the extension problem to be able to express the structure of \mathfrak{G}' in terms of relations between the conjugates of the relations r_1, r_2, \ldots, r_l . This problem has been solved by Reidemeister ⁶). It is necessary to repeat his conclusions to obtain another theorem on extensions (theorem 4).

Precisely the problem may be stated as follows. \Re is generated by all elements of \Im of form $a^{-1}r_i a$; it may therefore be regarded as the factor group Φ/\mathbf{P} of the the free group Φ with the generators $E_{i,a}$ with respect to some self conjugate subgroup \mathbf{P} . The problem is to find a set of elements of Φ whose conjugates generate \mathbf{P} . \mathbf{P} contains for instance all elements of form

$$E_{i, ab^{-1}r_{,b}} E_{j,b}^{-1} E_{i,a}^{-1} E_{j,b}.$$
(9)

If our method for finding the relations **P** is to be constructive it is necessary that the structure of the original group \mathfrak{G}' should be known, or what amounts to the same, that we have a constructive method for determining whether a given member of \mathfrak{F} is a member of \mathfrak{R} . If this is the case we can find a constructive function v_a defined for all a in \mathfrak{F} , constant in each coset of \mathfrak{R} , taking its value in that coset and satisfying $v_e = e$. These elements are a set of representatives of the cosets of \mathfrak{R} . If we put $v_a^{-1}a = r_a$ then r_a is a relation (member of \mathfrak{R}) for each a.

We define $r_{a,e}$ by the condition

$$v_a e_i = v_{ae_i} r_{a,e_i}$$

Then \Re is generated by the relations $b^{-1}r_{a,e_i}b$. For if $\overline{\Re}$ is the group generated by these and contains r_c , then

$$\left. \begin{array}{l} r_{ce_{i}} = r_{c, e_{i}} e_{i}^{-1} r_{c} e_{i} \epsilon \overline{\mathfrak{R}} \\ \\ r_{ce_{i}^{-1}} = e_{i} r_{ce_{i}^{-1}, e_{i}} r_{c} e_{i}^{-1} \epsilon \overline{\mathfrak{R}}. \end{array} \right\}$$
(10)

and

But $\overline{\Re}$ contains $r_e = e$; it therefore contains r_c for each c.

Now suppose that for each r_{v_e,e_i} we have chosen an element R_{v_e,e_i} of Φ corresponding to it in the homomorphism τ of Φ on \Re and let us define automorphisms χ_a by

⁶⁾ K. REIDEMEISTER, Knoten und Gruppen [Hamb. Abhandl. 5 (1926), 8-23].

A. M. Turing.

$$\chi_a(E_{i,b}) = E_{i,ba}. \tag{11}$$

Then we may define R_c recursively by the equations

$$\left. \begin{array}{l} R_{e} = E \\ R_{ce_{i}} = R_{v_{c}, e_{i}} \, \chi_{e_{i}} \left(R_{c} \right) \\ R_{ce_{i}^{-1}} = \chi_{e_{i}^{-1}} \left(R_{v_{c}, e_{i}} \, R_{c} \right) \end{array} \right\}$$
(12)

so that if either $k = e_i$ or $k = e_i^{-1}$ we shall have

$$R_{ck} = R_{v,k} \chi_k(R_c). \tag{13}$$

Our definition will be valid if and only if we always have

$$R_{(ce_i)e_i^{-1}} = R_{(ce_i^{-1})e_i} = R_c$$

It may easily be verified that this is so.

Since the equations (13) and

$$r_{ck} = r_{v_{a}k} \, k^{-1} \, r_{c} \, k \tag{14}$$

hold whenever k is a generator or its inverse, R_c must correspond to r_c in τ . Now for all b, i we have

 $r_{v_h r_i} = r_i$

and therefore $R_{v_b r_i}$ and $E_i(=E_{i,e})$ must belong to the same coset of **P**. I.e.

$$R_{v_b r_i} E_i^{-1} \tag{15}$$

must belong to **P**. By operating with the automorphisms χ_a we see that all elements of form

$$\chi_a(R_{v_b r_i} E_i^{-1}) \tag{16}$$

belong to \mathbf{P} . The structure of \Re may now be decribed by

THEOREM 3.

The group of relations **P** of \Re is the least self conjugate subgroup of Φ containing all elements of form (9) and (16).

Only a sketch is given for the proof of this theorem. The first step is to shew that

$$R_{ax} = R_{v_a x} \,\chi_x(R_a) \tag{17}$$

for all x, a. For this purpose we consider the set Ξ of all x such that (17) holds for all a. Then we can shew that xy belongs to Ξ if x and y belong to it. The generators e_i , e_i^{-1} belong to Ξ by (13).

364

Now let $\overline{\mathbf{P}}$ be the self conjugate subgroup of Φ generated by (9), (16). We shew that $R_{v_a r}$ is independent of a modulo $\overline{\mathbf{P}}$ and that if we allow K(r) to stand for the coset $\overline{\mathbf{P}}$ of containing R_r , then K(r) gives a homomorphism of \Re on $\Phi/\overline{\mathbf{P}}$. But there is certainly a homomorphism τ' of $\Phi/\overline{\mathbf{P}}$ on \Re determined by τ and satisfying $\tau'(K(r)) = r$. This is only possible if τ' and K are isomorphisms and $\mathbf{P} = \overline{\mathbf{P}}$.

To prove these properties of K we call **H** the totality of relations r for wich $R_{v_a r}$ is independent of a modulo **P**, and we shew successively

I) if r, s belong to **H** then $R_{v_s rs} \in K(r) K(s)$,

II) if r belongs to **H** then $R_{v_r}r^{-1} \in K(r)^{-1}$,

III) if r belongs to **H** and k is a generator or its inverse then $R_{v_ak}^{-1} r_k \epsilon \chi_k(K(r))$ (with an obvious adaptation of the meaning of χ_k).

For the proof of I), II), III), (17) is essential and so is the invariance of $\overline{\mathbf{P}}$ under the automorphisms χ_a .

Now let us return to the extension problem. For this purpose the only significant relations are those given by (15). In fact we have

THEOREM 4.

In theorem 2 we may replace the condition (6) by the condition that if the homomorphism ϑ of Φ on \Re be determined by

$$\vartheta(E_{i,a}) = \chi_a \left(\mathfrak{r}_i^* \mathfrak{z}_i^{-1} \right) \tag{18}$$

then we must have $\vartheta(X) = \mathfrak{e}$ for all X of form (15).

The homomorphism ϑ transforms the automorphism χ_a of § 2 into the automorphism χ_a of § 1. I.e.

$$\vartheta(\chi_a(X)) = \chi_a(\vartheta(X)).$$

In particular if $\vartheta(X) = \mathfrak{e}$ we shall have

$$\vartheta(\chi_a(X)) = \chi_a(e) = e$$

so that the elements of form (16) are mapped on the identity by ϑ . It remains to shew that $\vartheta(Z) = \mathfrak{e}$ for all Z of form (9).

$$\begin{split} \vartheta(E_{i,ab^{-1}r_{j}b} E_{j,b}^{-1} E_{i,a}^{-1} E_{j,b}) \\ &= \chi_{ab^{-1}r_{j}b} (\mathfrak{r}_{i}) \chi_{b}(\mathfrak{r}_{j}^{-1}) \chi_{a}(\mathfrak{r}_{i}^{-1}) \chi_{b}(\mathfrak{r}_{j}) \\ &= \chi_{b} (\chi_{ab^{-1}r_{j}}(\mathfrak{r}_{i}) \mathfrak{r}_{j}^{-1} \chi_{ab^{-1}}(\mathfrak{r}_{i}^{-1}) \mathfrak{r}_{j}) \\ &= \chi_{b}(e) \text{ by (5). We have put } \mathfrak{r}_{i}^{*} \mathfrak{z}_{b}^{-1} = \mathfrak{r}_{i}. \end{split}$$

A. M. Turing.

Thus ϑ maps the whole of **P** on the identity and the conditions of theorem 2 are satisfied.

§ 3. Cyclic extensions.

When \mathfrak{G}' is a cyclic group of order n we take \mathfrak{F} to be the free group with the single generator a and \mathfrak{R} to be the subgroup generated by $q \equiv a^n$. The representative elements v_b may be taken to be

$$e, a, a^2, \ldots, a^{n-1}.$$

We easily find that

$$r_{a^p,a} = e ext{ if } p \not\equiv -1 \pmod{n}$$

 $r_{a^{n-1},a} = q.$

If Q_{a^p} be the element of Φ corresponding to $a^{-p}qa^p$ we have

$$R_{a^{p},a} = E,$$

$$R_{a^{n-1},a} = Q$$

and from the equations (12) we obtain

$$egin{array}{ll} R_{a^p} &= E \ R_{a^{n+p}} &= Q_{a^p}. \end{array}$$
 $(0 \leq p \leq n-1)$

The expressions (15) are therefore

$$Q_{a^p}Q^{-1}$$
 $(p=0, 1, \ldots, n-1).$ (19)

If ϑ is a homomorphism of Φ and $\vartheta(Q_a^{-1}Q) = \mathfrak{e}$, then

$$\vartheta(Q_{a^p}) = \vartheta(Q_{a^{p-1}}) = \ldots = \vartheta(Q).$$
 (20)

Now making use of (19), (20), theorem 4 for a cyclic extension becomes

THEOREM 5.

A is a class of automorphisms of a group \mathfrak{N} . A^w is the first power of A which is the class of inner automorphisms and ξ is an arbitrary automorphism out of A. \mathfrak{r}^* is an element of \mathfrak{N} which induces the inner automorphism ξ^n . Then there is an extension of \mathfrak{N} by the cyclic group of order n realising the classes A, A^2 , ... of automorphisms if and only if there is an element \mathfrak{z} in the centre of \mathfrak{N} satisfying

$$\xi(\mathfrak{z})\mathfrak{z}^{-1} = \xi(\mathfrak{r}^*)\mathfrak{r}^{*-1}.$$
(21)

We have put

$$\vartheta(Q) = \mathfrak{r}^*\mathfrak{z}^{-1}$$
$$\vartheta(Q_a) = \xi(\mathfrak{r}^*\mathfrak{z}^{-1}).$$

If we put $\xi(\mathfrak{z})\mathfrak{z}^{-1} = \varphi(\mathfrak{z})$ then φ is a (possibly improper) automorphism of the centre \mathfrak{z} of \mathfrak{N} . For some groups all of the automorphisms φ are improper. This is the case for all cyclic groups whose order is a power of 2. In these cases we shall have unrealisable classes of automorphisms if $\xi(\mathfrak{r}^*)\mathfrak{r}^{*-1}$ is not in $\varphi(\mathfrak{Z})$. Suppose for instance that \mathfrak{N} is the dihedral group D_{10} of order 20, generated by a, b with the relations

$$a^{10} = b^2 = (ab)^2 = e.$$

The centre of this group consists of e and a^5 . We define the automorphism ξ by

$$egin{array}{ll} \xi(a)=a^7\ \xi(b)=ba^5, \end{array}$$

then

$$egin{array}{ll} \xi^2(a) = a^{-1} = b^{-1}ab, \ \xi^2(b) = b = b^{-1}bb. \end{array}$$

 r^* can therefore be taken to be b. The equation (21) becomes

$$\xi(z)z^{-1} = \xi(b)b^{-1} = a^5,$$

but $\xi(z)z^{-1} = e$ for both centre elements.

(Received March 22nd, 1937.)

[11]