

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/legal.php>). 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.

NUMDAM

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{N} by \mathfrak{G}' if \mathfrak{N} is a self conjugate subgroup of \mathfrak{G} and $\mathfrak{G}/\mathfrak{N} \cong \mathfrak{G}'$. The problem of finding the extensions of \mathfrak{N} 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{I} the subgroup of inner automorphisms. Then to each coset γ of \mathfrak{N} in \mathfrak{G} there corresponds a coset $X(\gamma)$ of \mathfrak{I} 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 $\mathfrak{A}/\mathfrak{I}$. Baer's investigations are concerned with finding all possible groups \mathfrak{G} when \mathfrak{N} , \mathfrak{G}' and the homomorphism $X(\nu)$ are given. As a first step towards the solution

of this problem the possible structures of $\mathfrak{G}/\mathfrak{Z}(\mathfrak{N})$ are found, where $\mathfrak{Z}(\mathfrak{N})$ 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{N} 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{R} (i.e. $\chi_a(b)$ as a function of b is an automorphism of \mathfrak{R} and satisfies

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

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

$$\left. \begin{aligned} a) \quad & \chi_a(b) = (w(a))^{-1}bw(a) \quad (\text{I}, a, b) \\ & w(r) = \alpha(r) \quad (\text{II}, r) \end{aligned} \right\} \quad (2)$$

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

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

c) $w(\mathfrak{R}) = \mathfrak{R} \cap w(\mathfrak{F})$

if and only if

$$\left. \begin{aligned} \chi_a(\alpha(r)) &= \alpha(a^{-1}ra) \quad (\text{I}, a, r) \\ \chi_r(b) &= (\alpha(r))^{-1}b\alpha(r) \quad (\text{II}, r, b) \end{aligned} \right\} \quad (3)$$

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

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

COROLLARY:

\mathfrak{F} is a free ⁴⁾ group with a self conjugate subgroup \mathfrak{R} ($\mathfrak{F}/\mathfrak{R} \cong \mathfrak{G}'$, 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{R} and \mathfrak{G} by German letters, and elements of $\mathfrak{F}/\mathfrak{R}$ by Greek letters. e, ϵ, ε 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 $\alpha(r)$ to be related to a function $w(a)$ as in the theorem. Let \mathfrak{G} be the cyclic group $\{b\}$ of order 4, \mathfrak{F} the cyclic group $\{g\}$ of order 2, and let \mathfrak{R} be $\{b^2\}$ and $\chi_g(b^2) = b^2$. Then we should have to have $\alpha(e) = e$. But $\alpha(e) = \alpha(g^2) = b^2$.

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

Proof of the theorem. The necessity of the conditions is trivial. (3, I, a, r) follows from (2, I, $a, \alpha(r)$), (2, II, r), (2, II, $a^{-1}ra$) and the fact that α is a homomorphism: (3, II, r, \mathfrak{b}) follows immediately from (2, I, r, \mathfrak{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, α) (a in \mathfrak{F} , α in \mathfrak{R}), (a', α') being equivalent to (a, α) if and only if $a^{-1}a'$ belongs to \mathfrak{R} and $\alpha(a^{-1}a') = \alpha' \alpha^{-1}$.

This is an equivalence relation, for

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

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

i.e. the relation is symmetric.

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

i.e. the relation is reflexive.

3) If $a^{-1}a' \in \mathfrak{R}, \quad a'^{-1}a'' \in \mathfrak{R},$

$$\alpha(a^{-1}a') = \alpha \alpha'^{-1} \text{ and } \alpha(a'^{-1}a'') = \alpha' \alpha''^{-1},$$

then

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

$$\alpha(a^{-1}a'') = \alpha(a^{-1}a') \alpha(a'^{-1}a'') = \alpha \alpha'^{-1} \alpha' \alpha''^{-1} = \alpha \alpha''^{-1},$$

i.e. the relation is transitive.

The product of two pairs is defined by

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

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

$$\left. \begin{aligned} a^{-1}a' \in \mathfrak{R}, \quad b^{-1}b' \in \mathfrak{R} \\ \alpha(a^{-1}a') = \alpha \alpha'^{-1} \text{ and } \alpha(b^{-1}b') = \mathfrak{b}\mathfrak{b}'^{-1} \end{aligned} \right\} \quad (4)$$

then

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

Now

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

and

$$\begin{aligned} a((ab)^{-1}(a'b')) &= \chi_b(a a'^{-1})bb'^{-1} \\ &= \chi_b(a)b \cdot b'^{-1} \cdot (bb'^{-1})^{-1} \chi_b(a'^{-1})bb'^{-1} \\ &= (\chi_b(a)b) \cdot (\chi_{b'}(a')b')^{-1} \end{aligned}$$

by (4), (3, II, $b^{-1}b'$, $\chi_b(a')$) and (1).

The product is also associative, for

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

and these two expressions are equal on account of (1) and the fact that χ_c 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.

$w(a)$ is defined by

$$w(a) = (a, e)$$

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

$$\begin{aligned} (w(a))^{-1}bw(a) &= (a^{-1}, e)b(a, e) \\ &= (a^{-1}, e)(a, \chi_a(b)) \\ &= (e, \chi_a(b)) = \chi_a(b). \end{aligned}$$

Since

$$\begin{aligned} (g, b) &= (g, e)(e, b) \\ &= w(g)b \end{aligned}$$

condition b is satisfied.

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

Proof of the corollary. Suppose \mathfrak{G} is a group with the required properties, e_1, e_2, \dots, 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, \dots, e_n be elements of \mathfrak{G} with the property that e_i is in the coset $\omega(e_i)$ of \mathfrak{N} and that

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

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

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

If we put $\mathfrak{w}(r) = a(r)$ for elements r of \mathfrak{R} 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.

\mathfrak{N} is a given group. \mathfrak{F} is a free group with the generators e_1, e_2, \dots

r_1, r_2, \dots, r_l . Let us put $\alpha(r_i) = r_i$ and $\beta_i = r_i^{-1}r_i^*$. β_i is certainly

$\alpha(p) = \alpha(e) = e$. But if we make use of (3, I) and the fact that $\alpha(r)$ is a homomorphism we obtain

$$\prod_{i=1}^N (r_i)$$

(2)

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

Suppose \mathfrak{F} is a free group with the generators e_1, \dots, e_n and \mathfrak{R} is the least self conjugate subgroup containing certain elements r_1, r_2, \dots, 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, \dots, r_l . This problem has been solved by Reidemeister⁶⁾. It is necessary to repeat his conclusions to obtain another theorem on extensions (theorem 4).

Precisely the problem may be stated as follows. \mathfrak{R} is generated by all elements of \mathfrak{F} of form $a^{-1}r_ia$; 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

$$E_{i,ab^{-1}r_jb} E_{j,b}^{-1} E_{i,a}^{-1} E_{j,b} \tag{9}$$

If our method for finding the relations \mathbf{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_i} by the condition

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

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

$$\left. \begin{aligned} r_{ce_i} &= r_{c,e_i} e_i^{-1} r_c e_i \in \overline{\mathfrak{R}} \\ r_{ce_i^{-1}} &= e_i r_{ce_i^{-1},e_i} r_c e_i^{-1} \in \overline{\mathfrak{R}}. \end{aligned} \right\} \tag{10}$$

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

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

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

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

Then we may define R_c recursively by the equations

$$\left. \begin{aligned} R_e &= E \\ R_{ce_i} &= R_{v_c, e_i} \chi_{e_i}(R_c) \\ R_{ce_i^{-1}} &= \chi_{e_i^{-1}}(R_{v_c, e_i} R_c) \end{aligned} \right\} \tag{12}$$

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

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

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

$$r_{ck} = r_{v_c, k} k^{-1} r_c k \tag{14}$$

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

$$r_{v_b, r_i} = r_i$$

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

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

must belong to \mathbf{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 \mathfrak{R} may now be described by

THEOREM 3.

The group of relations \mathbf{P} of \mathfrak{R} 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 \mathcal{E} of all x such that (17) holds for all a . Then we can shew that xy belongs to \mathcal{E} if x and y belong to it. The generators e_i, e_i^{-1} belong to \mathcal{E} by (13).

Thus ϑ maps the whole of \mathbf{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

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

We easily find that

$$\begin{aligned} r_{a^p, a} &= e \text{ if } p \not\equiv -1 \pmod{n} \\ r_{a^{n-1}, a} &= q. \end{aligned}$$

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

$$\begin{aligned} R_{a^p, a} &= E, \\ R_{a^{n-1}, a} &= Q \end{aligned}$$

and from the equations (12) we obtain

$$\begin{aligned} R_{a^p} &= E \\ R_{a^{n+p}} &= Q_{a^p}. \end{aligned} \quad (0 \leq p \leq n-1)$$

The expressions (15) are therefore

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

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

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

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

We have put

$$\begin{aligned}\vartheta(Q) &= r^*z^{-1} \\ \vartheta(Q_a) &= \xi(r^*z^{-1}).\end{aligned}$$

If we put $\xi(z)z^{-1} = \varphi(z)$ then φ is a (possibly improper) automorphism of the centre 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 $\xi(r^*)r^{*-1}$ is not in $m(\mathfrak{N})$.

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

$$\begin{aligned}\xi(a) &= a^7 \\ \xi(b) &= ba^5,\end{aligned}$$

then

$$\begin{aligned}\xi^2(a) &= a^{-1} = b^{-1}ab, \\ \xi^2(b) &= b = b^{-1}bb.\end{aligned}$$

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.)
