MÉMOIRES DE LA S. M. F.

LEONHARD GERHARDS

Grouptheoretical investigations on computers

Mémoires de la S. M. F., tome 49-50 (1977), p. 65-91

<http://www.numdam.org/item?id=MSMF_1977__49-50__65_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math. France
Mémoire 49-50, 1977, p. 65-91

GROUPTHEORETICAL INVESTIGATIONS ON COMPUTERS

by

Leonhard Gerhards

Many problems in the theory of finite groups depend on the knowledge of the structure of the lettice V(G) of subgroups of a finite group G and its automorphism group Aut G. Especially for solving problems in the theory of factorization of G and in the theory of group extensions the structure of V(G) and Aut G is fundamental. Therefore, a program for computational determination of V(G) and Aut G has been developed for the computer system IBM 7090/1410 at IIM/GMD*), Bonn [6], [11], [4].

The aim of this paper is to give a systematical survey about the program, the ideas and the mostly detailed theoretical concepts of which are considered in many other papers [1], [5], [7]. In 6 sections the present paper mainly written under computational aspects contains a complete description of the principal methods and algorithms of the program in a most effective form, as they are implemented in the computer.

Under the point of view that in general computational algorithms in group theory are based on time-saving methods for the representation and multiplication of elements of G, we develop in section 1. by using parts of the group table T(G) of G a most effective multiplication algorithm for elements of G represented by a "normal form" of abstract generators and defining relations. In section 2. methods for the generating of groups by a system of generating elements of G are discussed [4]. In section 3. the representation of subgroups of G by "characteristic numbers" [12] and the use of Boolean operations are introduced.

In the main section 4. the fundamental princips for determining V(G), namely the "method of filters" [6] and the "algorithm of composition" [11] are discussed. We notice that the developed method is of combinatorial type and does not require group theoretical ussumptions of G as in [12].

The central section 5. contains a complete description of the determination of Aut G for the general case that G contains a "Hall system" $H_1,\ldots,H_r$ of subgroups H_i (i=1,...,r) of G [7]. Taking the theory of factorization as a basis [1], [13], the automorphisms of G are obtained by "composition of allowable automorphisms" of the subgroups H_i(i=1,2) and special inner automorphisms. This algorithm-different from the concept of [5]-has been developed for solvable groups by E. Geller [4].

*) IIM Institut für Instrumentelle Mathematik, Univ. Bonn
GMD Gesellschaft für Mathematik und Datenverarbeitung, Bonn

Finally in section 6 the representation of automorphisms as permutations or as words of abstract generators are briefly discussed.

1. Methods for the representation of group elements in a computer [10], [4], [9]

1.1 Computational algorithms in finite group theory in general are based on effective methods for representing and multiplying the elements of a finite group G in a computer M.

1.1.1 A 1-1-mapping φ: G → S of G in a structure S is called a representation of G in M, if S can be realized in M and if

(1.1) $\varphi(a_i a_j) = \varphi(a_i) \cdot \varphi(a_j)$ for all pairs $(a_i, a_j) \subseteq G$.

1.1.2 The realization of S, however, means that the following conditions for φ are satisfied:

(1.2) Every element $a \in G$ can uniquely be represented by the "normal form" $\varphi(a)$ in M.

(1.3) There exists a most effective unique algorithm for the determination of the normal form $\varphi(a_i, a_j)$ of the product $a_i . a_j$ using the normal forms $\varphi(a_i)$ and $\varphi(a_j)$ of the factors a_i, a_j for all pairs $(a_i, a_j) \subseteq G$.

1.1.3 The group table T(G) of G as a special representation

Knowing the group table T(G) of G we can regard the columns of T(G) as a relation system of the greatest generating system of G with pairwise different elements or as the right regular representation of G by permutations of degree $|G|$. These representations satisfy the conditions (1.3) and (1.4).

Both interpretations of T(G) are extreme cases for representing G in M by abstract generators with a system of defining relations or by permutations.

1.2 Representation of G by permutations

1.2.1 If φ: G → S_r is an isomorphic map of G in the symmetric group S_r of degree r, then to every element $a \in G$ there corresponds as a normal

form a permutation $\varphi(a) = \begin{pmatrix} 1,\ldots,r \\ i_1,\ldots,i_r \end{pmatrix}$ of S_r stored in M as a product of well defined cycles. Such a representation of G satisfies the conditions (1.2) and (1.3). But only if the degree r of the permutations is relatively small ($r \leq 10$) the representation of the elements of G by permutations is useful, because multiplication of two permutations of high degree is a time-consuming process in M.

Therefore, if the degree of the smallest permutation subgroup of S_r isomorphic with G is relatively high, it seems to be necessary to represent the elements of G by abstract generators and defining relations.

1.3 Representation of G by abstract generators and defining relations [4], [16]

1.3.1 Special generating systems of G

If G is a finite group with a chain $\langle e\rangle = H_0 \subset \ldots \subset H_n = G$ of subgroups $H_i (i=1,\ldots,n)$ of G such that

$$H_i = \langle H_{i-1}, a_i\rangle, \quad H_i = H_{i-1} + H_{i-1}a_i + \ldots + H_{i-1}a_i^{r_i-1}, \quad a_i^{r_i} \in H_{i-1}$$

the system $\{a_1,\ldots,a_n\}$ is a generating system of G satisfying the defining relations:

$$a_i^{r_i} = a_1^{\nu_{i,1}} \cdot \ldots \cdot a_{i-1}^{\nu_{i,i-1}} \qquad (i=1,\ldots,n)$$

(1.4)

$$a_k^{\beta} a_i = a_1^{\mu_{k,\beta,i,1}} \cdot \ldots \cdot a_k^{\mu_{k,\beta,i,k}} \qquad \begin{bmatrix} k=2,\ldots,n,\ i=1,\ldots,k-1 \\ \beta=1,\ldots,r_k-1 \end{bmatrix}$$

Every element $g \in G$ can uniquely be written as a word of the generators $a_1,\ldots,a_n$:

$$g = a_1^{\lambda_1} \cdot \ldots \cdot a_n^{\lambda_n} \quad (0 \leq \lambda_i < r_i, \quad i = 1,\ldots,n),$$

and the representation φ: G → S is defined by

$$g \xrightarrow{\varphi} \varphi(g) = (\lambda_1,\ldots,\lambda_n)$$

We call a generating system of G satisfying (1.4) a special generating system of G.

1.3.2 Special generating systems for solvable groups

If G is solvable, one can always find a chain of subnormal subgroups of G:

$$\langle e\rangle = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_n = G$$

with cyclic factor groups N_i/N_{i-1} $(i=1,\ldots,n)$ such that

$$N_{i-1} = \langle a_1,\ldots,a_{i-1}\rangle \ , \ N_i = \langle N_{i-1},a_i\rangle \ .$$

Then the system $\{a_1,\ldots,a_n\}$ is a special generating system of G with the following system of defining relations:

$$\begin{aligned} & a_i^{r_i} \in N_{i-1} && (i=1,\ldots,n) \\ & a_k a_i a_k^{-1} \in N_{k-1} && (k=2,\ldots,n \ , \ i=1,\ldots,k-1) \end{aligned} \tag{1.5}$$

1.3.3 If the elements of G are represented as words of the elements of a special generating system of G with defining relations (1.4) or (1.5), the computing time for the normal form $\mathcal{P}(g_1g_2)$ of a product $g_1 \cdot g_2$ in G using the normal forms $\mathcal{P}(g_1)$ and $\mathcal{P}(g_2)$ of the factors g_1,g_2 mainly depends on the number of the generating elements of G and on the form of the defining relations (1.4) or (1.5). But by changing the representation of G and storing parts of the group table T(G) we are able to make multiplication in M more effective.

1.3.4 Change of the representation of G by storing parts of T(G)

Let be

$$\langle e\rangle = H_0 \subset H_1 \subset \ldots \subset H_n = G \tag{1.6}$$

any chain of subgroups of G with index $r_i := [H_i:H_{i-1}]$, $(i=1,\ldots,n)$. Further let $R_i := \{\alpha_i^{(j)} / \ j = 0,\ldots,r_i-1\}$ be a system of representatives

of a right coset decomposition of H_i by $H_{i-1}(i=1,\ldots,n)$, $\alpha_i^{(o)} = e$. Then every element $g \in G$ has a unique representation in the form:

$$g = \alpha_1^{(\lambda_1)} \cdot \alpha_2^{(\lambda_2)} \cdot \ldots \cdot \alpha_n^{(\lambda_n)} . \tag{1.7}$$

But if the relations

$$\alpha_j^{(\lambda_j)} \cdot \alpha_i^{(\lambda_i)} = \alpha_1^{(\mu_1)} \cdot \ldots \cdot \alpha_j^{(\mu_j)} ; \; \mu_\nu = f(\nu,j,i,\lambda_j,\lambda_i) \; (\nu=1,\ldots,j)$$

$$(j=1,\ldots,n \; , \quad i=1,\ldots,j, \; \lambda_j=0,\ldots,r_{j-1}, \quad \lambda_i=0,\ldots,r_{i-1}) \tag{1.8}$$

are known the system $\mathfrak{M} = \bigcup_{i=1}^{n} R_i$ is a generating system of G, and using (1.8) a product $g = g_1 \cdot g_2$ of two elements $g_1 = \alpha_1^{(\lambda_1)} \cdot \ldots \cdot \alpha_n^{(\lambda_n)}$, $g_2 = \alpha_1^{(\mu_1)} \cdot \ldots \cdot \alpha_n^{(\mu_n)}$ of G in normal form can be reduced in a finite number of steps on normal form.

To prove this we denote by W_j a word $\alpha_1^{(\nu_1)} \cdot \ldots \cdot \alpha_j^{(\nu_j)}$ of length j generated in normal form by elements of $\mathfrak{M}$. Further let $W_{n-1}^{(o)} = \alpha_1^{(\lambda_1)} \cdot \ldots \cdot \alpha_{n-1}^{(\lambda_{n-1})}$. Then using the defining relations:

$$\alpha_n^{(\lambda_n)} \alpha_1^{(\mu_1)} = W_{n-1}^{(1)} \alpha_n^{(\lambda_{n,1})}$$

$$\alpha_n^{(\lambda_{n,1})} \alpha_2^{(\mu_2)} = W_{n-1}^{(2)} \alpha_n^{(\lambda_{n,2})}$$

$$\ldots\ldots\ldots$$

$$\alpha_n^{(\lambda_{n,n-1})} \alpha_n^{(\mu_n)} = W_{n-1}^{(n)} \alpha_n^{(\lambda_{n,n})}$$

we reduce the product of two words of length n in n steps to the calculation of n products $\bar{W}_{n-1}^{(i)} = \bar{W}_{n-1}^{(i-1)} W_{n-1}^{(i-1)}$ $(i = 1,\ldots,n)$,

$\bar{W}_{n-1}^{(o)} := W_{n-1}^{(o)}$.

According to this result for the number Σ_n of effective entries in the relation table (1.8) by the computer we obtain the estimation:

$$\Sigma_n < n! \cdot e \quad \text{(e eulerian number)}$$

1.3.5

Representation and multiplication of the elements of G by syllables in the α's.

Let

$$(1.9) \qquad \langle e \rangle = H_o^* \subset H_1^* \subset \ldots \subset H_{m^*}^* = G;\ H_k^* = H_{i_k} \quad (k = 1,\ldots,m^*,\ 1 \leq m^* < n)$$

be a chain of subgroups of G, which is coarser than the chain (1.6). Then any representative $A_k^{(\nu_k)}$ of the right coset decomposition of H_k^* by H_{k-1}^* $(k = 1,\ldots,m^*)$ can be written as a word of the α's in normal form:

$$(1.10) \qquad A_k^{(\nu_k)} = \alpha_{i_{k-1}+1}^{(\lambda_{i_{k-1}+1})} \cdot \ldots \cdot \alpha_{i_k}^{(\lambda_{i_k})}$$

and every element $g \in G$ can be uniquely represented as a word in the syllables $A_k^{(\nu_k)}$:

$$g = A_1^{(\nu_1)} \cdot \ldots \cdot A_{m^*}^{(\nu_{m^*})}$$

The corresponding relation tables:

$$A_j^{(\lambda_j)} A_i^{(\lambda_i)} = A_1^{(\mu_1)} \cdot \ldots \cdot A_j^{(\mu_j)} \quad (j \geq i)$$

can be determined by using the multiplication for the α's.

1.3.6 Extension of special generating systems

If $\mathfrak{A} = \{a_1,\ldots,a_n\}$ is a special generating system of G satisfying the relations (1.4), then the groups H_k of the chain (1.6) and the representatives $\alpha_k^{(\sigma)}$ are given by $H_k = \langle a_1,\ldots,a_k \rangle$, $\alpha_k^{(\sigma)} = a_k^{\sigma}$ and for multiplying

elements of G represented in normal form described in 1.3.4 we still use the tables T_{ki} for the words of the right sides of the following extended relation system:

$$(1.11) \qquad a_k^{\beta} a_i^{\mu} = W_{ki}^{(\beta,\mu)}(a_1,\ldots,a_k) \quad \left[\begin{matrix}\beta = 1,\ldots,r_{k-1} \\ \mu = 1,\ldots,r_{i-1}\end{matrix} \quad ; \quad k > i\right]$$

It can easily be shown that it is possible to determine the tables T_{ki} $(i=1,\ldots,k-1)$, if the multiplication of elements of G of length $j \leq k-1$ can be executed by the computer. The latter, however, can be done, because the complete tables T_{ji} $(j > i,\ j = 2,\ldots,k-1,\ i = 1,\ldots,j-1)$ have already previously been determined and stored.

1.3.7 Decision of the multiplication form

Assuming that every $g = \alpha_1^{(\lambda_1)} \cdot \ldots \cdot \alpha_n^{(\lambda_n)} \in G$ represented as in 1.3.4 can be stored by a normal form as a n-tupel $\varphi(g) = (\lambda_1,\ldots,\lambda_n)$ in only one cell, the place using by the computer for storing the relation tables (1.8) amounts to

$$(1.12) \qquad R = \sum_{i=1}^{n}{}' r_i^2 + \sum_{\substack{i,k=1 \\ k>i}}^{n} r_k \cdot r_i \qquad \text{cells.}$$

In the case that the number of generators of G is greater than 2 the computer proves, if the sequence of the relative orders r_i of the generators α_i allows a multiplication in form of syllables in the sense of 1.3.5. Thereby a splitting of the words represented in the α's is selected by the computer in such a way that using the indices

$$S_k = \prod_{j=i_{k-1}+1}^{i_k} r_j = \left[H_k^* : H_{k-1}^*\right] \text{ of the chain (1.9) of G}$$

the number $S := \sum_{k=1}^{m^*} S_k^2 + \sum_{\substack{i,k=1 \\ k>i}}^{m^*} S_k \cdot S_i$ of cells for storing the multiplication tables is minimal. Empirically we get $m^* = 2,3,4$.

2. Methods for generating groups by a system of generating elements [4]

2.1 Let G be a group generated by the generating system $\{a_1,\ldots a_n\}$. Then if we develop a method, which allow us to construct $H_k = \langle H_{k-1}, a_k\rangle$ from H_{k-1} and a_k $(k = 1,\ldots,n)$, $H_o = \langle e\rangle$, G can be generated in n steps. If we denote by H a subgroup of G and by a an element of G with $a \notin H$, then $\bar{H} = \langle H,a\rangle$ can be obtained by determining appropriate cosets of H. For in the case that $U := \bigcup_i Hb_i$ is the union of all cosets of H determined in the process of generation and $ah \in U$ for every $h \in U$ we obtain $\bar{H} = U$.

2.2 Computational method

2.2.1 Fundamental princip of the method

Let H be a subgroup of G, $a \in G$, $a \notin H$ and let U denote the list for storing the group $\bar{H} = \langle H,a\rangle$ in the computer.
Starting with U := H every element $g \in U$ may be multiplied from the left side by a. If there exists an element $b = a\,g$ with $g \in U$, $b \notin U$, the list U must be extended by the coset $H\cdot b$ and $U := \langle H,a\rangle$ is completely determined if $a\cdot g \in U$ for all $g \in U$. Finding a new representative b, together with Hb all cosets Hb^j $(j = 2,\ldots,r-1)$ can be stored in U, where r is the smallest integer with $b^r \in H$.

2.2.2 Rationalization of the method

Because the generating process of a group is an often repeated procedure in group theoretical program systems, it seems to be profitable to abbreviate the method described in 2.2.1.
First of all it is easy to see that having determined the system $\mathcal{L}_1 = \{b_1,\ldots,b_s\}$ of all such representations of the coset decomposition of $\bar{H}$ by H with $b_i \in aH$ only additional representatives can be found among the products $b_i c_k$, where $c_k \in \mathcal{L}_2$ is the set of <u>all</u> representatives constructed up to now by the generating process. By this procedure we reduce the number of left multiplications with the element a, which must be executed by the method of 2.2.1.
Now, if the number of generators of G is greater than 2 we additionally can suppress further left multiplications.
Therefore, let $\mathcal{A} = \{a_1,\ldots,a_n\}$ be a generating system of G with

$H_i = \langle a_1,\ldots,a_i\rangle$, $H_o = \langle e\rangle$, $(i = 1,\ldots,n;\ n > 2)$ and $b_i^{(\nu)}(i = 1,\ldots,n;$ $\nu = o,\ldots,r_{\nu-1})$ may denote a representative of the coset decomposition of H_i by H_{i-1}. Further, set U as in 2.2.1. Then according to (1.7) every element $g \in G$ can be written as a normal form in the $b_i^{(\nu)}$'s:

$$g = b_1^{(\nu_1)} \cdot \ldots \cdot b_n^{(\nu_n)} \tag{2.1}$$

with the defining relations

$$b_k^{(\nu_k)} \cdot b_i^{(\nu_i)} = b_1^{(\mu_1)} \cdot \ldots \cdot b_k^{(\mu_k)}\ , \ (k \geq i). \tag{2.2}$$

If now $\mathfrak{b}_o = \{b_1^{(1)},\ldots,b_1^{(r_1-1)},\ldots,b_{k-1}^{(1)},\ldots,b_{k-1}^{(r_{k-1}-1)}\}$ is such a generating system of representatives for H_{k-1} without the representatives $b_i^{(\sigma)} = e$ $(i = 1,\ldots,k-1)$, every representative b of all cosets $H_{k-1}b$ with $a_k H_{k-1} \cap H_{k-1}b \neq \emptyset$ can be determined in the following way:

Storing $H_{k-1} \cup H_{k-1}a_k$ in U, $a := a_k$ is the first element of $\mathfrak{b}_1$.
Next we form the products $g = b_1 b_o$ of all $b_1 \in \mathfrak{b}_1$ of the increasing system $\mathfrak{b}_1$ and all elements $b_o \in \mathfrak{b}_o$. If $g \notin U$ we store g in $\mathfrak{b}_1$ and $H_{k-1}g$ in U.
Then $\mathfrak{b}_1$ is completely determined, if the described procedure cannot be countinued.

3. Representation of groups by characteristic numbers [6], [12]

3.1 Characteristic numbers

Let G be a finite group, {U} the set of all subgroups $U \leq G$ of G and {S(U)} the set of all systems S(U) consisting of all cyclic subgroups of G with prime power order contained in U. Then it is easy to prove that there exists a 1-1-correspondence {U} $\leftrightarrow$ {S(U)} between {U} and {S(U)}:

$$(3.1) \quad G \supseteq U \leftrightarrow S(U) = \{\langle z\rangle \subseteq G \;/\; \langle z\rangle \subseteq U,\ |\langle z\rangle| = p^{\alpha}, \alpha \geq 1,\ p \text{ prime}\}$$

Therefore, a system

$$(3.2) \quad E(U) = \{z_1,\ldots,z_m\} \quad (U \subseteq G,\ m = |S(U)|)$$

of generating elements of all cyclic subgroups of S(U) form a uniquely determined generating system of U of a special form.

First of all we list the elements of E(G) in the computer. Then, if $U \subseteq G$ and if $E(U) = \{z_{i_1},\ldots,z_{i_l}\} \subseteq E(G)$ ($\{i_1,\ldots,i_l\} \subseteq \{1,\ldots,|E(G)|\}$) is a complete generating system E(U) of U, by

$$(3.3) \qquad K[U] = \sum_{j=1}^{l} 2^{i_j - 1}$$

a dual number is defined, which uniquely corresponds to the subgroup U of G: $K[U] \leftrightarrow U$. This number K[U] shall be called the "characteristic number" of $U \subseteq G$, and every $U \subseteq G$ may be stored in the computer by its characteristic number K[U].

3.2 Boolean operations for characteristic numbers

The Boolean operations of intersection "$\wedge$" and disjunction "$\vee$" are useful for time-saving calculations with characteristic numbers:

$$(3.4) \quad \begin{array}{rcl} K[U] \wedge K[V] & = & K[U \cap V] \\ U \subseteq V & \leftrightarrow & K[U] \wedge K[V] = K[U] \qquad (U,V,W \subseteq G) \\ K[\langle U,V\rangle] & \geq & K[U] \vee K[V] \\ \langle U,V\rangle \subseteq W & \leftrightarrow & (K[U] \vee K[V]) \wedge K[W] = K[U] \vee K[V] \end{array}$$

4. Determination of the lattice V(G) of all subgroups of G [ ], [ ]

4.1. Fundamental princip for determining V(G)

4.1.1 Let ϕ^k be the set of all dual numbers with k digits, where $k = |E(G)|$, E(G) as in 3.1 .
Then for any dual number

$$(4.1) \qquad M(H) = \sum_{j=1}^{l} 2^{i_j - 1} \in \phi^k \quad (\{i_1,\ldots,i_l\} \subseteq \{1,\ldots,k\})$$

the corresponding subset $H = \{z_{i_1},\ldots,z_{i_l}\} \subseteq E(G)$ determines a subgroup $U := \langle H \rangle \subseteq G$ of G. It is obvious that different dual numbers $M(H), M(H') \in \phi^k$, $M(H) \neq M(H')$ may generate the same subgroup $\langle H \rangle = \langle H' \rangle$ of G.
Theoretically we obtain the set {U} of all subgroups $U \subseteq G$ of G in the following way:

4.1.2 Going forwards in the natural order of ϕ^k we seccessively determine the generating sets $\langle H \rangle =: U$ for all $M(H) \in \phi^k$. Then for every calculated U the generating system E(U) may be determined and the corresponding characteristic number K[U] - so far as different from the already listed - shall be stored in the list of characteristic numbers.

4.1.3 But this basic idea cannot be realized by the computer, because the number of dual numbers successively to be proved is 2^k, and the generating process of groups is a time-consuming procedure.
Therefore this considerations require the devolopment of a more effective method selecting only such dual numbers $M(H) \in \phi^k$, the corresponding subsets $\langle H \rangle$ of which in general are subgroups of G not yet generated.

4.2 Combinatorial method for the determination of V(G)

4.2.1 The filter method [6]

Starting with the dual number 0 and using the method mentioned in 4.1.2 we reach an uniquely determined dual number $F_1 := M(H^{(1)}) \in \phi^k$ - called a filter of ϕ^k - such that

$$\langle H^{(1)} \rangle = G, \quad \langle H' \rangle \neq G \quad \text{for all} \quad M(H') < M(H^{(1)}) .$$

By the filter F_1 the set $\psi[F_1] = \{M(H^{(j)}) \in \phi^k \,/\, M(H^{(j)}) \wedge F_1 = F_1\}$ is defined and $\psi[F_1]$ again defines a system

$$\sum[F_1] = \{\phi^{r_1}[F_1] \,/\, r_1 = 1, \ldots, |\psi[F_1]|\} \tag{4.2}$$

of ordered subsets $\psi^{r_1}[F_1]$ of ϕ^k, where $\psi^j[F_1]$ ($1 \leq j \leq |\psi[F_1]|$) consists of the 2^i-1 following dual numbers $M(H^{(\tau,j)})$ of the element $M(H^{(j)}) \in \psi[F_1]$ and where i is the exponent of the smallest power of 2 in F_1 being not 0. For all $M(H^{(\tau,j)})$ we get $\langle H^{(\tau,j)} \rangle = G$ and only a dual number $M(H) \in \Omega[F_1] :=$ $:= \phi^k \setminus \sum|F_1|$ can lead to a proper subgroup $U := \langle H \rangle \subset G$ of G. This, however, means that having determined F_1 the first dual number to be proved by the computer is $F_1 + 2^i$ lying in the number sequence $B[F_1]_1^2$ *) of all dual numbers between $\phi^1[F_1]$ and $\phi^2[F_1]$.

Proving $M(H^*) \in B[F_1]_1^2$ we obtain either:

(α) $M(H^*)$ determines a subgroup $U := \langle H^* \rangle$ of G, the characteristic number $K[U]$ of which is stored or not. If not, $K[U]$ must be stored and in both cases $M(H^*) + 1$ is the next dual number to be proved.

or:

(β) $M(H^*)$ determines $G = \langle H^* \rangle$.

If there does not exist a $M(H^*) \in B[F_1]_1^2$ such that $\langle H^* \rangle = G$, we reach the first dual nuber of $\phi^2[F_1]$ and by deleting all following 2^i-1 dual numbers, we are comming to the first dual number of $B[F_1]_2^3$ to be proved. But if we obtain $G = \langle H^* \rangle$ by a generating process, $F_2 := M(H^*)$ determines a new filter of ϕ^k.

Assuming now that we have already found j filters $F_1, \ldots, F_j$ of ϕ^k similar to the case of F_1 the filter F_j defines the set $\psi[F_j] = \{M(H^{(k)}) \in \phi^k \,/\, M(H^{(k)}) \wedge F_j = F_j\}$ and the set systems

*) Generally we denote in the following by $B[F_k]^{i+1}$ the set of all dual numbers between $\phi^i[F_k]$ and $\phi^{i+1}[F_k]$ ($1 \leq i$, $i^i+1 \leq r_k$ both defined by a filter F_k similar as for F_1.

$\Sigma[F_j]$ and $\Omega[F_j]$. The system $\Sigma[F_j]$ consists of the dual number sequences $\phi^{r_j}[F_j]$ $(r_j = 1,\ldots,|\psi[F_j]|)$, the elements of which are the 2^i-1 following dual numbers $M(H^{(r_j,\tau)})$ $(\tau = 1,\ldots,2^i-1)$ of the element $M(H^{(r_j)})$ of $\psi[F_j]$ and where i is determined by F_j.

If F_j has been constructed, only the $M(H^*) \in B[F_j]_i^{i+1}$ $(i = 1,\ldots,|\psi[F_j]|-1)$ must be proved:

(α') If $\langle H^*\rangle =: U \subseteq G$, we store $K[U]$ if $K[U] \neq K[U^*]$ for all $K[U^*]$ already been stored.

(β') If $M(H^*) \wedge F_t = F_t$ for $0 < t < j$, we get $\langle H^*\rangle = G$ and $M(H^*) + 2^i$ is the next dual number of ϕ^k to prove by the computer, where i is the exponent of the smallest power of 2 of F_t being not 0.

(γ') If $\langle H^*\rangle = G$ by a generating process, $F_{j+1} := M(H^*)$ of ϕ^k is a new filter of ϕ^k.

In the case that neither (β') nor (γ') is valid for $M(H^*) \in B[F_j]_i^{i+1}$, we are comming to the first dual number of $\phi^{i+1}[F_j]$ and using F_j to the first dual number of $B[F_j]_{i+1}^{i+2}$, which must be proved.

4.2.2 The algorithm of filters can be completed by introducing "filters of maximal subgroups" and "filter sequences". Using these supplementary conceptions developed in detail in [6] the program of determining V(G) can seccessfully be applied to finite groups G with relatively small order $|G|$ and less complicated lattice structure.

Therefore, it seems to be profitable to supplement the program by an additional "algorithm of composition" [11] described briefly in the following section.

4.2.3 The basic concepts of the algorithm of composition [11]

Generating G successively by $a_1,\dots,a_n$ we obtain a chain $\langle e\rangle = G_0 \subset G_1 \subset \dots \subset G_n = G$ of subgroups $G_i = \langle a_1,\dots,a_i\rangle$ $(i=1,\dots,n)$ of G. The generating systems $E(G_i)$ (see 3.1) may satisfy:

$$E(G_i) \cap E(G_k) = E(G_i) \quad (k \geq i,\ i,k = 1,\dots,n) .$$

Dividing the elements of $E(G_n)$ into sections C_i $(i=1,\dots,s)$ of length $1 \leq |E(G_n)|$ and one further section C_{s+1} of length r ($|E(G_n)| = s\cdot l+r$, $r < l$, $C_{s+1} = \emptyset$ if $r = 0$), the filter method described in 4.2.1 can be applied on each C_i obtaining a set T_i of subgroups of G. Any two of these T_i will not necessarily be disjoint, but by eleminating those corresponding characteristic numbers, we obtain the disjoint sets T_i^*. But in general $\bigcup_i T_i^*$ is not yet the wanted set {U} of all subgroups $U \leq G$.
We make the following definitions:
The determination of $K[H]$, $H = \langle U,V\rangle$, by $K[U]$ and $K[V]$ is called "composition" and $K[H]$ will also denoted by $K[K[U], K[V]]$.

A set $\mathfrak{C}$ of characteristic numbers is said to be closed by composition, if $K[K_1,K_2] \in \mathfrak{C}$ for arbitrary elements of $K_1,K_2 \in \mathfrak{C}$ and $C(\mathfrak{C})$ is called the closure of $\mathfrak{C}$.

We denote by:

$$E_i = \{K[U] / U \in T_i^*\}$$

$$E_{1,\dots,i} = C(E_1 \cup \dots \cup E_i)$$

$$D_{1,\dots,i} = E_{1,\dots,i} \setminus (E_1 \cup \dots \cup E_i) \quad , \quad (i = 1,\dots,s+1)$$

$$D_i = \{K[K_1,K_2] \notin E_i \cup E_{1,\dots,i-1} / K_1 \in E_i,\ K_2 \in E_{1,\dots,i-1}\}$$

Then clearly we obtain:

$$K\left[K[K_1,K_2], K[K_1',K_2']\right] = K\left[K[K_1,K_1'], K[K_2,K_2']\right] \tag{4.3}$$

$$E_i = C(E_i) \quad (i = 1,\dots,s+1) \tag{4.4}$$

By (4.3) and (4.4) we easily get for the elements of D_i:

If $K_\lambda \in D_i$ $(\lambda = 1,2 \; ; \; 2 \leq i \leq s+1)$, then there always exists $K_1^* \in E_i$ and $K_2^* \in E_{1,\ldots,i-1}$ such that $K[\bar{K}_1, K_2] = K[\bar{K}_1^*, K_2^*]$.

From this result it follows immediately

$$(4.5) \qquad C(E_1 \cup \ldots \cup E_i) = D_i \cup E_i \cup E_{1,\ldots,i-1} \quad (i=2,\ldots,s+1)$$

and by (4.5) we obtain an inductive algorithm for determining the set of all subgroups of G:

In the first step we have $E_1 = C(E_1)$. Suppose $C(E_1 \cup \ldots \cup E_i) = D_{1,\ldots,i} \cup E_1 \cup \ldots \cup E_i$ has already been determined. Then by successive composition of all $K \in E_{i+1}$, $K \notin D_{1,\ldots,i}$ with all $K' \in E_{1,\ldots,i}$ we get the closure $C(E_1 \cup \ldots \cup E_{i+1})$ This method must be repeated until finally we obtain $C(E_1 \cup \ldots \cup E_{s+1})$.

4.3 Output of the program for determining V(G)

4.3.1 Operating on the list of characteristic numbers by using a special sorting program and going downwards from G to <e> by determining the respective layer of maximal subgroups we get the following output of the program system:

A) Table of all subgroups of G devided in conjugation series and represented in the form of abstract generators and defining relations

B) Lattic V(G) in a special number code

4.3.2 Using special properties of group theory additionaly we obtain:

C) List of normalizators and centralizators of all subgroups of G

D) List of charachteristic subgroups of G and characteristic series: Centrum, Frattini group, Fitting group, commutator group, descending central series, commutator series, Ω- and $\mho$-series a.o..

5. Determination of the automorphism group Aut G of G [5], [7], [4], [1]

5.1 Range of the program system

5.1.1 Hall systems of a finite group G [1], [7]

The determination of Aut G by the program described in this section is possible, if the finite group G contains a system $\mathfrak{H} := \{H_1,\dots,H_r\}$ of subgroups H_i (i=1,...,r) of G - called a Hall system of G - such that the following conditions are satisfied:

(5.1)
a) $G = H_1 \cdot \dots \cdot H_r$
$H_i H_k = H_k H_i \qquad (i,k = 1,\dots,r;\ i \neq k)$
$(|H_i|, |H_k|) = 1$

b) Every two Hall systems of G are conjugate in G.

5.1.2 Sylow basis of a solvable group G [8]

If G is a finite solvable group with $|G| = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$, it is well known that G contains a complete Sylow system $P_1,\dots,P_r$ of p_i-Sylow subgroups of G (i=1,...,r) - called a Sylow basis of G - satisfying (5.1). Having constructed the lattice V(G) of G the computational determination of a Sylow basis $P_1,\dots,P_r$ easily follows from the determination of the p_i-Sylow complements $K_1,\dots,K_r$ of G, $|K_i| = \prod_{\substack{j=1 \\ j\neq i}}^{r} p^{\alpha_j}$, and the corresponding characteristic numbers $K[K_i]$ (i=1,...,r).

Since $P_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{r} K_i$ (i=1,...,r) defines a Sylow basis of G, we obtain:

(5.2) $$P_i \leftrightarrow K[P_i] = \bigwedge_{\substack{j=1 \\ j\neq i}}^{r} K[K_i] \qquad (i=1,\dots,r)$$

5.1.3 Groups containing a chain of normal Hall groups [7]

If there exists a chain of normal Hall groups for G, i.e. a chain $G = G_r \supset \dots \supset G_1 \supset G_0 = \langle e \rangle$ with $G_i \lhd G$, $(|G_i|, [G : G_i]) = 1$ (i=1,...,r), then G always contains a Hall system $H_1,\dots,H_r$ satisfying (5.1) ([7], Theorem 2.1). Beyond that it can be proved that if k is the only index with G_k/G_{k-1} not solvable; for every $i \neq k$ there exists a Sylow basis $P_{i_1},\dots,P_{i,n_i}$ of H_i such that

(5.3) $P_{1,1},\ldots,P_{1,n_1},\ldots,P_{k-1,1},\ldots,P_{k-1,n_{k-1}},H_k,P_{k+1,1},\ldots,P_{k+1,n_{k+1}},\ldots$
$\ldots,P_{r,1},\ldots,P_{r,n_r}$

is a "complete Hall system" of G satisfying (5.1) ([7], Theorem 4.1).

Considering the proof of [7], Theorem 4.1 it is possible to determin a complete Hall system (5.3) of G if V(G) is constructed.

5.2 Decomposition of Aut G of a finite group G containing a Hall system [7]

5.2.1 Let $G = H_1 \cdot \ldots \cdot H_r$ be a factorization of G by a Hall system $\mathfrak{H} := \{H_1,\ldots,H_r\}$. If $A \subseteq \mathrm{Aut}\ G$, $H \subseteq G$ we denote by:

$T_A(H) = \{\gamma \in A \mid \gamma H = H\}$ the fix group of H related to A

$N_G(H)$ the normalizer of H in G

$F(\mathfrak{H}) = \bigcap_{i=1}^{r} N_G(H_i)$ the system normalizer of $\mathfrak{H}$ in G

$\Gamma(\mathfrak{H}) = \bigcap_{i=1}^{r} T_{\mathrm{Aut}\ G}(H_i)$ the fixgroup of $\mathfrak{H}$

$\tau(g)$ the inner automorphism of G induced by $g \in G$

According to these definitions we obtain the following fundamental result of the decomposition of Aut G:

If $G = F(\mathfrak{H})g_1 + \ldots + F(\mathfrak{H})g_s$, then $\mathrm{Aut}\ G = \tau(g_1)\Gamma(\mathfrak{H}) + \ldots + \tau(g_s)\Gamma(\mathfrak{H})$

$$|\mathrm{Aut}\ G| = |\Gamma(\mathfrak{H})| \cdot [G:F(\mathfrak{H})] \ .$$

5.2.2 By this decomposition of Aut G it is obvious that every $\gamma \in \mathrm{Aut}\ G$ can be represented as a product $\tau(g_i)\circ\gamma_1$ of an element $\gamma_1 \in \Gamma(\mathfrak{H})$ and a special inner automorphism $\tau(g_i)$ of G. Therefore the determination of $\Gamma(\mathfrak{H})$ plays the fundamental role in the development of the program system.

5.3 Characteristic mappings and special subgroups of a factorization of G [1], [5]

5.3.1 Characteristic mappings

Let $G = H_1 \cdot H_2 = H_2 \cdot H_1$, $H_1 \cap H_2 = \langle e \rangle$ be a factorization of G by H_1, H_2. Then to every $h_i \in H_i$ (i=1,2) there corresponds a map $h_i k : H_k \to H_k$ defined by:

$$(5.4) \qquad h_1 {}^{2}h_2 = H_1 h_1 h_2 \cap H_1 \quad \text{for all } h_2 \in H_2$$

$$h_2 {}^{1}h_1 = h_2 h_1 H_2 \cap H_1 \quad \text{for all } h_1 \in H_1$$

It is easy to verify that these mappings are equivalent with

$$(5.5) \qquad h_1 \cdot h_2 = h_2 {}^{1}h_1 \cdot h_1 {}^{2}h_2$$

and by (5.5) multiplication in G is completely determined. Therefore, the mappings $h_i k$ (i=1,2) together with the defining relations of the components H_i(i=1,2) of G determine the structure of G. From the theory of factorization we get further that the mappings $h_i k$ form a permutation subgroup of the symmetric group $S_{|H_k|}$ of degree $|H_k|$.

5.3.2 Special subgroups of the factorizated group G [5]

There exists a homomorphism $\tau_{i,k} : H_i \to \Pi_{i,k}$ of H_i onto $\Pi_{i,k}$ with cernel

$$(5.6) \qquad N_i = \{h_i \in H_i \;/\; h_i k h_k = h_k \text{ for all } h_k \in H_k\} .$$

N_i is the maximal normal subgroup of G contained in H_i (i=1,2). An other group important for the determination of Aut G is the fix group F_i of $\Pi_{k,i}$:

$$(5.7) \qquad F_i = \{h_i \in H_i \;/\; h_k i h_i = h_i \text{ for all } h_k \in H_k\} ,$$

which can be represented by

$$(5.8) \qquad F_i = N_G(H_k) \cap H_i \quad (i,k=1,2;\ i \neq k) .$$

If $G = H_1 \cdot \ldots \cdot H_r$, then according to these investigations for every subgroup $G_{i,k} := H_i H_k = H_k H_i$ (i,k=1,...,r, i≠k) we can form the groups $\Pi_{i,k}, N_i^k, F_i^k$, the determination of which may be described in the following section.

5.4 Computational determination of $\Pi_{i,k}, F_i^k, N_i^k$

5.4.1 Determination of Π_{ik}

The elements of the components H_i $(i=1,\ldots,r)$ of $G = H_1 \cdot \ldots \cdot H_r$ may be numbered in the same sequence as they are generated by the generating program of H. Then, generating the subgroups $G_{i,k} = H_i H_k = H_k H_i$ $(i,k = 1,\ldots,r;\ i \neq K)$ on the one hand as a product of H_i, H_k on the other hand as a product of $H_k H_i$ we obtain by comparing the products:

$$(5.9)\quad h_i^{(1)} h_k^{(s)} = h_k^{(s_\nu)} h_i^{(1_\rho)} = h_i^{(1)}{}_k\, h_k^{(s)} \cdot h_k^{(s)}{}_i\, h_i^{(1)} \qquad \begin{bmatrix} (s=1,\ldots,|H_k|) \\ (1 \leq l \leq |H_i|) \end{bmatrix}.$$

From these relations we obtain the permutation $h_i^{(1)}{}_k$ of H_k related to the element $h_i^{(1)} \in H_i$: $h_i^{(1)} \to h_i^{(1)}{}_K = \begin{pmatrix} s \\ s_\nu \end{pmatrix}$ If l runs from 1 to $|H_i|$ we get $\Pi_{i,k}$. Fixing s $(1 \leq s \leq |H_k|)$ we similary can determine for variable l $(l = 1,\ldots,|H_i|)$ the permutation $h_k^{(s)}{}_i = \begin{pmatrix} l \\ l_\rho \end{pmatrix}$ related to $h_k^{(s)} \in H_k$ and if s runs from 1 to $|H_k|$ we get $\Pi_{k,i}$.

5.4.2 Determination of F_i^k and N_i^k

$E(H_i)$ may be defined as in 3.1 . Then by (5.8) resp. by the result after (5.6) F_i^k resp. N_i^k can be determined by a generating process:

$F_i^k = \langle z_i \rangle$ with $z_i \in E(H_i)$, $z_i z_k z_i^{-1} \in H_k$ for all $z_k \in E(H_k)$

$N_i^k = \langle z_i \rangle$ with $z_i \in E(H_i)$, $z_k z_i z_k^{-1} \in H_i$ for all $z_k \in E(H_k)$.

5.5 Determination of $\Gamma(\mathfrak{K})$

5.5.1 The monomorphism of $\Gamma(\mathfrak{K})$ in Aut $H_1 \times \ldots \times$ Aut H_r

For $\gamma \in \Gamma(\mathfrak{K})$ let $\gamma_{|H_i} \in$ Aut H_i be the automorphism of H_i obtained by the restriction of γ on H_i and A_i the group containing all $\gamma_{|H_i}$.
Then the map $\zeta_i : \Gamma(\mathfrak{K}) \to A_i$ defined by $\gamma \to \alpha_i := \gamma_{|H_i}$ defines a homomorphism of $\Gamma(\mathfrak{K})$ onto A_i, and it can easily be shown that

$$(5.7)\quad \begin{aligned} \zeta : \Gamma(\mathfrak{K}) &\to \Pi := \text{Aut } H_i \times \ldots \times \text{Aut } H_r \\ \gamma &\to \alpha := (\alpha_1,\ldots,\alpha_r)\ ;\ \alpha_i = \zeta_i \gamma \end{aligned}$$

is a monomorphism of $\Gamma(\mathfrak{K})$ in the direct product Aut $H_1 \times \ldots \times$ Aut H_r.

5.5.2

Necessary and sufficient conditions for $\alpha \in \Pi$ to be an automorphism of G [5]

Let be $\alpha = (\alpha_1,\ldots,\alpha_r) \in \Pi$, $\alpha_i \in$ Aut H_i. Then α is an automorphism of G, if and only if for all $h_i \in H_i$ and all $i,k = 1,\ldots,r$; $i \neq k$ the following relations applied on all $h_k \in H$ are satisfied:

$$\alpha_k \circ h_i^{k} \circ \alpha_k^{-1} = (\alpha_i h_i)^k \tag{5.8}$$

The relations (5.8), however, are valid if and only if they are valid for all elements $h_i^{(\rho)}$ of a generating system $\{h_i^{\rho}\}$ of H_i applied on all elements $h_k \in H_k$.

Further, because $\alpha_i F_i^k = F_i^k$ and $\alpha_i N_i^k = N_i^k$ $(i,k = 1,\ldots,r;\ i \neq k)$ with $\gamma \in \Gamma(\mathfrak{K})$, $\zeta(\gamma) = (\alpha_1,\ldots,\alpha_r)$, $\alpha_i \in$ Aut H_i, it follows that only such automorphisms $\alpha_i \in$ Aut H_i $(i = 1,\ldots,r)$ can lead to an automorphism γ of G which are elements of

$$A_i^* := \bigcap_{\substack{k=1 \\ k\neq i}}^{r} \left(T_{\text{Aut } H_i}(F_i^k) \cap T_{\text{Aut } H_i}(N_i^k) \right). \tag{5.9}$$

Before we describe the computational determination of the automorphism group A_i^*, $A_i \subseteq A_i^* \subseteq$ Aut H_i, we shall give an algorithm for determining $\Gamma(\mathfrak{K})$ in the following section.

5.5.3

Construction of $\Gamma(\mathfrak{K})$ by composition of allowable automorphisms of the A_i^* [4], [7]

Let G_1, G_2, K be finite groups and $\mu_i : G_i \to K$ $(i_1 = 1,2)$ epimorphisms of G_i on K, then $G_1 \underset{K}{\times} G_2 := \{(g_1,g_2) \mid g_i \in G_i,\ \mu_1 g_1 = \mu_2 g_2\}$ forms a subgroup of $G_1 \times G_2$, called the direct product of G_1, G_2 with united factor group K.

From [7] it follows:

If $G = U_1 \cdot U_2$, $U_1 \cap U_2 = \langle e \rangle$, $A_G \subseteq$ Aut G, $\Gamma_o = T_{A_G}(U_1) \cap T_{A_G}(U_2)$ and if $\zeta_o : \Gamma_o \to$ $\to$ Aut $U_1 \times$ Aut U_2 is defined by $\zeta_o \gamma = (\alpha_1,\alpha_2)$, $\gamma \in \Gamma_o$, $\alpha_i = \zeta_i \gamma = \gamma_{|U_i}$, $\alpha_i \in A_i := \Gamma_{o|U_i}$ $(i = 1,2)$, then

$$A := \zeta_o \Gamma = A_1 \underset{K}{\times} A_2 = \{(\alpha_1,\alpha_2) \mid \alpha_i \in A_i,\ \mu_1 \alpha_1 = \mu_2 \alpha_2\}$$

with $\mu_i : A_i \to K := A/Y$, cern $\mu_i = Y_i$ $(i = 1,2)$ and where $Y = Y_1 \times Y_2$ is the maximal normal subgroup of A, which can be represented as a direct product of the components $Y_i \in A_i$.

Using these results we can give an inductive algorithm for determining $\Gamma(\mathfrak{H})$ by composition of allowable automorphisms of A_i^*, $A_i \subseteq A_i^* \subseteq \mathrm{Aut}\, H_i$ $(i = 1,\ldots,r)$:

If $G = H_1 \cdot \ldots \cdot H_r$ is a factorization of G by the Hall system $\mathfrak{H} = \{H_1,\ldots,H_r\}$ it is obvious that $\mathfrak{H}_k := \{H_1,\ldots,H_k\}$ is a Hall system for $G_k := H_1 \cdot \ldots \cdot H_k$, and $\Gamma(\mathfrak{H}_k)$ is isomorphic with a subgroup $S_k \subseteq \mathrm{Aut}\, H_1 \times \ldots \times \mathrm{Aut}\, H_k$.

If we set $A^{(k)} := S_k \cap (A_1^* \times \ldots \times A_k^*)$, $A^{(1)} := A_1^*$ the group $A^{(r)} \cong \Gamma(\mathfrak{H})$ can inductively be determined in (r-1)-steps by calculating the groups $A^{(k)}$ from $A^{(k-1)}$ and A_k^* $(k = 2,\ldots,r)$.

Using the results mentioned above by setting $U_1 := G_{k-1}$, $U_2 := H_k$ we get $Y_1 = \{(\alpha_1,\ldots,\alpha_{k-1}) \in A^{(k-1)}/(\alpha_1,\ldots,\alpha_{k-1},\varepsilon_k) \in A^k$, $\varepsilon_k = \mathrm{id}|_{H_k}\}$, $Y_2 = \{\alpha_k \in A_k^* / (\varepsilon_1,\ldots,\varepsilon_k,\alpha_k) \in A^{(k)}$, $\varepsilon_i = \mathrm{id}_{H_i}$ $(i = 1,\ldots,k)\}$ and the computational test is given by proving a system of much simpler relations than (5.8):

$$(5.9)\quad (\alpha_1,\ldots,\alpha_{k-1}) \in Y_1 \leftrightarrow \alpha_j \circ h_k j \circ \alpha_j^{-1} = h_k j \qquad (j = 1,\ldots,k-1)$$
$$h_j k = (\alpha_j h_j)k$$

for all $h_k \in H_k$, $h_j \in H_j$ applied to all $h_j \in H_j$, $h_k \in H_k$, respectively.

$$(5.10)\quad \alpha_k \in Y_2 \leftrightarrow \alpha_k \circ h_j k \circ \alpha_k^{-1} = h_j k \qquad (j = 1,\ldots,k-1)$$
$$h_k j = (\alpha_k h_k)j$$

for all $h_j \in H_j$, $h_k \in H_k$ applied to all $h_k \in H_k$, $h_j \in H_j$, respectively.

If C_i is the automorphism group obtained by the restriction of the wanted group $A^{(k)}$ on U_i $(i = 1,2)$ and if $K := A^{(k)}/Y$, $Y = Y_1 \times Y_2$ it follows $A^{(k)} = C_1 \overset{\cdot}{\times}_K C_2$.

A representative $\beta := (\alpha_1,\ldots,\alpha_{k-1})$ of the decomposition of $A^{(k-1)}$ by Y_1 can be composed with a representative α_k of the decomposition of A_k^* by Y_2 to an element $(\alpha_1,\ldots,\alpha_{k-1},\alpha_k) \in A^{(k)}$, if and only if all pairs (α_i,α_k) $(i = 1,\ldots,k-1)$ satisfy the relations (5.8). Since $K \simeq C_{i/Y_i}$ $(i=1.2)$, we get for every representative β at most one representative α_k, which can be composed to $(\beta,\alpha_k) \in A^{(k)}$. Therefore, if $(\beta,\alpha_k) \in A^{(k)}$, then $(\beta\bar{\beta}, \alpha_k\bar{\alpha}_k) \in A^{(k)}$ with $\bar{\beta} = (\bar{\alpha}_1,\ldots,\bar{\alpha}_{k-1}) \in Y_1$ and $\bar{\alpha}_k \in Y_2$.

5.6. Determination of A^* [2], [4]

The method briefly described in the following has been developped in [2] and used for a Sylow basis of solvable groups in [4].

5.6.1 Homotypic and isotypic sets

Let A^* be the automorphism group defined by (5.9) for any group $H \in \mathfrak{H}$ of the Hall system $\mathfrak{H}$ of G.

If $\mathfrak{A} = \{a_1,\ldots,a_n\}$ is a generating system of H satisfying the defining relations $R_1(\mathfrak{A}) = \ldots = R_s(\mathfrak{A}) = e$, then a 1-1-mapping $\alpha : H \to H$ is an automorphism of H if and only if $H = \langle \alpha a_1,\ldots,\alpha a_n\rangle$ and $R_j(\alpha\mathfrak{A}) = e$ $(j=1,\ldots,s)$. The group A^* we want to construct determines a subset $I(h) = \{\alpha h/\alpha \in A^*\}$ of H, for every $h \in H$ and it is obvious that by the sets I(h) the set of elements of H is devided in disjoint classes.

The fundamental idea of the developped method is to determine for every $h \in H$ a subset $S(h) \subseteq H$ as small as possible such that $I(h) \subseteq S(h)$; $h_1 \in S(h) \to$ $\to S(h_1) = S(h_2)$.

Two elements $h_1,h_2 \in H$ are called "isotypic", if $I(h_1) = I(h_2)$, "homotypic", if $S(h_1) = S(h_2)$. Two subgroups U,V of H are called isotypic, homotypic, if the elements $\{u_i\},\{v_i\}$ $(i = 1,\ldots,r)$ of U,V can be ordered totally $\{u_{i_1},\ldots,u_{i_r}\}$, $\{v_{i_1},\ldots,v_{i_r}\}$ such that $I(u_{i_k}) = I(v_{i_k})$, $S(U_{i_k}) = S(v_{i_k})$ $(k = 1,\ldots,r)$, respectively.

Then it is evident that every system $\mathfrak{b}' = \alpha\mathfrak{b}$, $b_i' = \alpha b_i$ $(i = 1,\ldots,m)$, $\alpha \in A^*$

of a minimal generating systems $\mathfrak{b} = \{b_1,\ldots,b_m\}$ of H can be found among the systems $\mathfrak{b}' = \{b_1',\ldots,b_m'\}$ with $b_i' = S(b_i)$. These generating systems are also called homotypic.

5.6.2 The correspondence $h \to S(h)$, $h \in H$

The correspondence $h \to S(h)$, $h \in H$ can be obtained by using a decomposition of the lattice V(H) of H in disjoint classes developped by the method [3].

The group A^* induces an equivalence relation r_{A^*} on V(H) satisfying:

(5.11)

a) $U\, r_{A^*}\, V \Longrightarrow |U| = |V|$

b) $U\, r_{A^*}\, V \Longrightarrow$ U and V contain (are contained) the same number (in the same number) of subgroups of any class of r_{A^*}.

c) $U\, r_{A^*}\, V \wedge$ U cyclic, abelian, normal $\Longrightarrow$ V cyclic, abelian, normal, respectively.

d) Fix groups U rel. A^* generate classes consisting of only one element.

It can be verfied that to every equivalence relation r on V(H) there corresponds an uniquely defined equivalence relation $\eta(r)$, which is the supremum of all relations $r^* \leq r$ *) satisfying (5.11) a,b) ([3], [4]).

Further, if r_o is the coarsest relation on V(H) satisfying (5.11),a),c),d) then $h_1, h_2 \in H$; $U,V \in V(H)$ are homotypic if and only if $\langle h_1 \rangle\, \eta(r_o)\, \langle h_2 \rangle$, $U\, \eta(r_o) V$, respectively. Then it is possible to develop an algorithm for

---

*) $r_1 \leq r_2 \Longleftrightarrow U r_1 V \Longrightarrow U\, r_2\, V$ for all $U,V \in V(H)$. By the relation $\leq$ the system of all equivalence relations on V(H) forms a lattice, if infimum and supremum of r_1, r_2 are defined by:

$$U\,(r_1 \wedge r_2)\, V \Longleftrightarrow U r_1 V \vee U r_2 V$$

$U\,(r_1 \vee r_2)\, V \Longleftrightarrow$ There exists a chain $U = U_1,\ldots,U_n = V$ of subgroupf of H such that $U_i r_1 U_{i+1} \wedge U_i r_2 U_{i+1}$ $(i = 1,\ldots,n-1)$

constructing $\eta(r_o)$ starting with an equivalence relation $\bar{r}$ satisfying (5.11),a). In case of a Sylow basis for a solvable group G see [4].

If d(h) is the number of homotypic elements of h in H, then for any system $f = \{h_1,\ldots h_n\}$ of elements of H the number d(f) of homotypic systems of f in H is given by $d(f) = \prod_{i=1}^{n} d(h_i)$.

5.6.3 Optimal generating systems

There exists an algorithm [3] to determine an "optimal" generating system for H, i.e. a generating system $\mathfrak{b} = \{b_1,\ldots b_m\}$ such that d(b) is minimal. Optimal generating systems of H are minimal systems, but in general optimal generating systems are not appropriate generating systems of H for multiplication and generating procedures. Practically this means that beside an optimal generating system $\mathfrak{b} = \{b_1,\ldots b_m\}$ we use a situable generating system $\mathfrak{a} = \{a_1,\ldots,a_n\}$ of H with defining relations $R_s(\mathfrak{a}) = e$.

If we know a representation of the elements of $\mathfrak{a}$ as words in the b's and conversely: $\mathfrak{a} = V(b)$, $\mathfrak{b} = W(\mathfrak{a})$, then we can prove the homotypy of a system $\mathfrak{b}'$ in the following way.

If $\langle\mathfrak{b}'\rangle = H$, $\mathfrak{a}' = V(\mathfrak{b}')$, $\mathfrak{b}'' = W(\mathfrak{a}') = \mathfrak{b}'$, $R(\mathfrak{a}') = e$, then there exists an automorphism $\alpha \in \mathrm{Aut}\, H$ such that $\mathfrak{b}' = \alpha\mathfrak{b}$. For if $R(\mathfrak{a}') = e$, then $\alpha : \mathfrak{a} \to \mathfrak{a}'$ defines an endomorphism of H in H. Since $\mathfrak{b}'' = W(\mathfrak{a}') = W(\alpha\mathfrak{a}) = \alpha W(\mathfrak{a}) = \alpha\mathfrak{b}$ and $\mathfrak{b}'' = \mathfrak{b}'$ it follows $\mathfrak{b}' = \alpha\mathfrak{b}$ and according to $\langle\mathfrak{b}'\rangle = H$ α is an automorphism.

If H: = P is a p-Sylow subgroup of a solvable group, in [4] is deduced that if $\mathfrak{b} = \{b_1,\ldots b_m\}$ is a optimal generating system of P and if $\mathfrak{c} = \{c_1,\ldots,c_s\}$ is a special generating system of the commutator subgroup P', then the system $\mathfrak{a} = \mathfrak{b}\cup\mathfrak{c} = \{c_1,\ldots c_s, b_1,\ldots b_m\}$ is a special generating system of P.

5.7 Representation of automorphisms in the computer

5.7.1 Representation of automorphisms as permutations

Let $\mathfrak{b} = \{b_1,\ldots,b_m\}$ be an optimal generating system of H with a minimal number $d(\mathfrak{b})$ of homotypic systems and $M: = \bigcup_{i=1}^{m} S(b_i)$, then the complex $M = \{h_1; = b_1,\ldots,h_m: = b_m, h_{m+1}\ldots h_{m+t}\}$ is A^*-invariant. If $\alpha \in A^*$, then $\Pi(\alpha)$ may denote the permutation induced by α on M:

$\Pi(\alpha) = \begin{pmatrix} h_i \\ \alpha h_i \end{pmatrix} = \begin{pmatrix} h_i \\ h_{i_k} \end{pmatrix}$ ($i = 1,\ldots, m+t$). Since $b \subseteq M$, it follows immediately that A^* is isomorphic to the permutation group on M induced by A^*. By this permutation group A^* is represented in the computer.

5.7.2 Representation of automorphisms of $\Gamma(\mathfrak{K})$

The fix group $\Gamma(\mathfrak{K})$ is isomorphic to a subgroup of $D = A_1^* \times \ldots \times A_r^*$. If $\zeta : \gamma \to \alpha = (\alpha_1,\ldots,\alpha_r)$ is the homomorphism of $\Gamma(H)$ in D, the automorphism $\gamma \in \Gamma(\mathfrak{K})$ shall be represented by $\zeta(\gamma) = (\alpha_1,\ldots,\alpha_r)$. Multiplying $\gamma_1, \gamma_2 \in \Gamma$ the images $\zeta(\gamma_1)$ and $\zeta(\gamma_2)$ must multiplied componentwise. Using the representation as permutations for the components finally it is possible to represent the elements of A_i^* uniquely as normal words in abstract generators with defining relations. This importantly accelerates the process of multiplication for elements of $\Gamma(\mathfrak{K})$.

REFERENCES

[1] ALTMANN, E.:
Anwendung der Theorie der Faktorisierungen,
Forschungsbericht des Landes Nordrhein-Westfalen, No. 1902,(1968)

[2] FELSCH, V.:
Ein Programm zur Berechnung des Untergruppenverbandes und der Automorphismengruppe einer endlichen Gruppe, Diplomarbeit,
Kiel (1963)

[3] FELSCH, V. u. NEUBÜSER, J.:
Über ein Programm zur Berechnung der Automorphismengruppe einer endlichen Gruppe,
Num. Math. 11, 277-292, (1968)

[4] GELLER, E.:
Ein Programm zur Bestimmung der Automorphismengruppen endlicher auflösbarer Gruppen,
Berichte der Gesellschaft für Mathematik und Datenverarbeitung,
Bonn, 51, (1971)

[5] GERHARDS, L. u. ALTMANN, E.:
A computational method for determining the automorphism group of a finite solvable group,
(Proc. Conf. on Comp. Algebra, Oxford, Aug. 1967)
Pergamon Press, New York, 61-74, (1969)

[6] GERHARDS, L. u. LINDENBERG, W.:
Ein Verfahren zur Berechnung des vollständigen Untergruppenverbandes endlicher Gruppen auf Dualmaschinen,
Num. Math. 7, 1-10, (1965)

[7] GERHARDS, L.:
On the construction of the automorphism group of a finite group, will be published in Cahiers Mathématiques, Montpellier

[8] HALL, P.:
On the Sylow systems of a solvable group,
Proc. London Math, Soc. (2) 43, 316-323, (1937)

[9] JÜRGENSEN, H.:
Calculation with the elements of a finite group given by generators and defining relations,
(Proc. Conf. on Comput. Algebra, Oxford, Aug. 1967)
Pergamon, New York, 47-57, (1969)

[10] LINDENBERG, W.:
Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten,
Num. Math. 4, 151-153, (1962)

[11] LINDENBERG, W. and GERHARDS, L.:
Combinatorial construction by computer of the set of all subgroups of a finite group by composition of partial sets of its subgroups,
(Proc. Conf. on Comput. Algebra, Oxford, Aug. 1967)
Pergamon, New York, 75-82, (1969)

[12] NEUBÜSER, J.:
Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine,
Num. Math. 2, 280-292, (1960)

[13] REDEI, L.:
Die Anwendungen des schiefen Produktes in der Gruppentheorie,
J. reine u. angew. Math. 188, 201-228, (1950)

[14] REDEI, L.:
Zur Theorie der faktorisierbaren Gruppen,
Acta Math., Sci. Hung. 1, 74-98, (1950)

Leonhard GERHARDS
Gesellschaft für Mathematik
und Daten verarbeitung
M.B.H. BONN
5205 St-Augustin 1
Postfach 1240 R.F.A.