LEONHARD GERHARDS

Group-theoretical investigations on computers II

Astérisque, tome 38-39 (1976), p. 91-103
<http://www.numdam.org/item?id=AST_1976__38-39__91_0>

Société Mathématique de France
Astérisque 38-39 (1976) p.91-103

GROUP-THEORETICAL INVESTIGATIONS ON COMPUTERS II

by
Leonhard Gerhards

For solving group-theoretical problems often the structure of the maximal subgroups of a finite group G is of great importance. Although it is possible to determine the maximal subgroups of G by calculating the complete lattice V(G) of all subgroups of G [4], [10], it seems to be profitable to develop an effective computational algorithm for determining only the maximal subgroups of G.

Making use of theoretical results of a paper of E. Altmann [0] the present paper – mainly written under computational aspects – contains a complete description of the principal methods of such a program for a finite group G containing a „Hall system $\{H_i \,/\, i \in I\}$" of subgroups H_i if G [0], [5] .

The underlying group classes for the program are the class of finite solvable groups and the class of finite non solvable groups, which contain a chain of normal Hall groups [5].

In both cases the computational methods are based on results of the theory of factorizations of finite groups [1], [3]:

If G can be factorizated by the groups H_i of a Hall system $\{H_i \,/\, i \in I\}$ of G and if for any subgroup U of G there exists a conjugate group U^* such that U^* is a factorization by the subgroups $U^* \cap H_i$ of H_i, then assuming the computational construction of the lattice $V(H_i)$ of all subgroups of H_i the lattice V(G) of G can be determined by an iterative process constructing the maximal subgroups of maximal subgroups and their corresponding conjugate series.

The present paper consists of two central parts:

In section 1 we develop an effective algorithm for the determination of the maximal subgroups of a finite group G in the following cases:

a) G is solvable
b) G is non-solvable but contains a chain of normal subgroups.

In section 2 the algorithm will be exended to the calculation of the complete lattice V(G) of all subgroups of G.

1. Determination of the maximal subgroups of a finite group G factorizated by a Hall system

1.1 Preliminaries

1.1.1 Representation and multiplication of the elements of a finite group G

In the following any finite group G will be given abstractly by

a) a system $\mathfrak{A} = \{a_1, \dots, a_n\}$ of generating elements of G
b) a system $R_1(\mathfrak{a}) = e, \dots, R_t(\mathfrak{a}) = e$ of defining relations.

If any element $a \in G$ can be represented uniquely by a „normal form" $a = a_1^{r_1} \cdot \ldots \cdot a_n^{r_n}$ $(0 \leq r_i < |a_i|,\ a_i^0 = e)$ we get a representation $\varphi(a)$ of $a \in G$ in form of the n-tupel $<r_1, \ldots, r_n>$. Assuming further that $\varphi(a_i a_j)$ can be calculated uniquely from $\varphi(a_i)$ and $\varphi(a_j)$ for all pairs $\{a_i, a_j\} \subseteq G$, multiplication in G is well defined. If such an algorithm of multiplication exists, the generating system $\mathfrak{a} = \{a_1, \ldots, a_n\}$ is called a „special generating system of G".

Basic programs for the multiplication of the elements of G are developed in [2], [6], [8].

1.1.2 Representation of subgroups of G

Let $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ be the prime power decomposition of the order $|G|$ of G, $\{U\}$ the set of all subgroups $U \subseteq G$ and $\{S(U)\}$ the set of all systems $S(U)$ containing all cyclic subgroups of G of prime power order contained in U. Then we get a 1–1-correspondence $\{U\} \longleftrightarrow \{S(U)\}$ between $\{U\}$ and $\{S(U)\}$:

(1.1) $$G \supseteq U \longleftrightarrow S(U) = \{<z> \subseteq G \ / \ <z> \subseteq U,\ |<z>| = p^{\alpha},\ \alpha \geq 1,\ p \text{ prime}\}$$, and a system

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

of generating elements of all cyclic subgroups of $S(U)$ forms a uniquely determined generating system of $U \subseteq G$.

To store the subgroups $U \subseteq G$ of G in the computer by „characteristic numbers", the elements of $E(G)$ shall be listed. Then, if $E(U) = \{z_{i_1}, \ldots, z_{i_\ell}\} \subseteq E(G)$ $(\{i_1, \ldots, i_\ell\} \subseteq \{1, \ldots, |E(G)|\})$ is a generating system of U by

(1.3) $$K[U] = \sum_{j=1}^{\ell} 2^{i_j - 1}$$

a dual number is defined, which uniquely corresponds to the subgroup U of G : $U \longleftrightarrow K[U]$.

Using the Boolean operation of intersection "$\wedge$" we get

(1.4) $$\begin{array}{l} K[U] \wedge K[V] = K[U \cap V] \\ U \subseteq V \longleftrightarrow K[U] \wedge K[V] = K[U] \end{array} \qquad (U,V \subseteq G)$$

1.2 Factorization of G by a Hall system

1.2.1 Definition of a Hall system

A system $\mathcal{H} := \{H_i \ / \ i = 1, \ldots, r\}$ of subgroups of G is called a Hall system of G, if

(1.5)
- a) $G = H_1 \cdot \ldots \cdot H_r$
- b) $H_i H_k = H_k H_i \qquad (i,k = 1, \ldots, r;\ i \neq k)$
- c) $(|H_i|, |H_k|) = 1$
- d) $\{H_i \ / \ i = 1, \ldots, r\}$ is conjugate to every system $\{H_i^* \ / \ i = 1, \ldots, r\}$ of G satisfying a) . . . c) $(g H_i g^{-1} = H_i^*$ for some $g \in G)$.

If G contains a Hall system $\mathcal{H}$, we also say that G is „factorizated by the Hall system $\mathcal{H}$" .

1.2.2 Sylow basis of a solvable group G

Let G be solvable of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ (p_i prime number). Then G contains a system $\{P_i/i=1,\ldots,r\}$ of p_i-Sylow subgroups of G satisfying (1.5),a), . . . , d). $\{P_i/i=1,\ldots,r\}$ is called a „Sylow basis of G " [7].

1.2.3 Groups containing a chain of normal Hall groups

A subgroup chain

(1.6) $$G = G_r \supset \ldots \supset G_i \supset \ldots \supset G_1 \supset G_o = <e>$$

is called a „chain of normal Hall groups of G", if $G_i \lhd G$ and $(|G_i|, [G : G_i]) = 1$ $(i = 1, \ldots, r)$.
Since $P \subseteq G_i$ for all p-Sylow subgroups of G with $p/|G_i|$, G_i is a characteristic subgroup of G. Therefore, (1.6) is a chain of normal Hall groups of G, if and only if $G_i \lhd G_{i+1}$ and $(|G_i|, [G_{i+1} : G_i]) = 1$, $(i=1,\ldots,r-1)$.
In the case that G contains a chain of normal Hall groups, G can be factorizated by a Hall system [5] :

Theorem 1.1: Under the assumption that G contains a chain (1.6) of normal Hall groups we obtain:

a) G contains a Hall system $\{H_i/ i = 1, \ldots, r\}$ of subgroups of G such that:

(1.7)

α) $G_i = H_1 \cdot \ldots \cdot H_i$ β) $H_iH_k = H_kH_i$

γ) $(|H_i|, |H_k|) = 1$ δ) $H_i \lhd H_iH_k$ $(i < k)$

ε) $H_i \cong G_i/G_{i-1}$ $(i,k = 1, \ldots, r,\ i \neq k)$

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

If G is not solvable, by the theorem of Feit-Thompson in a chain (1.6) of normal Hall groups of G at most one factor G_k/G_{k-1} is not solvable.
Under this assumption on G it can be shown that every Hall group $H_i (i \neq k)$ of G can be substituted by a system of special Sylow subgroups of G [5]:

Theorem 1.2: Let G be a non solvable group with a chain (1.6) of normal Hall groups of G and let k be the only index such that G_k/G_{k-1} is not solvable. Then G contains a Hall system $\{H_i/i=1,\ldots,r\}$ satisfying (1.7) and:

a) For $i \neq k$ there exists a Sylow basis $P_{i,1}, \ldots, P_{i,n_i}$ of H_i such that the „complete Hall system"

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

satisfies (1.7)

b) Any two complete Hall systems of G are conjugate in G.

From Theorem 1.2 consequently follows that without regard to the non solvable part of G the development of a computational algorithm for a non solvable group G, which contains a chain of normal Hall groups, is similar to the case G being solvable.

1.3 Factorization of G [1], [3]

1.3.1 Let $G = H_1H_2 = H_2H_1$, $H_1 \cap H_2 = <e>$ be a factorization of G by H_1, H_2. Then for every $h_i \in H_i$ (i=1,2) we obtain a map $h_i{}^k : H_k \to H_k$ of H_k into H_k defined by :

(1.9)
$$h_1{}^2 h_2 = H_1h_2h_1 \cap H_2 \quad \text{for all } h_2 \in H_2$$
$$h_2{}^1 h_1 = h_2h_1H_2 \cap H_1 \quad \text{for all } h_1 \in H_1$$

These mappings $h_i{}^{\kappa}$ together with the defining relations of the components H_i (i=1,2) of G define the structure of G. This is obvious, because multiplication in G is completely determined by the relation:

$$h_2 \cdot h_1 = h_2{}^{1} h_1 \cdot h_1{}^{2} h_2 \ , \tag{1.10}$$

which is equivalent to (1.9).

1.3.2 By the theory of factorization [3] it follows that the set of mappings $h_i{}^{\kappa}$ forms a permutation subgroup $\Pi_{i,k}$ of the symmetric group $S_{|H_k|}$ of degree $|H_k|$. The set $N_i := \{h_i \in H_i / h_i{}^{\kappa} h_k = h_k$ for all $h_k \in H_k\}$ is the maximal normal subgroup of G contained in H_i, which determines the homomorphism $\tau_{i,k} : H_i \to \Pi_{i,k}$, $H_i/N_i \cong \Pi_{i,k}$ [3]. An other important group for the theory of factorization is the „fix group" $F_i := \{h_i \in H_i \ / \ h_k{}^{\iota} h_i = h_i$ for all $h_k \in H_k\}$ Between F_i and the normalizer $N_G(H_k)$ of H_k in G we obtain the following relation [5] :

$$F_i = N_G(H_k) \cap H_i \ , \quad N_G(H_k) = F_i H_k = H_k F_i \tag{1.11}$$

1.3.3 If $G = H_1 \cdot \ldots \cdot H_r$ is a factorization of G by a Hall system $\{H_i \ / \ i = 1, \ldots, r\}$ of G, we can apply the theory of factorization to the subgroups $G_{i,k} := H_i H_k$ $(i \neq k)$ of G. F_i^k may denote the fixgroup of $\Pi_{k,i}$ and N_i^k the maximal subgroup of $G_{i,k}$ contained in H_i.

Regarding the factorization $G = Q \cdot H_i$, $Q := H_1 \cdot \ldots \cdot H_{i-1} H_{i+1} \cdot \ldots \cdot H_r$, it follows

$$F_i = \bigcap_{\substack{k=1 \\ k\neq i}}^{r} F_i^k \ , \quad N_i = \bigcap_{\substack{k=1 \\ k\neq i}}^{r} N_i^k \tag{1.12}$$

and using (1.11):

$$\begin{aligned} N_G(Q) \cap H_i = F_i = \bigcap_{\substack{k=1 \\ k\neq i}}^{r} F_i^k &= \bigcap_{\substack{k=1 \\ k\neq i}}^{r} [N_{G_{i,k}}(H_k) \cap H_i] \\ &= \bigcap_{\substack{k=1 \\ k\neq i}}^{r} [N_G(H_k) \cap H_i] = [\bigcap_{\substack{k=1 \\ k\neq i}}^{r} N_G(H_k)] \cap H_i = [\bigcap_{k=1}^{r} N_G(H_k)] \cap H_i \end{aligned} \tag{1.13}$$

Since F_i consists of all elements of H_i normalizing all H_k, we get $f_i f_k f_i^{-1} f_k^{-1} \in H_i \cap H_k = \langle e \rangle$. Therefore, the system normalizer $F(\mathcal{H}) := \bigcap_{k=1}^{r} N_G(H_k)$ of G related to the Hall system $\mathcal{H} := \{H_i \ / \ i = 1, \ldots, r\}$ of G can be represented as the direct product of the F_i : $F(\mathcal{H}) = F_1 \times \ldots \times F_r$.

1.4 Calculation of $\Pi_{i,k}$, F_i^k, N_i^k , computational comparsion of products

1.4.1 Determination of $\Pi_{i,k}$

For the determination of $\Pi_{i,k}$ the elements of the components H_i $(i = 1, \ldots, r)$ of G may be numbered in the same sequence as they are generated by the generating process ([6]). Then, generating the subgroups $G_{i,k}=H_iH_k=H_kH_i$ $(i,k = 1, \ldots, r;\ i < k)$ one 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:

$$h_i^{(\ell)} h_k^{(s)} = h_k^{(s_\nu)} h_i^{(\ell_\rho)} = h_i^{(\ell)}{}^{k} h_k^{(s)} \cdot h_k^{(s)}{}^{i} h_i^{(\ell)} \qquad \begin{matrix} (s = 1, \ldots, |H_k|) \\ (1 \leq \ell \leq |H_i|) \end{matrix} \tag{1.14}$$

From these relations we obtain the permutation $h_i^{(\ell)}{}^{\kappa}$ of H_k related to the element $h_i^{(\ell)} \in H_i$: $h_i^{(\ell)} \to h_i^{(\ell)}{}^{k} = \binom{s}{s_\nu}$.

If ℓ runs from 1 to $|H_i|$ we get $\Pi_{i,k}$. Fixing $s(1 \leq s \leq |H_k|)$ we similarly can determine for variable ℓ (ℓ=1,...,$|H_i|$) the permutation $h_k^{(s)}i = \binom{\ell}{\ell_\rho}$ related to $h_k^{(s)} \in H_k$, and if s runs from 1 to $|H_k|$ we get $\Pi_{k,i}$.

1.4.2 Determination of F_i^k and N_i^k

Let $G = H_1 \cdot \ldots \cdot H_r$ be a factorization by a Hall system $\{H_i \mid i = 1, \ldots, r\}$ and $E(H_j)$ (j = i,k) defined as in 1.1.2.
Then using the results of 1.3.2 by a fundamental well known generating process [6] the groups F_i^k and N_i^k can be determined:

$$(1.15)\qquad \begin{aligned} F_i^k &= \langle z_i \rangle \text{ generated by all } z_i \in E(H_i),\ z_i z_k z_i^{-1} \in H_k \quad \text{for all } z_k \in E(H_k) \\ N_i^k &= \langle z_i \rangle \text{ generated by all } z_i \in E(H_i),\ z_k z_i z_k^{-1} \in H_i \quad \text{for all } z_k \in E(H_k)\,. \end{aligned}$$

1.4.3 Comparsion of products

Let $G = H_1 \cdot \ldots \cdot H_r$ be a factorization of G by a Hall system $\{H_i \mid i = 1, \ldots, r\}$ of G. Then, for proving the equality $U_i H_k = H_k U_i$, $U_i \subset H_i$ $(k \neq i)$ we have to verify the invariance of U_i, P_k by applying the permutations $h_k i \in \Pi_{k,i}$, $u_i k \in \Pi_{i,k}$ to U_i, H_k, respectively. Since H_k is invariant against all $h_i k \in \Pi_{i,k}$ we only have to prove, whether U_i is invariant applying all $h_k i \in \Pi_{k,i}$ to U_i. According to [[3], Theorem 2.2] it is sufficient to prove $h_k^{(\ell)} i\, u_i \in U_i$ for all $u_i \in U_i$ and for all $h_k^{(\ell)}$ of a system $\{h_k^{(\ell)}\}$ of generating elements of H_k. Such comparsions of products will be used in the algorithm of determining the maximal subgroups of a finite group G. (cf. 1.7.3).

1.5 Determination of a Sylow basis of a solvable group G

1.5.1 The Sylow basis as a intersection of Sylow-complements [1], [3]

Let G be a solvable group of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Then, calculating a system $\{K_i \mid i = 1, \ldots, r\}$ of p_i-Sylow complements K_i of G of order $|K_i| = \prod_{\substack{j=1 \\ j \neq i}} p_j^{\alpha_j}$, we get a Sylow basis of G by

$$\{P_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{r} K_j \mid i = 1, \ldots, r\}\,.$$

1.5.2 Determination of the system $\{K_i \mid i = 1, \ldots, r\}$ of p_i-Sylow complements

Let $M_i = \{z_1, \ldots, z_t\} \subseteq E(G)$ be the set of generating elements of all cyclic subgroups $\langle z_\ell \rangle \subseteq G$ (ℓ = 1,...,t) of p_k-prime power order, where $p_k \neq p_i$.
If K_i is a p_i-Sylow complement of G, then $E(K_i) \subseteq M_i$, and conversely to every $z \in M_i$ there exists a p_i-Sylow complement containing z.
A p_i-Sylow complement K_i of G can successively be generated by the calculation of the subgroup chain

$$\langle e \rangle \subset U_1 \subset \ldots \subset U_s = K_i \text{ with } U_1 = \langle z_1 \rangle,\ U_k = \langle U_{k-1}, z_{i_k} \rangle\ (k=1,\ldots,s)\,,$$

where $1 < i_2 < \ldots < i_k < \ldots < i_s$ and i_k is the minimum of all $j \leq t$, such that

$$z_j \notin U_{k-1} \ \underline{\text{and}}\ p_i \not|\, |\langle U_{k-1}, z_j \rangle|\,.$$

There exists an algorithm for determining $\langle U,g \rangle$ ($U \subseteq G$, $g \notin U$) described in [6].

1.6 Construction of a chain of normal Hall groups for a non-solvable group G and the determination of a complete Hall system of G

In the following let G be a non-solvable group of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$.

1.6.1 The lattice of normal Hall groups of G

The set of normal Hall groups of G forms a complete and distributive lattice $\mathfrak{L}(G)$. Any two subgroups series of $\mathfrak{L}(G)$ have isomorphic refinements. Therefore, a complete Hall system of G belonging to a chain of normal Hall groups, which cannot be refined, is up to an inner automorphism of G uniquely determined [O] .

1.6.2 Construction of special minimal Hall groups

For any prime number $p_i / |G|$ we get a minimal group $N_{(i)} \in \mathfrak{L}(G)$ such that $p_i / |N_{(i)}|$.

To construct $N_{(i)}$ let $Z_i := < z_{i,1}, \ldots, z_{i,s_i} >$ be the subgroup of G generated by the generating elements $z_{i,k}$ of all cyclic p_i-subgroups $< z_{i,k} >$ of prime power order of G $(i = 1, \ldots, r)$.

We set $M_i^1 := \{p_l \,/\, p_l / |Z_i|\}$ and define inductively:

$$M_i^{k+1} := M_i^k \cup \bigcup_{p_j \in M_i^k} M_j^1 \qquad (i = 1, \ldots, r) \tag{1.16}$$

Then to any M_i^k $(i = 1, \ldots, r)$ there uniquely corresponds a vector

$$(\beta_{i1}^k, \ldots, \beta_{ir}^k), \quad \text{where} \quad \begin{array}{l} \beta_{ij}^k = 1, \ \text{if } p_j \in M_k^i \\ \beta_{ij}^k = 0, \ \text{if } p_j \notin M_i^k \end{array}$$

and these vectors together form a matrix (β_{ij}^k) $(1 < i,j < r)$.

Using the Boolean operations for addition:

$$0 + 0 = 0$$
$$a + b = 1 \quad , \quad \text{if at least one term of the sum is} \neq 0$$

from (1.16) we get by matrix multiplication:

$$(\beta_{ij}^k) = (\beta_{ij}^1)^k \qquad (i,j = 1, \ldots, r; \ 1 < k < r - 1) \tag{1.17}$$

If $(\beta_{ij}^1)^k = (\beta_{ij}^1)^{k+1}$, then $|N_{(i)}| = p_1^{\beta_{i1}^k \alpha_1} \cdot \ldots \cdot p_r^{\beta_{ir}^k \alpha_r}$ and $N_{(i)}$ can be generated by the generating elements of all cyclic p_j-subgroups of prime power order of G, where p_j is running through the set of all prime numbers, the exponent β_{ij}^k of which is equal to 1.

1.6.3 Determination of a chain of normal Hall groups of G

Because $N \in \mathfrak{L}(G)$ is uniquely determined by the set of prime numbers dividing $|N|$, we get $N = \prod_{p_i / |N|} N_{(i)}$. Using fundamental program systems described in [6] it is possible to determine the lattice $\mathfrak{L}(G)$ and consequently an appropriate chain of normal Hall groups.

1.6.4 Determination of a complete Hall system of G

In the following let G be a finite non solvable group with a chain (1.6) of normal Hall groups. Without loss of

generality for our investigations we can consider the chain $G = G_3 \supset G_2 \supset G_1 \supset G_o = \langle e \rangle$, where G_2/G_1 is not solvable and G_2/G_1 does not contain a normal Hall group.
If $|G_1| = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$, by the method described in 1.5 it is possible to determine a p_i-Sylow complement Q_i $(i = 1, \ldots, t)$ and $F = \bigcap_{i=1}^{t} Q_i$ is a subgroup of G such that G is a splitting extension of G_1 by F :

$$G_1 \lhd G = F \cdot G_1, \quad F \cap G_1 = \langle e \rangle, F \cong G/G_1$$

Further, the system

$$\{P_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{t} (Q_j \cap G_1) \; / \; i = 1, \ldots, t\}$$

is a Sylow basis of G_1 such that $P_i \lhd FP_i$ $(i = 1, \ldots, t)$. $H = F \cap G_2$ is a subgroup of G, which represents the factor group G_2/G_1 in G_1. Since $H \cong G_2/G_1$, by assuption H does not contain a normal Hall group, and we still have to construct a complete Hall system for the chain $F \supset H \supset \langle e \rangle$:

If P_j is a p_j-Sylow subgroup of H with $p_j / |H|$, we get by [12] , IV, Exerc.:

$$N_F(P_j)/N_H(P_j) \cong F/H,$$

which means that $N_H(P_j)$ is a normal Hall group of $N_F(P_j)$. By the theorem of Feit-Thompson H has even order. In the case $p_j = 2$ it follows that $N_H(P_j)/P_j$ is of odd order and consequently solvable. Therefore, $N_H(P_j)$ and moreover $N_F(P_j)$ are solvable. Calculating a subgroup L of $N_F(P_j)$ such that $N_F(P_j) = L \cdot N_H(P_j)$ and applying the method of 1.5 to L we obtain a Sylow basis $P_{t+1}, \ldots, P_{t+s}$ of L. Then the system $P_1, \ldots, P_t, H, P_{t+1}, \ldots, P_{t+s}$ is a complete Hall system of G as desired in Theorem 1.2.

1.7 Algorithm for the determination of the maximal subgroups of a solvable group G

In this section let G be a solvable group of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Then $G = P_1 \cdot \ldots \cdot P_r$, where $\{P_i \; / \; i = 1, \ldots, r\}$ is a Sylow basis of G.

1.7.1 Basic theorems

Without proofs we write up the basic theorems, which will be used for the development of the computational algorithm for determining all maximal subgroups of G :

Theorem 1.3: Let U be a subgroup of the solvable group G, $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, $|U| = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$ $(0 \leq \beta_i \leq \alpha_i; i = 1, \ldots, r)$. Then to any Sylow basis $P_1(U), \ldots, P_r(U)$ of U there corresponds a Sylow basis $P_1, \ldots, P_r$ of G such that $P_i(U) = P_i \cap U$ $(i = 1, \ldots, r)$ ([7], p 666) .

Theorem 1.4: Every maximal subgroup M of G has prime power index in G ([7], p. 164) .

Theorem 1.5: Let M be a maximal subgroup of G. Then:

a) If $M \lhd G$, then $|G/M| = p$ (p prime number)

b) If $M \not\lhd G$, $[G : M] = p^n$, and if G'_p is a p-Sylow complement of G such that $G'_p \subseteq M$, then $N_G(G'_p) \subseteq M$ ([7], p. 734) .

1.7.2 Consequences of Theorems 1.3.–1.5 for the development of the algorithm

A) Let M be a maximal subgroup of G. Since any two Sylow bases are conjugate in G, it follows from Theorem 1.3 that there exists a conjugate maximal subgroup M^* of G such that from the factorization $G = P_1 \cdot \ldots \cdot P_r$

we obtain a factorization $M^* = (M^* \cap P_1) \circ \ldots \cdot (M^* \cap P_r)$ for M^*.

B) By Theorem 1.4, however, only one term $M^* \cap P_i$ is different from P_i : $M^* \cap P_k = P_k$ ($k \neq i$), hence $M^* = P_1 \cdot \ldots \cdot (M^* \cap P_i) \cdot \ldots \cdot P_r$.

C) $G'_p = P_1 \cdot \ldots \cdot P_{i-1}P_{i+1} \cdot \ldots \cdot P_r$ is a p_i–Sylow complement contained in M^*.
If $M \not\triangleleft G$, by Theorem 1.5 we get $N_G(G'_p) \subseteq M^*$, hence $F_i = N_G(G'_p) \cap P_i \subseteq M^* \cap P_i$, where F_i is the i-th component of the system normalizer $F = F_1 \times \ldots \times F_r$ of G (1.3.3). F_i depends only on the factorization $G = P_1 \cdot \ldots \cdot P_r$ of G. In the case $M \triangleleft G$ we get

$$G/_M = P_1 \cdot \ldots \cdot P_r \Big/ P_1 \cdot \ldots \cdot P_{i-1}(M \cap P_i)P_{i+1} \cdot \ldots \cdot P_r \cong P_i/M \cap P_i .$$

This means that $M \cap P_i$ is a maximal subgroup of P_i with $[P_i : (M \cap P_i)] = p_i$, $(M \cap P_i)P_k = P_k(M \cap P_i)$ $(k = 1, \ldots, r,\ k \neq i)$.

1.7.3 The algorithm

By the following algorithm it is possible to calculate all maximal subgroups of the solvable group $G = P_1 \cdot \ldots \cdot P_r$ of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ factorizated by the p_i-Sylow groups of a Sylow basis $\{P_i \,/\, i = 1, \ldots, r\}$ of G.
We assume that the lattice $V(P_i)$ of all subgroups of $P_i (i = 1, \ldots, r)$ has been determined by one of the methods described in [2], [4], [10].
Let us fix the index i ($1 \leq i \leq r$). Since $|P_i| = p_i^{\alpha_i}$, $V(P_i)$ consists of $\alpha_i + 1$ layers. The s-th layer Σ_s of $V(P_i)$ contains only those subgroups of P_i having order p_i^s $(o \leq s \leq \alpha_i)$.
The groups $Q_{o,1}, \ldots, Q_{o,s_o}$ of the layer $\Sigma_{\alpha_i - 1}$ of $V(P_i)$, which satisfy

(1.18) $\quad Q_{o,j}P_k = P_k Q_{o,j} \; (j=1, \ldots, s_o,\ k = 1, \ldots, r,\ k \neq i)$ *)

are the components of the normal maximal subgroups

$$M_{o,j} = P_1 \cdot \ldots \cdot P_{i-1}Q_{o,j}P_{i+1} \cdot \ldots \cdot P_r \qquad (j = 1, \ldots, s_o)$$

of G, for which $P_i \not\subseteq M_{o,j}$.
For the further iterative procedure only the groups of the set

$$S_o(P_i) := \{H \in \bigcup_{\nu=2}^{\alpha_i} \Sigma_{\alpha_i - \nu} \,/\, F_i \subseteq H\} \quad {}^{**)}$$

are relevant.
Now we define inductively that part of the algorithm, by which non-normal maximal subgroups of G are defined:
If $S_t(P_i) \neq \emptyset$ $(1 \leq t \leq \alpha_i)$, where

$$S_t(P_i) = \{H \in S_{t-1}(P_i) \,/\, H \not\subseteq Q_{t-1,j} \text{ and } |H| \neq p^{\alpha_i - t} \qquad (j = 1, \ldots, s_{t-1})\}$$

we pick up all subgroups $Q_{t,1}, \ldots, Q_{t,s_t} \in S_t(P_i)$, which belong to the $(\alpha_i - t - 1)$-th layer of $V(P_i)$ and satisfy the relations:

$$Q_{t,j}P_k = P_k Q_{t,j} \quad (j = 1, \ldots, s_t,\ k = 1, \ldots, r,\ k \neq i).$$

*) For prooving the relations 1.18 see (1.4.3).

**) $\bigcup_{\nu=2}^{\alpha_i} \Sigma_{\alpha_i - \nu}$ is equal to the union of all groups $H \in V(P_i)$ contained in the layers $\Sigma_{\alpha_i - \nu}$ $(\nu = 2, \ldots, \alpha_i)$ of $V(P_i)$.

Then the groups

$$M_{t,j} = P_1 \cdot \ldots \cdot P_{i-1}\, Q_{t,j} P_{i+1} \cdot \ldots \cdot P_r \quad (j = 1, \ldots, s_t)$$

are non-normal subgroups of G, for which $P_1, \ldots, P_{i-1}, M_{t,j} \cap P_i, P_{i+1}, \ldots, P_r$ is a Sylow basis.

$S_{t+1}(P_i)$ will be obtained from $S_t(P_i)$ by eliminating all groups of $S_t(P_i)$, which are subgroups of the $Q_{t,j}$ $(j = 1, \ldots, s_t)$ or satisfy a special order relation:

$$S_{t+1}(P_i) = \{H \in S_t(P_i) \;/\; H \not\subseteq Q_{t,j} \text{ and } |H| \neq p^{\alpha_i - t - 1} \quad (j = 1, \ldots, s_t)\}$$

If $S_m(P_i) = \emptyset$ $(1 < m < \alpha_i)$ all maximal subgroups M of G, for which $P_1, \ldots, P_{i-1}, M \cap P_i, P_{i+1}, \ldots, P_r$ is a Sylow basis, are determined.

Repeating this method for each $i \in \{1, \ldots, r\}$ we get the set $\mathfrak{R}$ of all maximal subgroups M of G, for which $M \cap P_1, \ldots, M \cap P_r$ is a Sylow basis.

From the theory of Sylow systems finally follows that the set $\mathfrak{C}$ of all maximal subgroups of G will be obtained by the application of special inner automorphisms $\tau(g_i)$ of G on all elements

$$K \in \mathfrak{R} : \tau(g_i)K := g_i^{-1} K g_i \;,$$

where g_i are the representatives of the coset decomposition $G = Fg_1; \ldots \cdot Fg_t$ $(g_1 = e)$ of G by the system normalizer $F = \bigcap_{j=1}^{r} N_G(P_j)$ of G.

1.8 The algorithm for non-solvable groups containing a chain of normal Hall groups

1.8.1 Basic theorems

Let G be a finite non solvable group, which contains a chain $G = G_r \supset \ldots \supset G_i \supset \ldots \supset G_1 \supset \langle e \rangle$ of normal Hall groups. Then, similar to the theorems of section 1.7 in [0] the following fundamental results are proved:

Theorem 1.6: Let $G = G_r \supset \ldots \supset G_i \supset \ldots \supset G_1 \supset \langle e \rangle$ be a chain of normal Hall groups of G and M a maximal subgroup of G. Then $[G : M] \,/\, |G_{i}/G_{i-1}|$ for some $i \in \{1, \ldots, r\}$. Additionally, if G_i / G_{i-1} is solvable, $[G : M]$ is a prime power. ([0], Theorem II, 1.4).

Theorem 1.7: Let $G = G_r \supset \ldots \supset G_i \supset \ldots \supset G_1 \supset \langle e \rangle$ be a chain of normal Hall groups of G and U a subgroup of G with a chain $U = U_r \supseteq \ldots \supseteq U_i \supseteq \ldots \supseteq U_1 \supseteq \langle e \rangle$ of normal Hall groups $U_i = U \cap G_i$ $(i = 1, \ldots, r)$ of U. Then to every complete Hall system $\mathcal{H}(U)$ of U there exists a complete Hall system $\mathcal{H}(G)$ of G such that the elements of $\mathcal{H}(U)$ can be obtained by intersecting the elements of $\mathcal{H}(G)$ with U. ([0]), Theorem II. 1.11).

Theorem 1.8: Let $G = G_r \supset \ldots \supset G_i \supset \ldots \supset G_1 \supset \langle e \rangle$ be a chain of normal Hall groups of G. With regard to this chain let further

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

be a complete Hall system of G, where H_k is the non solvable part of the Hall system. Then:

a) If M is a maximal subgroup of G such that $[G : M] \not| \, |H_k|$, then $[G : M] = p^{\alpha}$ for some prime number p.

b) If $M \lhd G$, $[G : M] \not| \, |H_k|$, then $[G : M] = p$.

c) If $M \ntriangleleft G$, $[G : M] \not| \, |H_k|$, then there exists a maximal subgroup M^* of G, which is conjugate to M, such that

$$P_{1,1} \cap M^*, \ldots, P_{1,n_1} \cap M^*, \ldots, P_{k-1,1} \cap M^*, \ldots, P_{k-1,n_{k-1}} \cap M^*, H_k, P_{k+1,1} \cap M^*, \ldots, P_{k+1,n_{k+1}} \cap M^*, \ldots, P_{r,1} \cap M^*, \ldots, P_{r,n_r} \cap M^*$$

is a complete Hall system of M^* with:

$$P_{j,i} \cap M^* = P_{j,i}, \text{ if } p \not| |P_{j,i}|$$
$$P_{r,s} \cap M^* = P^*_{r,s} \supseteq F_{r,s}, \text{ if } p \,/\, |P_{r,s}|$$
$$F_{r,s} = P_{r,s} \cap N_G(H_k) \bigcap_{j,i \neq r,s} N_G(P_{j,i}) \;. \qquad \text{([0], Theorem II. 1.13)}$$

1.8.2 Some remarks about the proofs of Theorem 1.6 – Theorem 1.8

Theorem 1.6 follows trivially for $n > 2$, if it is true for $n = 2$. Therefore, let $G = F \cdot N$, $N \lhd G$, $(|N|, |F|) = 1$ be a splitting extension of G and let futher M be a maximal subgroup of G.
Then, if $M \supseteq N$, M/N is maximal in G/N and Theorem 1.6 follows from Theorem 1.4. If $M \not\supseteq N$, we get $G = M \cdot N$, hence $|G| = |M| \cdot |N| \,/\, |M \cap N|$, which yields $[G : M] = |N| \,/\, |M \cap N|$. In the case N being solvable for an appropriate prime number p N contains a non-trivial characteristic p-subgroup C. For $C \not\subseteq M$ we get $G = M \cdot C$ and for $C \subseteq M$ the result follows by induction.
If G is a solvable group of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, A a subgroup of its automorphism group such that $(|A|, |G|) = 1$ and if further π is a set of prime numbers dividing $|G|$, then it can be shown that any A–allowable π–subgroup U of G is contained in an A–allowable π–Hall group of G. Using this result under the same assumptions on G it follows that to every A–allowable Sylow system $P_1(U), \ldots, P_r(U)$ of an A-allowable subgroup U of G there corresponds an A–allowable Sylow system $P_1, \ldots, P_r$ of G such that $P_i \cap U = P_i(U)$ $(i = 1, \ldots, r)$. Making use of this result Theorem 1.7 follows immediately.

Let M be a maximal A–allowable subgroup of the solvable group G. Then, if $M \lhd G$ and A induces the identity on G/M, G/M is cyclic of prime order. In the case that $M \lhd G$ and A does not induce the identity on G/M or $M \ntriangleleft G$, we obtain $[G : M] = p^\alpha$ $(\alpha > 1)$ for some prime number p and $[N_G(G'_p)]^A \subseteq M$ for a p-complement G'_p of G contained in M. From this Theorem 1.8 follows consequently.

1.8.3. Computational consequences

From the point of view of computation Theorem 1.8 shows, that the algorithm in the case of a non solvable group G, which contains a complete Hall system $P_1, \ldots, P_t, H, P_{t+1}, \ldots, P_{t+s}$, with the exception of the non solvable part H of G is exactly the same as in the case G being solvable.

Proceeding from a generating system E(H) (cf. 1.1.2) and using a subgroup chain

$$\langle e \rangle = K_0 \subset K_1 \subset \ldots \subset K_s = H \text{ where } K_i = \langle K_{i-1}, z_{t_i} \rangle,\ z_{t_i} \in E(H) \quad (i = 1, \ldots, s)$$

in [6], 1 it is pointed out, that making coarser this subgroup chain it is possible to find an appropriate generating system of H, the elements of which can be multiplied most effectively.

A complete Hall system $P_1, \ldots, P_t, H, P_{t+1}, \ldots, P_{t+s}$ can be determined by the method developed in 1.6.4.

Since H is not solvable, it is necessary to calculate V(H) by an algorithm described in [4], [6], [10].

By Theorem 1.6, Theorem 1.7 and the property of conjugateness of a Hall system it follows that in the case M being maximal in G with $[G : M] / |H|$ there exists a conjugate subgroup M^* of M in G such that $M^* = P_1 \cdot \ldots \cdot P_t Q P_{t+1} \cdot \ldots \cdot P_s$, $Q \subset H$. But if $M^* \lhd G$, Q is not generally maximal in H. Therefore, the normality of M^* must be proved separately.

If $Q_{j,1}, \ldots, Q_{j,s(j)}$ are the subgroups of the j–th layer of V(H) such that $M^*_{j,k} = P_1 \cdot \ldots \cdot P_{t-1} Q_{j,k} P_{t+1} \cdot \ldots \cdot P_{t+s}$ $(k = 1, \ldots, s(j))$ are maximal in G, then only subgroups of the lower layers of V(H), which are not contained in the $Q_{j,k}$'s, can generate further maximal subgroups of G.

Taking notice only of this property the algorithm developed for p-Sylow groups P can also be used in the case H being a non-solvable group of the Hall system of G.

2. Extension of the method for determining the maximal subgroups of a finite group G to an algorithm for the determination of the complete lattice V(G) of G

2.1 The case of a solvable group G

2.1.1 The semi-lattice $T(P_1, \ldots, P_r)$ as the underlying structure of V(G)

Let $\{P_i \,/\, i = 1, \ldots, r\}$ be a Sylow basis of a solvable group G of order $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$. Then, having calculated the semi-lattice $T(P_1, \ldots, P_r)$ of all subgroups U of G, for which $U \cap P_1, \ldots, U \cap P_r$ is a Sylow basis, by Theorem 1.3 and by making use the properties of a Hall system we obtain the complete lattice V(G) of G from $T(P_1, \ldots, P_r)$ by the application of special inner automorphisms $\tau(g_i)$ $(i = 1, \ldots, s)$ to the elements of $T(P_1, \ldots, P_r)$ where g_i are the representatives of the coset decomposition of G by the System normalizer F of the Sylow basis $\{P_i \,/\, i = 1, \ldots, r\}$.

2.1.2 Construction of $T(P_1, \ldots, P_r)$

To construct $T(P_1, \ldots, P_r)$ of G, it is necessary to determine the maximal subgroups M of G with $M \cap P_1, \ldots, M \cap P_r$ being a Sylow basis of M and for every M similar the maximal subgroups M′ with $M' \cap P_1, \ldots, M' \cap P_r$ being a Sylow basis of M′, a.s.o. .

Assuming that U is a subgroup of G such that $U \cap P_1, \ldots, U \cap P_r$ is a Sylow basis of U, a maximal subgroup V of U with Sylow basis

$$V \cap (U \cap P_1) = V \cap P_1, \ldots, V \cap (U \cap P_r) = V \cap P_r$$

can be determined, if it is possible to calculate the permutation groups $\Pi_{i,k}(U)$ related to the factorization $U = (U \cap P_1) \cdot \ldots \cdot (U \cap P_r)$ of U.

2.1.3 Calculation of the permutation group $\Pi_{i,k}(U)$

Let $\mathfrak{A}_i = \{a_{i,1}, \ldots, a_{i,t(i)}\}$ be a generating system of P_i ([6]),1) and $\{a_{i,1}k, \ldots, a_{i,t(i)}k\}$ the set of permutations of $\Pi_{i,k}$ related to $\mathfrak{A}_i$.
Then, if $p_i^{(\ell)}$ are the elements of a generating system $\{p_i^{(\ell)}\}$ of $U \cap P_i$ and if

$$p_i^{(\ell)} = a_{i,1}^{c_1} \cdot \ldots \cdot a_{i,t(i)}^{c_{t(i)}}$$

is the representation of $p_i^{(\ell)}$ as a word of the $a_{i,j}$'s $(j = 1, \ldots, t(i))$, we obtain the following permutations $p_i^{(\ell)}k$ of P_k:

$$p_i^{(\ell)}k = (a_{i,1}k)^{c_1} \cdot \ldots \cdot (a_{i,t(i)}k)^{c_{t(i)}} \qquad (i > k)$$
$$(2.1)$$
$$p_i^{(\ell)}k = (a_{i,t(i)}k)^{c_{t(i)}} \cdot \ldots \cdot (a_{i,1}k)^{c_1} \qquad (i < k)$$

The restrictions of these permutations on $U \cap P_k$ are the required generating elements of the groups $\Pi_{i,k}(U)$. In this way we are able to construct $\Pi_{i,k}(U)$ for every $U \in T(P_1, \ldots, P_r)$.

2.2 The case of a non solvable group G containing a chain of normal Hall groups

Let $P_1, \ldots, P_t, H_0, P_{t+1}, \ldots, P_{t+s}$ be a complete Hall system of the non solvable group G related to a chain of normal Hall groups.
If $U \in T(P_1, \ldots, P_t, H_0, P_{t+1}, \ldots P_{t+s})$, then we use an appropriate generating system for H_0 to calculate $\Pi_{0,k}(U)$ from $\Pi_{0,k}$ $(k = 1, \ldots, t + s)$.

2.2.1 Determination of an appropriate generating system of H_o

Outgoing from a generating system $E(H_o)$ of H_o (cf. 1.1.2), such a generating system for H_o can be determined by an appropriate subgroup chain:

$<e> = K_o \subset \ldots \subset K_j \subset \ldots \subset K_s = H_o$ where $K_j = <K_{j-1}, h_j>$, $h_j \in E(H_o)$, $[K_j : K_{j-1}] = r_j$, $(j=1, \ldots, s)$.
If $R_j := \{\alpha_j^{(\nu)} \mid \nu = o, \ldots, r_j - 1\}$ is a system of representatives of a right coset decomposition of K_j by K_{j-1} $(j = 1, \ldots, s)$, $\alpha_j^{(o)} = e$, every element $h_o \in H_o$ has a unique representation in the form

$$h_o = \alpha_1^{(\lambda_1)} \cdot \alpha_2^{(\lambda_2)} \cdot \ldots \cdot \alpha_s^{(\lambda_s)} \tag{2.2}$$

and if the relations

$$\alpha_k^{(\lambda_k)} \alpha_\ell^{(\lambda_\ell)} = \alpha_1^{(\mu_1)} \cdot \ldots \cdot \alpha_k^{(\mu_k)} \qquad \begin{bmatrix} \mu_\nu = f(\nu, k, \ell, \lambda_k, \lambda_\ell) \\ \nu = 1, \ldots, k \end{bmatrix} \tag{2.3}$$

$$(k=1, \ldots, s,\ \ell=1, \ldots, k,\ \lambda_k = o, \ldots, r_{k-1},\ \lambda_\ell = o, \ldots, r_{\ell-1})$$

are known, the system $\mathfrak{A} = \bigcup_{j=1}^{s} R_j$ is a generating system of H_o of the desired form ([6], 1.3.4).

2.2.2 Computational Reduction for the calculation of $\Pi_{o,k}$

Since $P_k \lhd H_o \cdot P_k$ $(k = 1, \ldots, t)$ and $H_o \lhd H_o \cdot P_k$ $(k = t+1, \ldots, t+s)$, the elements of $\Pi_{o,k}$ $(k = 1, \ldots, t)$ are automorphisms of P_k and $\Pi_{o,k}$ $(k = t+1, \ldots, t+s)$ only consists of the identical permutation of P_k. Therefore, the operation of $\Pi_{o,k}$ on P_k $(k = 1, \ldots, t)$ is already uniquely determined by the operation of the elements $\alpha_j^{(\lambda_j)}{}_k$ (related to the elements $\alpha_j^{(\lambda_j)}$ of the generating system of H_o) applied to a generating system of P_k ([3], Theorem 2.2). Similar conditions are valid for $\Pi_{k,o}$. But using these reductions the calculation of $\Pi_{o,k}(U)$ from $\Pi_{o,k}$ for $U \in T(P_1, \ldots, P_t, H_o, P_{t+1}, \ldots, P_{t+s})$ is a time-saving procedure in the computational program.

References

[0] Altmann, E.:
Über ein Verfahren zur Berechnung der maximalen Untergruppen einer endlichen Gruppe mit einer Hallschen Normalverteilerkette,
Berichte der Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 19, (1969)

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

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

[3] Gerhards, L. a. Altmann, E.:
A computational method for determining the automorphism group of a finite solvable group,
(Proc. Conf. on Comp. Algebra, Oxford, August 1967), Pergamon Press, New York, 61–74, (1969)

[4] Gerhards, L. a Lindenberg, W.:
Ein Verfahren zur Berechnung des vollständigen Untergruppenverbandes endlicher Gruppen auf Dualmaschinen,
Num. Math. 7, 1–10, (1965)

[5] Gerhards, L.:
On the construction of the automorphism group of a finite group,
will be published in Cahiers Mathematiques, Montpellier

[6] Gerhards, L.:
Group theoretical investigations on computers,
will be published in Proceedings of the conference „Utilisation des calculateurs en mathématiques pures",
Limoges, (1975)

[7] Huppert, B.:
Endliche Gruppen I,
Berlin, (1967)

[8] 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)

[9] Lindenberg, W.:
Über eine Darstellung von Gruppenelementen in digitalen Rechenautomaten,
Num. Math. 4, 151–153, (1962)

[10] Lindenberg, W. a. 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)

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

[12] Zassenhaus, H.:
The theory of groups,
Celsea Publ. Comp. (1958)

Leonhard GERHARDS
Gesellschaft für Mathematik
und Datenverarbeitung
D-5205 ST. AUGUSTIN 1
Schloss Birlinghoven
Postfach 1240 (R.F.A.)