

Computational algorithms for deciding some problems for nilpotent groups

by

A. Włodzimierz Mostowski (Warszawa)

1. Introduction.

1.1. Problems considered. This paper deals with nilpotent groups of a given nil (degree of nilpotency). When having a presentation of a group by generators x_1, \dots, x_n and relations

$$(1.1.1) \quad r_1(x_1, \dots, x_n) = 1, \dots, r_k(x_1, \dots, x_n) = 1,$$

one can ask such questions as the word problem, the inclusion problem, or the finiteness problem. For nilpotent groups all these problems are decidable. For the references concerning this question cf. my paper [3].

In this paper we shall look for "practically useful" ⁽¹⁾ algorithms for deciding these problems in the special case where we know that the groups presented by presentations (1.1.1) are nilpotent and the bound of nilpotency is explicitly given. The algorithms are given in sections 4.2-4.4. Now we shall explain the ideas of constructing the algorithms given here.

1.2. The abelian case. The easiest and well-known case is where we deal with abelian groups. Then the abelian free group is well described as a group of linear forms over a ring of integers. The subgroup generated by the left sides of relations (1.1.1) is an abelian free group. One can easily compute in an effective way the basis of this subgroup. The knowledge of the basis allows us to decide the word problem, the inclusion problem (the question whether an element belongs to a given subgroup) and the finiteness problem by simple arithmetic computations. The required computations are such as are used in linear algebra for solving equations with integral coefficients, finding the greatest common divisor, and so on.

1.3. Generalizations to the case of nilpotent groups. The idea explained in 1.2 is used in this paper for constructing the algorithms for nilpotent groups.

⁽¹⁾ For the exact meaning of this phrase, see 1.4 and 4.1.

The theory of basic commutators developed by M. Hall [1], gives the standard form of elements in a nilpotent free group. This allows us to decide the word problem in this case.

The subgroup theorem given in section 3 of this paper is a strict analogue of the subgroup theorem for abelian free groups. This permits the construction, described in section 4, of algorithms for deciding the word problem, the inclusion problem, and the finiteness problem for any class of nilpotent groups with a given bound of nilpotency. The algorithms are *mutatis-mutandis* generalizations of algorithms from the abelian case.

1.4. Possible applications to automatic decisions. In recent years some successful experiments were done by Hao Wang, Gelertner, and others in so-called automatical proving of theorems in lower predicate calculus and in some fragments of geometry. The author believes that the algorithms presented in this paper can be used for deciding automatically (i.e. by a digital computer) the word problem, the inclusion problem and the finiteness problem in the case of nilpotent groups of a given nil (degree of nilpotency). The author supposes that a successful programming of the algorithms on a digital computer can be done, and the computations realised.

1.5. Notions and notation. The terminology of this paper is the same as in M. Hall's book [1]. It is supposed that the reader is familiar with the theory of basic commutators presented in chapter 11 of this book. But some examples are given, mostly in section 2, for explaining the main differences and the main similarities between the abelian case and the case of nilpotent groups.

At the end of this introduction the author wishes to express his gratitude to professor J. Łoś for the helpful suggestions and remarks offered during the preparation of this paper and for the scholarship which I was granted by the Institute of Mathematics of the Polish Academy of Sciences.

2. Nilpotent groups.

2.1. Nilpotent free groups. The variety of nilpotent groups of nil c is composed of all groups satisfying the law $(y_1, \dots, y_{c+1}) = 1$ (an identical relation), where

$$(y_1, y_2) = y_1^{-1} y_2^{-1} y_1 y_2 \quad \text{and} \quad (y_1, \dots, y_n, y_{n+1}) = ((y_1, \dots, y_n), y_{n+1}).$$

The free groups in that variety (i.e. nilpotent free groups of nil c) can be represented as factor groups $F(X)/V^{F(X)}$, where $F(X)$ is the free group (absolutely free group), freely generated by set X , and $V^{F(X)}$ is a word subgroup generated by the set V composed from the word (y_1, \dots, y_{c+1}) .

2.2. Normal bases. A set g_1, \dots, g_t of elements of a group G is called a *normal basis* of G iff any element $g \in G$ can be uniquely represented as

$$(2.2.1) \quad g = g_1^{a_1} \cdot g_2^{a_2} \dots g_t^{a_t} \quad \text{where} \quad a_1, a_2, \dots, a_t \text{ are integers.}$$

For instance, in any abelian free group, a free generating set is an example of a normal basis. Nilpotent free groups are examples of non-commutative groups with normal bases.

2.3. Basic commutators. The notion of basic commutators was introduced by M. Hall, cf. [1], Chapter 11. We shall omit the definition and the theory of basic commutators; to this notion and to notations we refer the reader to the book of M. Hall just cited.

In the nilpotent free group $G(x_1, \dots, x_n)$, freely generated by x_1, \dots, x_n , basic commutators in x_1, \dots, x_n will be denoted by c_1, c_2, \dots, c_t . Their number t is a function of n and the nil c of the group:

$$t = \sum_{s=1}^c \sum_{d|s} \frac{1}{s} \mu(d) n^{s/d}.$$

where $\mu(d)$ is a Möbius function on integers, cf. [1] or [2].

The basic commutators c_1, \dots, c_t form a normal basis of the group. Any element g of the group can be uniquely expressed as

$$(2.3.1) \quad g = c_1^{a_1} \cdot c_2^{a_2} \dots c_t^{a_t}.$$

The correspondence between the element g of the group $G(x_1, \dots, x_n)$ and the t -tuple $[a_1, a_2, \dots, a_t]$ given by formula (2.3.1) is one-to-one. This allows us to use the notation of elements of $G(x_1, \dots, x_n)$ as t -tuples $[a_1, a_2, \dots, a_t]$ of integers.

M. Hall has proved that a correspondence like the above is recursive. Strictly speaking, when we have a word $f(x_1, \dots, x_n)$ of the free group $F(x_1, \dots, x_n)$ presenting an element $g = [a_1, a_2, \dots, a_t]$ of $G(x_1, \dots, x_n)$, then the function leading from $f(x_1, \dots, x_n)$ to the t -tuple $[a_1, \dots, a_t]$ is recursive. A process which Hall calls the collecting process gives an algorithm for computing the function. For a detailed description of the collecting process cf. [1] or [2]. The algorithm is most suitable for Turing machines.

P. Hall in [2] has proved that if

$$a = c_1^{a_1} \cdot c_2^{a_2} \dots c_t^{a_t} = [a_1, \dots, a_t], \\ b = c_1^{b_1} \cdot c_2^{b_2} \dots c_t^{b_t} = [b_1, \dots, b_t],$$

then the exponents $\bar{d}_1, \dots, \bar{d}_t$ in

$$a \cdot b = \bar{d} = c_1^{\bar{d}_1} \cdot c_2^{\bar{d}_2} \dots c_t^{\bar{d}_t}$$

and the exponents v_1, \dots, v_t in

$$a^m = v = c_1^{v_1} \cdot c_2^{v_2} \dots c_t^{v_t}$$

for an integer m are given by the formulas

$$(2.3.2) \quad \begin{aligned} d_i &= a_i + b_i + f_i(a_1, \dots, a_{i-1}, b_1, \dots, b_{i-1}), \\ v_i &= ma_i + h_i(a_1, \dots, a_{i-1}, m), \end{aligned}$$

where f_i and h_i are polynomials with rational coefficients, $i = 1, 2, \dots, t$ (f_1 and h_1 are understood to be zero). They are called *Hall polynomials*, *product* and *exponential*, respectively.

Since for any a and b in a group $a \cdot 1 = a$ and $1 \cdot b = b$, it follows from formulas (2.3.2) that

$$(2.3.3) \quad \begin{aligned} f_i(a_1, \dots, a_{i-1}, 0, \dots, 0) &= 0, \\ f_i(0, \dots, 0, b_1, \dots, b_{i-1}) &= 0 \end{aligned}$$

for $i = 1, 2, \dots, t$ and for any integers a_1, \dots, b_1, \dots . Moreover, from $1^m = 1$, for any integer m , we have

$$(2.3.4) \quad h_i(0, \dots, 0, m) = 0, \quad i = 1, 2, \dots, t.$$

These important formulas show how close is the case of nilpotent free groups to that of abelian free groups. The formulas imply that the operations $a \cdot b$ and a^m on presentations of elements as vectors $[a_1, \dots, a_t]$, i.e. on presentations (2.3.1), are additive and homogeneous up to the second non-zero coordinate. One can also easily deduce that the operation $(a, b) = a^{-1}b^{-1}ab$ is a zero operation up to the second non-zero coordinate of a (or b).

2.4. Example. Now we shall give an example explaining some parts of the theory of basic commutators, not developed here.

Let $G = G(x_1, x_2)$ be a nilpotent free group of nil 3, i.e. the group with the law $(y_1, y_2, y_3, y_4) = 1$. For $n = 2$, $c = 3$, the number t of basic commutators is 5. The basic commutators in x_1, x_2 are:

$$(2.4.1) \quad \begin{aligned} c_1 &= x_1, & c_2 &= x_2, & c_3 &= (x_2, x_1), \\ c_4 &= (x_2, x_1, x_1), & c_5 &= (x_2, x_1, x_2). \end{aligned}$$

Then any element $a \in G$ can be uniquely represented as:

$$(2.4.2) \quad a = x_1^{a_1} x_2^{a_2} (x_2, x_1)^{a_3} (x_2, x_1, x_1)^{a_4} (x_2, x_1, x_2)^{a_5},$$

where a_1, a_2, \dots, a_5 are integers. We shall write the presentation in the form

$$a = [a_1, \dots, a_5], \quad \text{or} \quad b = [b_1, \dots, b_5]$$

for another element $b \in B$. Then for

$$\begin{aligned} d &= a \cdot b = [d_1, \dots, d_5], \\ u &= a^{-1} = [u_1, \dots, u_5], \\ v &= a^m = [v_1, \dots, v_5], \\ w &= b^{-1}ab = a^b = [w_1, \dots, w_5], \\ k &= a^{-1}b^{-1}ab = (a, b) = [k_1, \dots, k_5], \end{aligned}$$

we shall compute Hall polynomials, for $n = 2$, and $c = 3$. This requires the use of the following formulas valid in any group:

$$(2.4.3) \quad x \cdot y = y \cdot x \cdot (x, y),$$

$$(2.4.4) \quad (y, x) = (x, y)^{-1};$$

$$(x \cdot y, z) = (x, z)^y (y, z) = (x, z)(x, z, y)(y, z),$$

$$(x, y \cdot z) = (x, z)(x, y)^z = (x, z)(x, y)(x, y, z),$$

$$(x, y^{-1}) = (y, x)^{y^{-1}},$$

$$(x^{-1}, y) = (y, x)^{x^{-1}}.$$

We shall give only the final results of the computation, i.e.: The product polynomials:

$$d_1 = a_1 + b_1,$$

$$d_2 = a_2 + b_2,$$

$$d_3 = a_3 + b_3 + a_2 b_1,$$

$$d_4 = a_4 + b_4 + a_3 b_1 + 1/2(a_2 b_1 (b_1 - 1)),$$

$$d_5 = a_5 + b_5 + a_3 b_2 + 1/2(a_2 b_1 (a_2 - 1)) + a_2 b_1 b_2.$$

The exponence polynomials:

$$v_1 = ma_1,$$

$$v_2 = ma_2,$$

$$v_3 = ma_3 + \frac{m(m-1)}{2} a_2 a_1,$$

$$v_4 = ma_4 + \frac{m(m-1)}{2} a_3 a_1 - 1/4(m(m-1)) a_2 a_1 + 1/12(m(m-1)(2m-1)) a_2 a_1 a_1,$$

$$v_5 = ma_5 + \frac{m(m-1)}{2} a_3 a_2 - 1/4(m(m-1)) a_2 a_1 + 1/12(m(m-1)(4m+1)) a_2 a_1 a_2.$$

From these polynomials we can compute as a special case: The inverse polynomials:

$$\begin{aligned} u_1 &= -a_1, \\ u_2 &= -a_2, \\ u_3 &= -a_3 + a_2 a_1, \\ u_4 &= -a_4 + a_3 a_1 - 1/2(a_2 a_1(a_1 + 1)), \\ u_5 &= -a_5 + a_3 a_2 - 1/2(a_2 a_1(a_2 + 1)). \end{aligned}$$

The conjugacy polynomials:

$$\begin{aligned} w_1 &= a_1, \\ w_2 &= a_2, \\ w_3 &= a_3 + (a_2 b_1 - a_1 b_2), \\ w_4 &= a_4 + (a_3 b_1 - b_2 a_1) + 1/2(a_2 b_1(b_1 - 1) - b_2 a_1(a_1 - 1)), \\ w_5 &= a_5 + (a_3 b_2 - b_2 a_2) + (a_2 b_1 b_2 - b_2 a_1 a_2) + \\ &\quad + 1/2(a_2 b_1(a_2 - 1) - b_2 a_1(b_2 - 1)). \end{aligned}$$

The commutator polynomials

$$\begin{aligned} k_1 &= 0, \\ k_2 &= 0, \\ k_3 &= a_2 b_1 - a_1 b_2, \\ k_4 &= (a_3 b_1 - b_2 a_1) + 1/2(a_2 b_1(b_1 - 1) - b_2 a_1(a_1 - 1)), \\ k_5 &= (a_3 b_2 - b_2 a_2) + (a_2 b_1 b_2 - b_2 a_1 a_2) + 1/2(a_2 b_1(a_2 - 1) - b_2 a_1(b_2 - 1)). \end{aligned}$$

2.5. Lemmas on presentations of nilpotent groups. Now we shall prove the following lemma.

LEMMA 1. *Let G be a nilpotent group of nil c , generated by a finite set $X = (x_1, \dots, x_n)$; then for any subset R of G the normal closure $N(R)$ of the set R is a subgroup generated by the following set R^* composed of the elements*

$$(2.5.1) \quad r, (r, x_{j_1}^{\varepsilon_1}), \dots, (r, x_{j_1}^{\varepsilon_1}), \dots, (r, x_{j_1}^{\varepsilon_1}, \dots, x_{j_{c-1}}^{\varepsilon_{c-1}})$$

where r ranges over R , j_a ranges over $1, \dots, n$ for $a = 1, \dots, c-1$, and the exponents ε range over ± 1 , independently.

In other words, for a set R of relations of the group, to obtain a generating set of the normal closure of R (i.e. the set of all relations of the group) we must: firstly join with R all commutators of elements of R , commuted with generators of the group of powers ± 1 ; secondly, to join the commutators of elements from the set just obtained, commuted with generators of the group of powers ± 1 ; thirdly repeat the

operation as regards joining the last non-vanishing commutators, i.e. the commutators of length c , where c is the nilpotency of the group.

An immediate corollary to this lemma is

LEMMA 2. *For nilpotent groups the normal closure of a finite set is generated by the finite set explicitly given by formula (2.5.1).*

Proof of Lemma 1. It is evident that $R^* \leq N(R)$. Now it remains to prove that for any $f \in G$ and any $r \in R$ the element $f^{-1}rf$ can be generated by the set R^* . Let

$$f = x_{a_1}^{n_1} x_{a_2}^{n_2} \dots x_{a_p}^{n_p}; \quad a_1, \dots, a_p \in (1, \dots, n).$$

The proof is by induction on $m = |n_1| + |n_2| + \dots + |n_p|$.

For $m = 1$, we have $f = x_j^\varepsilon$, where $\varepsilon = \pm 1$. Then

$$x_j^{-\varepsilon} r x_j^\varepsilon = r \cdot (r, x_j^\varepsilon) \in \{R^*\}.$$

We now present $f = x_{a_1}^{n_1} x_{a_2}^{n_2} \dots x_{a_p}^{n_p} = x_{a_1}^{n_1} \cdot f'$. By the inductive assumption, the hypothesis is true for f' , since $|n_1 - \varepsilon| + \dots + |n_p| = m - 1$. By a suitable formula (2.4.4),

$$(r, f) = (r, x_{a_1}^\varepsilon \cdot f') = (r, x_{a_1}^\varepsilon) (r, f')^{x_{a_1}^\varepsilon}.$$

Evidently $(r, x_{a_1}^\varepsilon) \in R^*$. Now by the inductive assumption $(r, f') \in \{R^*\}$, and so there exist a $u_1, \dots, u_s \in R^*$ and a $\mu_1 = \pm 1, \dots, \mu_s = \pm 1$ such that

$$(r, f') = u_1^{\mu_1} \dots u_s^{\mu_s}.$$

By the last equality, in order to prove that $(r, f)^{x_{a_1}^\varepsilon} \in \{R^*\}$, it remains to prove that for any $u \in R^*$ and $x \in X \cup X^{-1}$ both $(u^{-1})^x$ and u^x belong to $\{R^*\}$. By formulas (2.4.2),

$$(u^{-1})^x = x^{-1} u^{-1} x = (x, u) \cdot u = (u, x)^{-1} \cdot u.$$

Now since $u \in R^*$, we have that $(u, x) \in \{R^*\}$ or equals 1. In both cases $(u^{-1})^x \in \{R^*\}$. Evidently $u^x = u \cdot (u, x) \in \{R^*\}$.

Thus we have proved that for f of length m is $(r, f) \in \{R^*\}$, and consequently $f^{-1} r f \in \{R^*\}$. The proof is finished by induction.

Thus we have proved that $N(R) = \{R^*\}$, as required in lemma 1.

Now we shall prove a lemma of a similar character.

LEMMA 3. *Let G be any group generated by a set X , finite or not. Let V_m be a set consisting of a single word (y_1, \dots, y_m) . Then the word subgroup V_m^G is a normal closure of the set R_m of elements of the form*

$$(2.5.2) \quad (x_{a_1}, \dots, x_{a_m}) \quad \text{for any } x_{a_1}, \dots, x_{a_m} \in X.$$

The lemma shows that the law $(y_1, \dots, y_m) = 1$, i.e. an identical relation in a group, is equivalent to a finite number of relations between

generators in the case of the group being finitely generated by a set X . The relations are

$$(w_{a_1}, \dots, w_{a_m}) = 1 \quad \text{for any } w_{a_1}, \dots, w_{a_m} \in X.$$

The proof of the lemma is by induction on m . For $m = 1$, the set V_1 consists of a single word y_1 . Since $R_1 = X$ and $V_1^G = G$, this is a trivial case.

Suppose the lemma is proved for $m-1$. The set of elements of the form

$$(2.5.3) \quad (f_1(X), \dots, f_{m-1}(X), f_m(X)) = ((f_1(X), \dots, f_{m-1}(X)), f_m(X)),$$

where $f_1(X), \dots, f_m(X)$ are any words in X , generates the subgroup V_m . It must be proved that any element (2.5.3) belongs to $N(R_m)$. By the inductive assumption $f = (f_1(X), \dots, f_{m-1}(X)) \in N(R_{m-1})$. This means that there exists $\tau_1, \dots, \tau_k \in R_{m-1}$ such that

$$f = (\tau_1^{\varepsilon_1})^{g_1} \dots (\tau_k^{\varepsilon_k})^{g_k}$$

for some $\varepsilon_i = \pm 1$, and $g_i \in G$ for $i = 1, \dots, k$.

First we shall prove that there exist words $s_i(X)$ in variables in X and elements h_i of G and $\mu_i = \pm 1$, $i = 1, \dots, k$, such that

$$(2.5.4) \quad (f_1, \dots, f_m) = (f, f_m) = [(\tau_1, s_1^{h_1})^{\mu_1} \dots [(\tau_k, s_k)^{h_k \mu_k}]]$$

The proof is by induction on k , with the use of formulas (2.4.2).

For $k = 1$:

$$(2.5.5) \quad ((\tau_1^{\varepsilon_1})^{g_1}, f_m) = (\tau_1^{\varepsilon_1}, f_m^{\sigma_1^{-1}})^{g_1}.$$

For $\varepsilon_1 = +1$,

$$s_1(X) = f_m(X)^{\sigma_1^{-1}}, \quad h_1 = g_1, \quad \mu_1 = +1.$$

For $\varepsilon_1 = -1$, from formula (2.5.5) and a suitable formula (2.4.2) we have

$$((\tau_1^{\varepsilon_1})^{g_1}, f_m) = (f_m^{\sigma_1^{-1}}, \tau_1)^{\tau_1^{-1} \cdot g_1} = [(\tau_1, f_m^{\sigma_1^{-1}})^{-1} \cdot \sigma_1]^{-1},$$

which gives

$$s_1(X) = f_m(X)^{\sigma_1^{-1}}, \quad h_1 = \tau_1^{-1} \cdot g_1, \quad \mu_1 = -1.$$

The step from $k-1$ to k easily follows from the formula

$$(((\tau_1^{\varepsilon_1})^{g_1} \dots (\tau_{k-1}^{\varepsilon_{k-1}})^{g_{k-1}})^{\sigma_1^{-1}}, f_m) = \{((\tau_1^{\varepsilon_1})^{g_1} \dots (\tau_{k-1}^{\varepsilon_{k-1}})^{g_{k-1}}), f_m\}^{\sigma_1^{-1} \cdot g_k} \cdot ((\tau_k^{\varepsilon_k})^{g_k}, f_m)$$

and from the case $k = 1$.

To finish the induction on m it now remains to prove, by (2.5.4), that $(\tau, s) \in N(R_m)$ for any $\tau \in R_{m-1}$ and any $s \in G$. This is quite easy by induction on the length of $s(X) = s$ with the use of formulas (2.4.2).

Let $s(X) = x_{a_1}^{\varepsilon_1} \dots x_{a_l}^{\varepsilon_l}$; $x_{a_1}, \dots, x_{a_l} \in X$, $\varepsilon_i = \pm 1$, for $i = 1, \dots, l$. For $l = 1$, in the case of $s(X) = x_{a_1}$

$$(\tau, s) = (\tau, x_{a_1}) \in R_m, \quad \text{since } \tau \in R_{m-1}.$$

In the case of $s(X) = x_{a_1}^{-1}$ we have

$$(\tau, s(X)) = (\tau, x_{a_1}^{-1}) = ((\tau, x_{a_1})^{\sigma_{a_1}^{-1}})^{-1} \in N(R_m).$$

If $(\tau, s_1) \in N(R_m)$ for any $\tau \in R_{m-1}$ and any s_1 of length $l-1$, then

$$(\tau, s) = (\tau, x_{a_1}^{\varepsilon_1} \dots x_{a_l}^{\varepsilon_l}) = (\tau, x_{a_1}^{\varepsilon_1}) \cdot (\tau, x_{a_1}^{\varepsilon_1} \dots x_{a_{l-1}}^{\varepsilon_{l-1}})^{\sigma_{a_1}^{\varepsilon_1}} \in N(R_m)$$

since both $(\tau, x_{a_1}^{\varepsilon_1})$ and $(\tau, x_{a_1}^{\varepsilon_1} \dots x_{a_{l-1}}^{\varepsilon_{l-1}})$ belong to $N(R_m)$ by the inductive assumption.

Now the proof is complete.

3. Subgroup theorem.

3.1. Formulation of the theorem. In the next section we prove a theorem concerning subgroups of groups with normal bases. The theorem is a very natural generalization of the subgroup theorem for abelian free groups. In the proof some properties of a normal basis of the group are assumed. They are all listed below, and are called *assumptions I* in the sequel.

ASSUMPTIONS I. The group G has a normal basis c_1, \dots, c_t , i.e. any element $a \in G$ can be uniquely expressed as

$$a = c_1^{a_1} \cdot c_2^{a_2} \cdot \dots \cdot c_t^{a_t}, \quad \text{where } a_1, \dots, a_t \text{ are integers.}$$

(We shall write for the sake of brevity $a = [a_1, a_2, \dots, a_t]$.) The basis has the following properties:

If $a = c_i^{a_i} \cdot c_{i+1}^{a_{i+1}} \cdot \dots \cdot c_t^{a_t}$ and $b = c_i^{b_i} \cdot c_{i+1}^{b_{i+1}} \cdot \dots \cdot c_t^{b_t}$ then, for $d = a \cdot b = [d_1, \dots, d_t]$ and $v = a^{-1} = [v_1, \dots, v_t]$, $d_1 = d_2 = \dots = d_{i-1} = 0$, $d_i = a_i + b_i$ and d_{i+1}, \dots, d_t depends on a and b in a more complicated way; $v_1 = v_2 = \dots = v_{i-1} = 0$, $v_i = -a_i$ and v_{i+1}, \dots, v_t depends on a in a more complicated way.

If $a = c_i^{a_i} \cdot c_{i+1}^{a_{i+1}} \cdot \dots \cdot c_t^{a_t}$ and b is any element of G , or if $b = c_i^{b_i} \cdot c_{i+1}^{b_{i+1}} \cdot \dots \cdot c_t^{b_t}$ and a is any element of G , then for $(a, b) = k = [k_1, \dots, k_t]$ we have $k_1 = k_2 = \dots = k_{i-1} = k_i = 0$ and k_{i-1}, \dots, k_t depends in a certain, possibly complicated way on a and b .

Note that the last property implies the nilpotency of the group.

We now give the subgroup theorem.

THEOREM 1. (The subgroup theorem.) *If a group G satisfies assumptions I according to the normal basis c_1, \dots, c_t , then any subgroup H has a normal basis u_1, \dots, u_s , $s \leq t$, i.e. any $u \in H$ can be uniquely represented as*

$$(3.1.1) \quad u = u_1^{a_1} \cdot u_2^{a_2} \cdot \dots \cdot u_s^{a_s}.$$

Moreover, the basis u_1, \dots, u_s can be chosen in such a way that

$$\begin{aligned}
 (3.1.2) \quad u_1 &= c_1^{a_{11}} \cdot c_2^{a_{12}} \cdot \dots \cdot c_t^{a_{1t}} = [a_{11}, a_{12}, \dots, a_{1t}], \\
 u_2 &= c_2^{a_{22}} \cdot \dots \cdot c_t^{a_{2t}} = [0, a_{22}, \dots, a_{2t}], \\
 &\dots \dots \dots \\
 u_s &= c_s^{a_{ss}} \cdot \dots \cdot c_t^{a_{st}} = [0, 0, \dots, a_{ss}, \dots, a_{st}].
 \end{aligned}$$

3.2. Proof of the subgroup theorem. The proof given here is under assumptions I from the previous section, which are used in almost every step of the proof. Therefore we shall not mention the use of them. As below, the proof is by the construction of u_1, \dots, u_s starting from any generators h_1, \dots, h_k of H . But the construction can be done, with only small changes, even if we start from an infinite set of generators of H . The inequality $s \leq t$ follows in any case from (3.1.2).

Proof. The theorem is true if H is a subgroup of a cyclic group generated by c_t , i.e. if $H \leq \{c_t\}$. Then

$$h_1 = c_t^{b_1}, h_2 = c_t^{b_2}, \dots, h_k = c_t^{b_k}.$$

If we take $d = \text{GCD}(b_1, \dots, b_k)$, then there exist integers l_1, \dots, l_k such that $d = l_1 b_1 + \dots + l_k b_k$. Then for $u_1 = h_1^{l_1} \dots h_k^{l_k} = c_t^{l_1 b_1 + \dots + l_k b_k} = c_t^d$ we have $\{u_1\} = H$, and (3.1.1) and (3.1.2) holds.

To form an inductive proof we assume that the theorem is true for any $H' \leq \{c_{m+1}, \dots, c_t\}$, and we shall prove it in the case where $H \leq \{c_m, c_{m+1}, \dots, c_t\}$. Then

$$\begin{aligned}
 h_1 &= c_m^{b_1} \cdot c_{m+1}^{d_1} \dots c_t^{f_1}, \\
 &\dots \dots \dots \\
 h_k &= c_m^{b_k} \cdot c_{m+1}^{d_k} \dots c_t^{f_k}.
 \end{aligned}$$

If $b_1 = \dots = b_k = 0$, then $H \leq \{c_{m+1}, \dots, c_t\}$. There remains the case where a certain b differs from zero. Define $d = \text{GCD}(b_1, \dots, b_k)$, l_1, \dots, l_k as before; so $l_1 b_1 + \dots + l_k b_k = d$. Write $h = h_1^{l_1} \dots h_k^{l_k}$. By the properties assumed by assumptions I:

$$(3.2.1) \quad h = c_m^d \cdot c_{m+1}^e \dots c_t^f,$$

where d is the d defined before, and e, \dots, f depend on the coordinates in a more complicated way. Now, for: $m_1 = b_1/d, \dots, m_k = b_k/d$, the elements

$$(3.22) \quad h, h'_1 = h^{-m_1} \cdot h_1, \dots, h'_k = h^{-m_k} \cdot h_k$$

form a generating set of H .

In our procedure it is to construct explicitly a finite generating set of the normal closure H' in H of the set h'_1, \dots, h'_k . As we shall prove below, H' is generated by the set

$$(3.2.3) \quad h'_1, \dots, h'_k, (h'_1, h), \dots, (h'_k, h), \dots, (h'_1, h, \dots, h)_{c-1 \text{ times}}, \dots, (h'_k, h, \dots, h)_{c-1 \text{ times}}.$$

Since (2.2.3) is contained in H' , it remains to prove that for any f from (2.2.3) both $h^{-1}fh$ and hfh^{-1} are generated by elements (3.2.3). Since $h^{-1}fh = f \cdot (f, h)$ and (f, h) belongs to (3.2.3) or is equal 1, it remains to prove that hfh^{-1} is generated by elements (3.2.3). One can easily check the following formula $hfh^{-1} = f \cdot (f, h^{-1}) = f \cdot (f_1, h^{-1})^{-1} \cdot f_1^{-1} = ff_2 \cdot (f_2, h^{-1}) f_1^{-1}$, where $f_1 = (f, h)$ and $f_2 = (f_1, h)$. Let us define $f_{i+1} = (f_i, h)$, then by successive application of the former formula, we obtain $hfh^{-1} = ff_2 f_4 \dots f_s^{-1} f_1^{-1}$. Since f, f_1, f_2, \dots are elements from (3.2.3), or elements equal 1 (e.g. for sufficiently large indices), the proof is finished.

Now we shall continue the proof of the theorem.

By (3.2.2) since (3.2.1), according to the assumptions I, all elements (3.2.3) belong to $\{c_{m+1}, \dots, c_t\}$. This proves that $H' \leq \{c_{m+1}, \dots, c_t\}$. Moreover, by the definition of the elements (3.2.3), the subgroup H' is a normal subgroup of H .

By the inductive assumption H' has a basis with the required properties. Adding to the basis the element h , defined by (3.2.1), we obtain a normal basis of H (i.e. a basis satisfying (3.1.1)) with property (3.1.2). This completes the proof of the theorem.

3.3. Some remarks concerning the subgroup theorem. If we deal with a nilpotent free group of a given nil and an explicitly given set X of free generators x_1, \dots, x_n , then the basic commutators c_1, \dots, c_t form a normal basis with the properties listed in assumptions I (cf. section 2.3). Thus the subgroup theorem can be applied to a nilpotent free group.

In this case, if we start from h_1, \dots, h_k explicitly given as words in generators x_1, \dots, x_n , the construction of a normal basis u_1, \dots, u_s of $H = \{h_1, \dots, h_k\}$ described in the proof of the theorem is effective. Precise considerations of the effective question are given in section 4.1. Here we shall give only an example of effective calculation. We shall compute the normal basis with property (3.1.2), for a subgroup H , of a group from the example given in section 2.4. Let H be generated by $h_1 = x_1^3 x_2$ and $h_2 = x_1^3 x_2^3$. Then

$$h_1 = [3, 1, 0, 0, 0], \quad h_2 = [3, 3, 0, 0, 0]$$

is a presentation in basic commutators c_1, \dots, c_5 (cf. (2.4.1) and (2.4.2)).

The $\text{GCD}(3, 3) = 1 \cdot 3 + 0 \cdot 3$. This gives the element (3.2.1), $h = h_1^1 \cdot h_2^0 = h_1$. The elements (3.2.2) are

$$h = h_1, \quad h'_1 = 1, \quad h'_2 = x_2^2 = [0, 2, 0, 0, 0].$$

The generating system of H' given by (3.2.3) is

$$(3.3.1) \quad h'_1 = 1, \quad h'_2 = x_2^2, \quad (h'_1, h), \quad (h'_2, h), \quad (h'_1, h, h), \quad (h'_2, h, h).$$

Elements equal to unity can be omitted, as well as recurrent elements. For the next operations the normal form of the elements must be calculated. After a simple computation we obtain

$$(3.3.2) \quad (h'_2, h) = (x_2^2, x_1^3 \cdot x_2) = (x_2, x_1)^6 (x_2, x_1)^6 (x_2, x_1, x_2)^9, \\ (h'_2, h, h) = ((x_2, x_1)^6 (x_2, x_1)^6 (x_2, x_1, x_2)^9, x_1^3 \cdot x_2) = (x_2, x_1, x_1)^{18} (x_2, x_1, x_2)^6.$$

These are the normal forms of the elements. Using the square bracket notation, we have the normal form of elements (3.3.1) as

$$(3.3.3) \quad h = [0, 2, 0, 0, 0], \quad (h'_2, h) = [0, 0, 6, 6, 9], \\ (h'_2, h, h) = [0, 0, 0, 18, 6].$$

No further calculation is required, since in this special example the elements (3.3.3) form a basis with properties (3.1.1) and (3.1.2). Adding to elements (3.3.3) the element h , we obtain a normal basis of the whole subgroup H , satisfying (3.1.1), with a triangular matrix in (3.1.2)

$$u_1 = h = h_1 = [3, 1, 0, 0, 0], \quad u_2 = h'_2 = [0, 2, 0, 0, 0], \\ u_3 = (h'_2, h) = [0, 0, 6, 6, 9], \quad u_4 = (h'_2, h, h) = [0, 0, 0, 18, 6].$$

4. Some effective algorithms for the decision procedure.

4.1. Effectiveness of the construction from theorem 1.

Now we shall analyse the effectiveness problem of the construction of u_1, \dots, u_s given in the proof of theorem 1 for nilpotent free groups.

First let us observe that if we have a finite generating set X of a nilpotent free group, then the construction of basic commutators c_1, \dots, c_t in variables in X is effective. The construction is explicitly given in M. Hall's book [1] (cf. also [2]). The collecting process of M. Hall, described there, gives an effective method of the computation of presentation (2.3.1), for any $g \in G$ given as a word in X . I believe that the Turing machine is an extremely good tool for describing the algorithm giving the collecting process. The action of the machine can be simulated by a digital computer. In this way we can hope to obtain a practical method of calculating presentation (2.3.1) for words in X , if n, c , and the length of the calculated word are not very large.

An alternative way of calculating presentation (2.3.1) is to begin by calculating Hall's polynomials. A systematic method of calculating

the polynomials is given in [2]. The knowledge of the polynomials reduces the calculation of presentation (2.3.1) to simple arithmetic operations. This method was implicitly used in example 3.3.

If the group G is nilpotent free of nil c , freely generated by a finite explicitly given set X , the proof of theorem 1, given in 3.2, describes an algorithm of constructing the matrix of (3.1.2) for any h_1, \dots, h_k given as words in X . The algorithm requires the following operations:

- finding the basic commutators for the given n and c ;
- calculation of the presentation (2.3.1);
- simple arithmetic operations, such as addition and multiplication;
- finding a GCD of integers, and so on.

Thus the algorithm can be programmed on a digital computer. In general we cannot hope that the computer shall calculate the result. The number of data to be stored by the computer during the calculation can exceed the number of places in the storage, or the number of operations to be made by the computer can make the calculation take up an absurdly long time. But the author believes that when n, c , and the maximum length of h_1, \dots, h_k are small numbers, the calculation can be effectively done. This cannot be verified until a routine on some computer is prepared, and a model calculation is done.

4.2. An effective algorithm for the inclusion problem.

Now we shall give an effective algorithm, based on the subgroup theorem (theorem 1) for solving the inclusion problem for nilpotent groups. In this section we shall investigate the algorithm in the case where the group is nilpotent free of a given nil.

We must construct an algorithm to decide for any words f, h_1, \dots, h_k , whether or not

$$f(x_1, \dots, x_n) \in \{h_1(x_1, \dots, x_n), \dots, h_k(x_1, \dots, x_n)\} = H$$

holds in the nilpotent free group G generated by the set $X = (x_1, \dots, x_n)$.

Description of the algorithm. At first we find for h_1, \dots, h_k a system u_1, \dots, u_s with properties (3.1.1) and (3.1.2) from theorem 1. An algorithm for this procedure is described in the proof of theorem 1; cf. also 3.3 and 4.1.

Then we find a presentation

$$(4.2.1) \quad f = c_1^{b_1} \cdot c_2^{b_2} \dots c_t^{b_t}$$

of f . The procedure to decide whether or not $f \in H$ is by recursion on a number m such that the first $t-m$ coefficients b in (4.2.1) are zeros, i.e. on the smallest m such that $f \in \{c_{t-m+1}, \dots, c_t\}$.

For $m = 0$, all $b_1 = \dots = b_t = 0$ then $f \in H$, since $f = 1$ in the group G . If we have a decision procedure whether or not $f \in H$, for any $f \in \{c_{t-m+1}, \dots, c_t\}$, then for any $f^* \in \{c_{t-m}, \dots, c_t\}$ the procedure is as follows:

Let $f^* = c_{t-m}^{b_{t-m}} \dots c_t^{b_t}$. The element $f^* \in H$ iff either $f^* = 1$ or $t-m \leq s$ and moreover there exist integers d_{t-m}, \dots, d_s such that

$$f^* = u_{t-m}^{d_{t-m}} \dots u_s^{d_s}.$$

According to (3.1.2), this gives

$$f^* = (c_{t-m}^{a_{t-m,t-m}} \dots c_t^{a_{t-m,t}})^{d_{t-m}} \dots (c_s^{a_{ss}} \dots c_t^{a_{st}})^{d_s}$$

or

$$(4.2.2) \quad f^* = c_{t-m}^{a_{t-m,t-m} d_{t-m}} \cdot c_t^{a'_{t-m+1}} \dots c_t^{a'_t} = c_{t-m}^{b_{t-m}} \dots c_t^{b_t}$$

where the coefficient of c_{t-m} is $a_{t-m,t-m} \cdot d_{t-m} = b_{t-m}$, and the coefficients of c_{t-m+1}, \dots, c_t are

$$a'_{t-m+1} = b_{t-m+1}, \dots, a'_t = b_t.$$

Now if $a_{t-m,t-m}$ does not divide b_{t-m} , then we decide that f^* does not belong to H . If $a_{t-m,t-m}$ divides b_{t-m} , then the formula (4.2.2) does not give us a decision procedure for deciding whether or not $f^* \in H$, since a'_{t-m+1}, \dots, a'_t depends on undetermined coefficients d_{t-m+1}, \dots, d_t . But we can do as follows: First we determine $d_{t-m} = b_{t-m}/a_{t-m,t-m}$ (or $d_{t-m} = 0$ when both b_{t-m} and $a_{t-m,t-m}$ are zeros). Then

$$f = f^* \cdot u_{t-m}^{-d_{t-m}}$$

belongs to $\{c_{t-m+1}, \dots, c_t\}$. The decision procedure for f gives a decision procedure for f^* .

4.3. Inclusion problem. In this section we shall give an algorithm for solving the inclusion problem for any nilpotent group when the nilpotency of the group is given. The algorithm is based on an algorithm given in 4.2 for nilpotent free groups.

When having a finite set X of generators and a finite set R of words in elements of X , we deal with a presentation of a group in generators from X and relations $r(x_1, \dots, x_n) = 1$ for $r \in R$.

For applications of the algorithm we must know that the group with the presentation in question is nilpotent of a nil at most c ; thus the group can be presented as a factor group of the nilpotent free group of nil c generated by the set X , by a normal closure of the set R of relations.

The inclusion problem consists in deciding for any X and R as above and for any words f, h_1, \dots, h_s in X whether or not

$$(4.3.1) \quad f \in \{h_1, \dots, h_s\}.$$

This is equivalent to

$$(4.3.2) \quad f \in \{h_1, \dots, h_s, R^*\} = H$$

in the nilpotent free group of nil c , where R^* is a finite set explicitly given by formula (2.5.1) (cf. lemma 2). Indeed, $\{R^*\} = N(R)$, which gives $H = \{h_1, \dots, h_s\} \cdot N(R)$ when the normal closure is taken in a nilpotent free group. This proves the equivalence of (4.3.1) and (4.3.2).

For a nilpotent free group of nil c , there exists an algorithm for decision (4.3.2). This is the algorithm given in section 4.2.

Note that the inclusion problem in the special case where all h_1, \dots, h_s are trivial words is a word problem. Thus the algorithm given in this section solves both the inclusion problem and the word problem.

4.4. Finiteness problem. In this section we shall give an algorithm for solving the finiteness problem for nilpotent groups of a given nil. The algorithm is based on the algorithm given in the proof of theorem 1 (cf. sections 3.2 and 4.1). We start with some algebraic considerations.

A nilpotent group B is finite iff all abelian groups B_i/B_{i+1} are finite. Here B_i denotes an i th member of the lower central series, i.e. the series defined as follows:

$$B_1 = B, \quad B_{i+1} = (B, B_i) \quad \text{for } i = 1, 2, \dots$$

If $B = G/N$ where G is a nilpotent group of the same nil, then, by the Zassenhaus lemma and isomorphism theorem, since $B_i = G_i \cdot N/N = G_i/G_i \cap N$ we have

$$(4.4.1) \quad B_i/B_{i+1} = G_i \cdot N/N/G_{i+1} \cdot N/N = G_i \cdot N/G_{i+1} \cdot N = G_i/G_{i+1} \cdot (G_i \cap N).$$

The finiteness problem consists in deciding for any finite set X of generators and any finite set R of words in X whether or not the group generated by X , with the relations $r(x_1, \dots, x_n) = 1$ for $r \in R$, is finite.

Denote the group by B . If it is ensured that the nilpotency of B is equal or less than a given number c , then B is a factor group G/N where G is the nilpotent free group of nil c , generated by X , and N is the normal closure of R in G . Then by (4.4.1) we must decide whether or not all abelian groups $G_i/G_{i+1} \cdot (G_i \cap N)$; $i = 1, \dots, c$, are finite.

By lemma 1, we can effectively find, having R , the elements h_1, \dots, h_k which generates N . Let us now find for h_1, \dots, h_k the normal base u_1, \dots, u_s of the subgroup N of G , with properties (3.1.1) and (3.1.2). For the matrix given by (3.1.2)

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1t} \\ 0 & a_{22} & \dots & a_{2t} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{st} \end{bmatrix}$$

the vector space generated by strokes over the ring of integers will be denoted by $M(R)$. This is the subspace of the space O^t (the t -dimen-

sional space over the ring of integers). The quotient space $C^t/M(R)$ is isomorphic to the cartesian direct product of the abelian groups $G_i/G_{i+1} \cdot (G_i \cap N)$ for $i = 1, \dots, c$. The finiteness of the space $C^t/M(R)$ is equivalent to the rank of $M(R)$ equal t ($s = t$ and $a_{ii} \neq 0$ for $i = 1, \dots, t$).

The effectiveness of the construction of the matrix $M(R)$ (cf. 3.2 and 4.1) gives an algorithm to decide whether or not the rank of $M(R)$ is equal to t . This gives an algorithm to decide for any presentation for which the set X of generators and the set R of relations is finite, whether or not the group so presented is finite, if it is ensured that the nilpotency of the group is equal to or less than a given number c .

4.5. Final remarks. This final section is a continuation of the remarks contained in section 4.1.

In sections 4.2-4.4 the following two algorithms were described.

I. The algorithm for deciding the inclusion problem and the word problem relative to the class of all finite presentations of nilpotent groups of a given nil (described in 4.2-4.3).

II. The algorithm for deciding the finiteness problem relative to the same class as in I (described in 4.4).

The base, for both I, and II, was the algorithm of constructing a normal base for a subgroup of a nilpotent free group of a given nil. The algorithm was described in section 3.2, where the subgroup theorem was proved by giving the explicit method of the construction. A possibility of programming this algorithm for a computer was discussed in section 4.1.

The author believes that algorithms I and II can also be programmed for a computer.

The author does not know how deep is the interest of topology and other branches, in the practical possibility of deciding the word problem and the finiteness problem in such a narrow class of presentations as that for which the algorithms I and II are applicable. But he is glad that he has been able to construct algorithms, practical as he hopes, for a larger class of groups than the class of Abelian groups.

References

[1] M. Hall, *The theory of groups*, New York 1959.
 [2] P. Hall, *Nilpotent groups*, Canadian Mathematical Congress 1957, Litographed notes.
 [3] A. W. Mostowski, *On the decidability of some problems in special classes of groups*, Fund. Math. this volume, pp. 123-135.

On topologies for F^t

by

Michael Gemignani (Buffalo, N. Y.)

The terminology and propositions referred to by number are those of [1].

Let X be a space with geometry G of length $m-1 \geq 0$. The purpose of this paper is to investigate possible topologies on F^t , the set of i -flats of G . Two possible topologies of F^t are defined as follows:

I. Let $\{f^v\}_{v \in N}$ be a net of i -flats. Define $\overline{\lim} f^v = \{x \mid x \text{ is a limit point for some net } \{x_v\}_{v \in N}, x_v \in f^v\}$ and $\underline{\lim} f^v = \{x \mid \text{there is a net } \{x_v\}_{v \in N}, x_v \in f^v, \text{ with } x_v \rightarrow x\}$. We say that $f^v \rightarrow f$ if f is an i -flat and $\overline{\lim} f^v = \underline{\lim} f^v = f$.

II. Define $L_i(X) \subset X^{i+1}$ by $L_i(X) = \{(x_0, \dots, x_i) \in X^{i+1} \mid \{x_0, \dots, x_i\} \text{ is linearly independent in } X\}$. If $z = (x_0, \dots, x_i) \in L_i(X)$, let z^* denote $\{x_0, \dots, x_i\}$. For $w, z \in L_i(X)$, define $w \sim z$ if $f_i(w^*) = f_i(z^*)$. \sim is an equivalence relation. Let $Y_i = L_i(X)/\sim$ with the quotient topology. There is a natural map $p: Y_i \rightarrow F^i$ defined by $p(y) = f(y^*)$. p is obviously 1-1 and onto, hence topologize F^i so as to make p a homeomorphism.

II is clearly equivalent to

II'. Let $\{f^v\}_{v \in N}$ be a net of i -flats. Then $f^v \rightarrow f$ iff there is a basis $\{x_0^v, \dots, x_i^v\}$ for each f^v such that $(x_0^v, \dots, x_i^v) \rightarrow (x_0, \dots, x_i) = x$ in $L_i(X)$ and x^* is a basis for f .

That topology I is not necessarily the same as topology II is shown by the following example:

EXAMPLE 1. Let $X = \{(x, y) \in R^2 \mid x^2 + y^2 < 1\} \cup \{(x, y) \mid 1 \leq x \leq 2, y = 0\}$ and let X have geometry G_X induce from R^2 (with the usual Euclidean geometry). Consider the sequence of 1-flats $\{f^n\}_{n \in I}$ where $f^n = \{(x, y) \mid y = \frac{1}{n}x\} \cap X$. Then in topology I, this sequence fails to converge, but in topology II, $f^n \rightarrow f = \{(x, y) \mid y = 0\} \cap X$.

Example 2 shows that the topology defined by II is not always T_2 , even when X is.