Czechoslovak Mathematical Journal

Jaroslav Ježek

The lattice of equational theories. Part I: Modular elements

Czechoslovak Mathematical Journal, Vol. 31 (1981), No. 1, 127–152

Persistent URL: `http://dml.cz/dmlcz/101731`

Czechoslovak Mathematical Journal, 31 (106) 1981, Praha

THE LATTICE OF EQUATIONAL THEORIES PART I: MODULAR ELEMENTS

JAROSLAV JEŽEK, Praha

(Received November 2, 1979)

0. INTRODUCTION

An equational theory of type Δ is a set of equations (identities, ordered pairs of terms) of type Δ containing all its consequences. There are various papers devoted to the study of the lattice $\mathscr{L}_\Delta$ of equational theories of an arbitrary type Δ (or to the study of the lattice of varieties of Δ-algebras, which is antiisomorphic to $\mathscr{L}_\Delta$); some of them are listed in the bibliography at the end of this paper. The present treatise will be a continuation of this study. It will be divided into several parts. The present Part I brings the proof of a single result – the description of all modular elements of the lattice $\mathscr{L}_\Delta$, i.e. elements that are not the central elements of any subpentagon of $\mathscr{L}_\Delta$. Various aspects and consequences of this result will be contained in a further part of this treatise. The result is formulated in Theorems 4.1, 4.2 and 5.1. Theorems 4.1 and 4.2 solve the case of a small type, while in Theorem 5.1 nine conditions necessary and sufficient for an equational theory of a large type Δ to be a modular element of $\mathscr{L}_\Delta$ are formulated. The proof of 5.1 is divided into six sections; in Sections 6, 7 and 8 the necessity and in Sections 9, 10 and 11 the sufficiency of the nine conditions is proved. For every full set U of Δ-terms (i.e. a set of terms such that if $t \in U$ then $f(t) \in U$ and $u \in U$ for any substitution f and any term u extending t) we can define two equational theories M_U and N_U as follows: $(a, b) \in M_U$ iff a, b are terms such that either $a = b$ or $a, b \in U$; $(a, b) \in N_U$ iff either $a = b$ or $a, b \in U$ and a, b contain the same variables. It turns out that M_U and N_U are modular elements of $\mathscr{L}_\Delta$. Moreover, for any modular element T of $\mathscr{L}_\Delta$ (in the case of a large type Δ) there exists a full set U of terms such that T differs only "a little" from either M_U or N_U; in fact, T results from either M_U or N_U by adding a set of equations of the form $(a, p(a))$ where p is a permutation of the set of variables occurring in the term a. The following condition is necessary (but not sufficient) for T to be modular: for every term a, the set of the permutations p such that $(a, p(a)) \in T$ is a modular element of the subgroup lattice of the symmetric group over the (finite) set of variables occurring in a. For the description of all modular elements of $\mathscr{L}_\Delta$

it is thus necessary to know all modular elements of the subgroup lattice of the symmetric group over any finite set. These modular subgroups are described in Section 3. In Section 1 we give a brief formulation of some basic notions from equational logic that are necessary for our investigation. For a more detailed explanation of these notions see e.g. [3], [12], [13], [17].

1. BASIC NOTIONS FROM EQUATIONAL LOGIC

By a type we mean a set of operation symbols. Every operation symbol F is associated with a non-negative integer, called the arity of F. Symbols of arity n are called n-ary; for $n = 0, 1, 2$, n-ary symbols are called nullary, unary, binary. A type containing either at least one symbol of arity $\geqq 2$ or at least two unary symbols is said to be large; all the remaining types are said to be small.

We fix an infinite countable sequence $x_1, x_2, x_3, x_4, \ldots$ of symbols, called variables. The set of variables is denoted by V. For every type Δ, the set of Δ-terms is just the least set with the following two properties:

(i) every variable is a Δ-term;

(ii) if $n \geqq 0$, $F \in \Delta$ is an n-ary symbol and $t_1, \ldots, t_n$ are Δ-terms, then the inscription $F(t_1, \ldots, t_n)$ is a Δ-term, too.

Especially, every nullary symbol from Δ is a Δ-term. The set of Δ-terms is an absolutely free Δ-algebra over V (with respect to the operations defined in the natural way); it will be denoted by W_Δ. If the type Δ is fixed, we write W instead of W_Δ and call the elements of W terms; various similar conventions will be often used without explicit preliminary notice. If $F \in \Delta$ is unary and t is a term, then the term $F(t)$ will be sometimes denoted by Ft.

The length $\lambda(t)$ of a term t is defined as follows: if $t \in V$ then $\lambda(t) = 1$; if $t = F(t_1, \ldots, t_n)$ then $\lambda(t) = 1 + \lambda(t_1) + \ldots + \lambda(t_n)$.

For every term t, the set of subterms of t is defined in this way: if $t \in V$ then t is the only subterm of t; if $t = F(t_1, \ldots, t_n)$ then u is a subterm of t iff either $u = t$ or u is a subterm of at least one of the terms $t_1, \ldots, t_n$. The set of subterms of any term t is finite. By a proper subterm of t we mean a subterm of t different from t. The set of variables occurring in t, i.e. variables that are subterms of t, will be denoted by $\operatorname{var}(t)$; it is a finite subset of V. For every $x \in V$ and every term t we define a non-negative integer $P_x(t)$, called the number of occurrences of x in t, as follows: if $t = x$ then $P_x(t) = 1$; if $t \in V \setminus \{x\}$ then $P_x(t) = 0$; if $t = F(t_1, \ldots, t_n)$ then $P_x(t) = P_x(t_1) + \ldots + P_x(t_n)$. We have $x \in \operatorname{var}(t)$ iff $x \in V$ and $P_x(t) \neq 0$.

By a substitution (in W_Δ) we mean an endomorphism of the algebra W_Δ. Evidently, if f, g are two substitutions and $f(t) = g(t)$ for a term t, then $f(x) = g(x)$ for all $x \in \operatorname{var}(t)$.

For any set M, the identical permutation of M will be denoted by 1_M. If f is a mapping of a set $M \subseteq V$ into W_Δ, then the mapping $f \cup 1_{V \setminus M}$ can be uniquely extended to a substitution; this substitution will be denoted by $\bar{f}$ and we shall sometimes write $f\langle t\rangle$ instead of $\bar{f}(t)$. If x is a variable and u is a term, then the substitution $\bar{f}$, where f is the (unique) mapping of $\{x\}$ into $\{u\}$, will be denoted by σ_u^x. If $x \in V$ and $t, u \in W_\Delta$, we put $t_{(x)}[u] = \sigma_u^x(t)$; for every $k \geqq 0$ we define a term $t_{(x)}^{(k)}[u]$ by $t_{(x)}^{(0)}[u] = u$ and $t_{(x)}^{(k+1)}[u] = t_{(x)}[t_{(x)}^{(k)}[u]]$. If $\operatorname{var}(t) = \{x\}$, we put $t[u] = t_{(x)}[u]$ and $t^{(k)}[u] = t_{(x)}^{(k)}[u]$.

Evidently, u is a subterm of t iff $t = v_{(x)}[u]$ for some variable x and some term v with a single occurrence of x. Using this observation, the notion of an occurrence of a subterm in t could be defined precisely. A term t is said to be a constant extension of a term u if there exists a variable x and a term v with a single occurrence of x such that $\operatorname{var}(v) = \{x\}$ and $t = v[u]$. Evidently, if the type Δ contains no nullary symbols then t is a constant extension of u iff $t = F_1 \dots F_n(u)$ for some finite sequence $F_1, \dots, F_n$ of unary symbols from Δ.

Let a, b be two terms. We write $a \leqq b$ if there exists a substitution f such $f(a)$ is a subterm of b. If $a \leqq b$ and $b \leqq a$, we write $a \sim b$ and say that the terms a, b are similar. Evidently, $a \sim b$ iff $b = f(a)$ for an automorphism f of W_Δ; also, $a \sim b$ iff $b = \bar{p}(a)$ for a one-to-one mapping p of $\operatorname{var}(a)$ onto $\operatorname{var}(b)$. If $a \leqq b$ and a, b are not similar, we write $a < b$. There exists no infinite sequence $a_0, a_1, a_2, \dots$ of terms such that $a_i > a_{i+1}$ for all i.

By an equation (of type Δ) we mean an ordered pair of terms (of type Δ). An equation (c, d) is said to be an immediate consequence of an equation (a, b) if there exist a substitution f, a variable x and a term t having a single occurrence of x such that $c = t_{(x)}[f(a)]$ and $d = t_{(x)}[f(b)]$.

Let E be a set of equations (i.e. a binary relation in W_Δ). By an E-proof we mean a non-empty finite sequence $a_0, \dots, a_n$ of terms such that for every $i \in \{1, \dots, n\}$ either (a_{i-1}, a_i) or (a_i, a_{i-1}) is an immediate consequence of an equation belonging to E. The number n is called the length of $a_0, \dots, a_n$. An E-proof $a_0, \dots, a_n$ is said to be an E-proof from a to b if $a_0 = a$ and $a_n = b$. By a minimal E-proof we mean any E-proof $a_0, \dots, a_n$ such that there is no E-proof from a_0 to a_n of length less than n. An equation (c, d) is said to be a consequence of E if there exists an E-proof from c to d.

By an equational theory of type Δ we mean a set T of equations of type Δ such that every consequence of T belongs to T. Equivalently: T is an equational theory of type Δ iff T is a fully invariant congruence of the algebra W_Δ, i.e. a congruence such that $(a, b) \in T$ implies $(f(a), f(b)) \in T$ for any substitution f. The set of all equational theories of type Δ is a complete algebraic lattice with respect to inclusion; it will be denoted by $\mathscr{L}_\Delta$. 1_{W_Δ} is the least and $W_\Delta \times W_\Delta$ is the greatest element of $\mathscr{L}_\Delta$. The lattice $\mathscr{L}_\Delta$ is antiisomorphic to the lattice of varieties of Δ-algebras.

If A, B are two equational theories, then $A \vee B$ (the join of A, B in the lattice $\mathscr{L}_\Delta$) is just the equational theory generated by $A \cup B$. Thus $(a, b) \in A \vee B$ iff there exists an $A \cup B$-proof from a to b. Evidently, a non-empty finite sequence $a_0, \dots, a_n$

is an $A \cup B$-proof iff $(a_{i-1}, a_i) \in A \cup B$ for all $i \in \{1, \ldots, n\}$. The join of an arbitrary family of equational theories can be described similarly. The meet of a family of equational theories coincides with its intersection. The lattice $\mathscr{L}_\Delta$ is a complete sublattice of the equivalence lattice of W_Δ.

For every type Δ, one particular equational theory of type Δ, namely E_Δ, will play an important role in this paper. It is defined as follows: $(u, v) \in E_\Delta$ iff $\operatorname{var}(u) = \operatorname{var}(v)$.

By a full subset of W_Δ we mean a subset U such that $a \in U$ and $a \leqq b$ imply $b \in U$. Evidently, if U is a full subset of W_Δ then $(U \times U) \cup 1_{W_\Delta}$ is an equational theory.

2. MODULAR ELEMENTS IN GENERAL LATTICES AND IN EQUIVALENCE LATTICES

An element e of a lattice L is called modular if $(a \vee e) \wedge b = a \vee (e \wedge b)$ for all the pairs a, b of elements of L such that $a \leqq b$.

Let L be a lattice and $e, a, b, c, d \in L$. We write $\operatorname{Pent}(e, a, b, c, d)$ if $c < e < d$, $c < a < b < d$, $e \vee a = d$, $e \wedge b = c$ (so that the elements e, a, b, c, d constitute a five-element non-modular sublattice of L).

2.1. Proposition. *Let L be a lattice and $e \in L$. The following four conditions are equivalent*:

(1) *e is a modular element of L;*

(2) *e is a modular element of the dual of L;*

(3) *$(a \vee e) \wedge b \leqq a \vee (e \wedge b)$ for all $a, b \in L$ such that $a < b$;*

(4) *there exist no elements $a, b, c, d \in L$ such that* $\operatorname{Pent}(e, a, b, c, d)$.

Proof. The equivalence of the first three conditions is clear. (1) implies (4): if it were $\operatorname{Pent}(e, a, b, c, d)$ for some $a, b, c, d \in L$, then $b = (a \vee e) \wedge b = a \vee (e \wedge b) = a$, a contradiction. (4) implies (1): suppose that e is not modular, so that $a \vee (e \wedge b) < (a \vee e) \wedge b$ for some $a, b \in L$ with $a < b$; then evidently $\operatorname{Pent}(e, a \vee (e \wedge b), (a \vee e) \wedge b, e \wedge b, e \vee a)$, a contradiction.

2.2. Proposition. *Let M be a set and I an equivalence on M. Then I is a modular element of the equivalence lattice of M iff $I = (N \times N) \cup 1_M$ for some $N \subseteq M$.*

Proof. First, let I be modular. It is enough to derive a contradiction from the existence of pairwise different elements $a, b, c, d \in M$ such that $(a, b) \in I$, $(c, d) \in I$, $(a, c) \notin I$. Denote by A the equivalence on M with a single non-one-element block $\{a, c\}$ and by B the equivalence with just two non-one-element blocks $\{a, c\}$, $\{b, d\}$. We have $(b, d) \in (A \vee I) \cap B = A \vee (I \cap B)$, so that there exists a finite sequence $a_0, \ldots, a_n$ such that $a_0 = b$, $a_n = d$ and $(a_{i-1}, a_i) \in A \cup (I \cap B)$ for all $i \in \{1, \ldots, n\}$.

Evidently, if $i \in \{1, \ldots, n\}$ and $a_{i-1} = b$, then $a_i = b$, too. Hence $a_n = b$ and we get a contradiction, since $a_n = d \neq b$.

Next, let $I = (N \times N) \cup 1_M$ where N is a subset of M. Suppose that I is not modular, so that $\mathrm{Pent}(I, A, B, C, D)$ for some equivalences A, B, C, D. There exists a pair $(a, b) \in B \setminus A$; since $B \subseteq I \vee A$, there exists a finite sequence $b_0, \ldots, b_m$ such that $b_0 = a$, $b_m = b$ and $(b_{i-1}, b_i) \in I \cup A$ for all $i \in \{1, \ldots, m\}$. Let $a_0, \ldots, a_n$ be a finite sequence of minimal length among all the finite sequences such that $(a_0, a_n) \in B \setminus A$ and $(a_{i-1}, a_i) \in I \cup A$ for all $i \in \{1, \ldots, n\}$. Then $(a_0, a_1) \in I$ and $a_0 \neq a_1$, since otherwise $(a_0, a_1) \in A$ would imply that $a_1, \ldots, a_n$ is a sequence contradicting the minimality of $a_0, \ldots, a_n$. Hence $a_0 \in N$. Quite similarly, $a_n \in N$ and so $(a_0, a_n) \in I \cap B \subseteq A$, a contradiction.

3. MODULAR ELEMENTS IN THE SUBGROUP LATTICE OF S_M

For every finite set M we denote by S_M the group of all permutations of M and by A_M its subgroup formed by the even permutations of M. The identical permutation of M will be denoted by 1_M (or only 1). If $a_1, \ldots, a_n$ are pairwise different elements of M and $n \geqq 2$ then $[a_1, \ldots, a_n]$ denotes the permutation p of M such that $p(a_1) = a_2, \ldots, p(a_{n-1}) = a_n$, $p(a_n) = a_1$ and $p(b) = b$ for all $b \in M \setminus \{a_1, \ldots, a_n\}$. If $a_1, \ldots, a_n, b_1, \ldots, b_m$ are pairwise different elements of M and $n, m \geqq 2$, we put $[a_1, \ldots, a_n; b_1, \ldots, b_m] = [a_1, \ldots, a_n][b_1, \ldots, b_m]$.

3.1. Proposition. *Let M be a finite set of cardinality $\geqq 5$; let G be a subgroup of S_M. Then G is a modular element of the subgroup lattice of S_M iff either $G = \{1\}$ or $G = A_M$ or $G = S_M$.*

The proof of this proposition will be divided into several lemmas. First of all, the subgroups $\{1\}$, A_M, S_M are modular elements of the subgroup lattice of S_M, since they are normal subgroups and it is easy to see that any normal subgroup of any group is a modular element in the subgroup lattice of the group. Now let G be a modular element of the subgroup lattice of S_M and $G \neq \{1\}$. Since A_M is a maximal subgroup, it is enough to prove $G \supseteq A_M$.

3.2. Lemma. *Suppose that there are three pairwise different elements $a, b, c \in M$ such that $[a, b, c] \in G$ and $[b, c] \in G$. Then $G = S_M$.*

Proof. Let d, e be any pair of elements of M such that the elements a, b, c, d, e are pairwise different. Denote by A the subgroup of S_M generated by $[a, d; b, e]$ and by B the subgroup generated by $[a, b, d, e]$. We have $A \subset B$ and $[a, b, d, e] = [a, b, c][a, d; b, e][a, b, c][a, d; b, e][b, c] \in (A \vee G) \cap B = A \vee (G \cap B)$; hence $G \cap B \nsubseteq A$, so that $G \cap B = B$, i.e. $B \subseteq G$. We have proved $[a, b, d, e] \in G$.

It is enough to prove that if i, j are two different elements of M then $[i, j] \in G$. If $i, j \in \{a, b, c\}$ then either $[i, j] = [b, c]$ or $[i, j] = [a, c] = [b, c][a, b, c]$ or

$[i, j] = [a, b] = [a, b, c]\,[b, c]$, so that $[i, j] \in G$. If $i, j \notin \{a, b, c\}$ then $[i, j] = [a, b, j, i]\,[a, b, i, j]\,[a, b, j, i]$, so that $[i, j] \in G$ by the above argument. Now it is enough to consider the following case: $i \notin \{a, b, c\}$ and $j = a$. Since $\operatorname{Card}(M) \geqq 5$, there exists an element $k \in M \setminus \{a, b, c, i\}$. We have $[i, a] = [a, b]\,[a, b, i, k] \,.\, [a, b, k, i]$ and so $[i, j] = [i, a] \in G$ by the above proved result.

3.3. Lemma. *Suppose that there are two different elements $a, b \in M$ such that $[a, b] \in G$. Then $G = S_M$.*

Proof. There exist three different elements $c, d, e \in M \setminus \{a, b\}$. Denote by A the subgroup of S_M generated by $[a, c, d]$ and by B the subgroup of S_M generated by $[a, c, d]$ and $[a, c]$. We have $A \subset B$, $[a, c] = [a, b]\,[a, c, d]\,[a, c, d]\,[a, b] \,.\, [a, c, d]\,[a, b]\,[a, c, d] \in (A \vee G) \cap B = A \vee (G \cap B)$, so that $G \cap B \nsubseteq A$. Hence either $[a, c] \in G$ or $[a, d] \in G$ or $[c, d] \in G$. If $[a, c] \in G$ then $[a, b, c] = [a, c] \,.\, [a, b] \in G$, so that $G = S_M$ by 3.2. If $[a, d] \in G$ then $[a, b, d] = [a, d]\,[a, b] \in G$, so that $G = S_M$ by 3.2 again. Hence it is enough to consider the case $[c, d] \in G$. Quite analogously, it is enough to consider the case $[c, e] \in G$. We have $[c, d, e] = [c, e]\,[c, d] \in G$; this together with $[c, d] \in G$ gives $G = S_M$ by 3.2.

3.4. Lemma. *Suppose $[a, b, c] \in G$ for some triple a, b, c of pairwise different elements of M. Then $G \supseteq A_M$.*

Proof. It is easy and well known that the group A_M is generated by the permutations $[i, j, k]$ (i, j, k being pairwise different elements of M). So it is enough to prove $[i, j, k] \in G$ for all triples i, j, k of pairwise different elements of M.

Let $d \in M \setminus \{a, b, c\}$. Denote by A the subgroup of S_M generated by $[b, d]$ and by B the subgroup generated by $[b, d]$ and $[a, d]$. We have $A \subset B$ and $[a, d] = [a, b, c]^{-1}\,[b, d]\,[a, b, c] \in (A \vee G) \cap B = A \vee (G \cap B)$, so that $G \cap B \nsubseteq A$. This together with 3.3 implies $[a, b, d] \in G$.

Hence if $\{i, j, k\}$ has at least two elements in common with $\{a, b, c\}$, then $[i, j, k] \in G$. If $\{i, j, k\}$ has exactly one element in common with $\{a, b, c\}$ (say $a = i$), then by the proved result $[a, b, k] \in G$ and applying the above argument again we get $[a, j, k] \in G$, i.e. $[i, j, k] \in G$. Finally, let $\{a, b, c\}$, $\{i, j, k\}$ be disjoint. Applying the above proved result we get $[a, j, k] \in G$ and applying the above result again we get $[i, j, k] \in G$.

3.5. Lemma. *Suppose $[a, b; c, d] \in G$ for some quadruple a, b, c, d of pairwise. different elements of M. Then $G \supseteq A_M$.*

Proof. There exists an element $e \in M \setminus \{a, b, c, d\}$. Denote by A the subgroup of S_M generated by $[a, e]$ and by B the subgroup generated by $[a, e]$ and $[b, e]$. We have $A \subset B$ and $[b, e] = [a, b; c, d]\,[a, e]\,[a, b; c, d] \in (A \vee G) \cap B = A \vee (G \cap B)$, so that $G \cap B \nsubseteq A$. This by 3.3 implies that $[a, b, e] \in G$ and so $G \supseteq A_M$ by 3.4.

3.6. Lemma. $G \supseteq A_M$.

Proof. Assume first there exist a permutation $p \in G$ and an element $a \in M$ such that the elements $a, p(a), p^2(a)$ are pairwise different. Denote by A the subgroup of S_M generated by $[a, p(a)]$ and by B the subgroup generated by $[a, p(a)]$ and $[p(a), p^2(a)]$. We have $A \subset B$ and $[p(a), p^2(a)] = p[a, p(a)]\, p^{-1} \in (A \vee G) \cap B = A \vee (G \cap B)$, so that $G \cap B \nsubseteq A$. It follows from 3.3 and 3.4 that $G \supseteq A_M$.

Now assume that $p^2 = 1$ for any $p \in G$; let $q \in G$, $q \neq 1$. If q is a transposition, we have $G = S_M$ by 3.3. In the opposite case there exist pairwise different elements $a, b, c, d \in M$ with $q(a) = c$, $q(c) = a$, $q(b) = d$, $q(d) = b$. Denote by A the subgroup of S_M generated by $[a, b]$ and by B the subgroup generated by $[a, b]$ and $[c, d]$. We have $A \subset B$ and $[c, d] = q[a, b]\, q \in (A \vee G) \cap B = A \vee (G \cap B)$, so that $G \cap B \nsubseteq A$; by 3.3 and 3.5 we get $G \supseteq A_M$.

This completes the proof of 3.1.

Let us recall that x_1, x_2, x_3, x_4 are four pairwise different variables. We define three subgroups P_1, P_2, P_3 of $S_{\{x_1,x_2,x_3\}}$ as follows:

$$P_1 = \{1, [x_1, x_2]\},$$
$$P_2 = \{1, [x_1, x_3]\} = [x_2, x_3]\, P_1 [x_2, x_3],$$
$$P_3 = \{1, [x_2, x_3]\} = [x_1, x_3]\, P_1 [x_1, x_3].$$

Moreover, we define four subgroups Q, R_1, R_2, R_3 of $S_{\{x_1,x_2,x_3,x_4\}}$ as follows:

$$Q = \{1, [x_1, x_2; x_3, x_4], [x_1, x_3; x_2, x_4], [x_1, x_4; x_2, x_3]\},$$
$$R_1 = Q \cup \{[x_1, x_2, x_3, x_4], [x_1, x_4, x_3, x_2], [x_1, x_3], [x_2, x_4]\},$$
$$R_2 = Q \cup \{[x_1, x_2, x_4, x_3], [x_1, x_3, x_4, x_2], [x_1, x_4], [x_2, x_3]\} = [x_3, x_4]\, R_1 [x_3, x_4],$$
$$R_3 = Q \cup \{[x_1, x_3, x_2, x_4], [x_1, x_4, x_2, x_3], [x_1, x_2], [x_3, x_4]\} = [x_2, x_3]\, R_1 [x_2, x_3].$$

3.7. Proposition. *If* $\operatorname{Card}(M) \leqq 3$ *then every subgroup of* S_M *is a modular element of the subgroup lattice of* S_M. *The subgroup lattice of* $S_{\{x_1,x_2,x_3\}}$ *has exactly six elements, namely, the following ones:*

$$\{1\},\ P_1,\ P_2,\ P_3,\ A_{\{x_1,x_2,x_3\}},\ S_{\{x_1,x_2,x_3\}}\,.$$

We have $A_{\{x_1,x_2,x_3\}} = \{1, [x_1, x_2, x_3], [x_1, x_3, x_2]\}$.

Proof. It is evident.

3.8. Proposition. *The subgroup lattice of* $S_{\{x_1,x_2,x_3,x_4\}}$ *has exactly seven modular elements, namely, the following ones:*

$$\{1\},\ Q,\ R_1,\ R_2,\ R_3,\ A_{\{x_1,x_2,x_3,x_4\}},\ S_{\{x_1,x_2,x_3,x_4\}}\,.$$

We have $A_{\{x_1,x_2,x_3,x_4\}} = Q \cup \{[i, j, k];\ i, j, k \in \{x_1, x_2, x_3, x_4\},\ i \neq j,\ i \neq k,\ j \neq k\}$.

Proof. It is a routine work of drawing a picture of the subgroup lattice of $S_{\{x_1,x_2,x_3,x_4\}}$ and finding all its modular elements.

4. MODULAR ELEMENTS IN THE LATTICE OF EQUATIONAL THEORIES OF A SMALL TYPE

4.1. Theorem. *Let Δ be a type consisting of nullary operation symbols only and let T be an equational theory of type Δ. Then T is a modular element of $\mathscr{L}_\Delta$ iff either $T = W_\Delta \times W_\Delta$ or $T = (C \times C) \cup 1_{W_\Delta}$ for some $C \subseteq \Delta$.*

Proof. It follows from 2.2, since the elements of $\mathscr{L}_\Delta$ different from $W_\Delta \times W_\Delta$ constitute a sublattice of $\mathscr{L}_\Delta$ isomorphic to the equivalence lattice of Δ.

4.2. Theorem. *Let $\Delta = \{F\} \cup \Delta_0$ where F is a unary operation symbol and Δ_0 is a set of nullary operation symbols; let T be an equational theory of type Δ. Denote by Y the set of all the terms t such that* var $(t) = \emptyset$ *and $(t, t') \in T$ for some $t' \neq t$. Then T is a modular element of $\mathscr{L}_\Delta$ iff at least one of the following three conditions is satisfied:*

(1) *$T = (U \times U) \cup 1_{W_\Delta}$ for some full subset U of W_Δ;*

(2) *$T \subseteq E_\Delta$ and $Y \times Y$ is a block of T;*

(3) *$T \subseteq E_\Delta$ and there exists a $c \in \Delta_0$ such that whenever $t \in Y$ then $t = F^k c$ for some $k \geqq 0$.*

The proof of this theorem will be divided into several lemmas.

4.3. Lemma. *Let T be modular; let $c, d \in \Delta_0$, $c \neq d$, $k, l \geqq 0$, $(F^k c, F^l d) \in T$. Then $(F^k c, F^{k+m} c) \in T$ for some $m > 0$.*

Proof. Denote by A the equational theory generated by $(F^l d, F^{l+1} d)$ and by B the equational theory generated by $(F^k c, F^{k+1} c)$, $(F^l d, F^{l+1} d)$. We have $(F^k c, F^{k+1} c) \in (A \vee T) \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_n$ be a minimal $A \cup (T \cap B)$-proof from $F^k c$ to $F^{k+1} c$. Since $\{F^k c\}$ is a block of A and $a_0 \neq a_1$, we cannot have $(a_0, a_1) \in A$; hence $(a_0, a_1) \in T \cap B$. The set $\{F^k c, F^{k+1} c, F^{k+2} c, \ldots\}$ is a block of B and so $a_1 = F^{k+m} c$ for some $m > 0$. We get $(F^k c, F^{k+m} c) \in T$.

4.4. Lemma. *Let T be modular; let $c, d \in \Delta_0$, $c \neq d$, $k, l \geqq 0$, $m, n > 0$, $(F^k c, F^{k+m} c) \in T$, $(F^l d, F^{l+n} d) \in T$. Then $(F^k c, F^l d) \in T$.*

Proof. Denote by A the equational theory generated by $(F^{k+m} c, F^{l+n} d)$ and by B the equational theory generated by $(F^k c, F^l d)$, $(F^{k+m} c, F^{l+n} d)$. We have $(F^k c, F^l d) \in (A \vee T) \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_r$ be a minimal $A \cup (T \cap B)$-proof from $F^k c$ to $F^l d$. Since $\{F^k c\}$ is a block of A and $a_0 \neq a_1$, we cannot have $(a_0, a_1) \in A$; hence $(a_0, a_1) \in T \cap B$. Since $\{F^k c, F^l d\}$ is a block of B, $a_1 = F^l d$. Hence $(F^k c, F^l d) \in T$.

4.5. Lemma. *Let T be modular and $T \nsubseteq E_\Delta$. Then (1) takes place.*

Proof. Since $T \nsubseteq E_\Delta$, there exists a positive integer n such that $(F^n x_1, F^n x_2) \in T$. Denote by U the set of all the terms u such that $(u, v) \in T$ for some $v \neq u$. Evidently, U is a full subset of W_Δ and it is enough to prove $(u, F^n x_1) \in T$ for all $u \in U$. Let $(u, v) \in T$ and $u \neq v$. If either $\operatorname{var}(u) = \emptyset$ or $\operatorname{var}(v) = \emptyset$ or $u = F^k c$ and $v = F^l c$ for some $k, l \geqq 0$ and some $c \in \Delta_0$, then $(u, F^n x_1) \in T$ follows from the fact that T is an equational theory. The case $u = F^k c$ and $v = F^l d$ where $k, l \geqq 0$, $c, d \in \Delta_0$ and $c \neq d$ remains. By 4.3 we have $(F^k c, F^{k+m} c) \in T$ for some $m > 0$; hence we get $(F^k c, F^n x_1) \in T$.

4.6. Lemma. *Let T be modular and $T \subseteq E_\Delta$. Then either (2) or (3) takes place.*

Proof. It follows from 4.3 and 4.4.

4.7. Lemma. *Let either (1) or (2) or (3) be satisfied. Then T is modular.*

Proof. Suppose that T is not modular, so that $\operatorname{Pent}(T, A, B, C, D)$ for some $A, B, C, D \in \mathscr{L}_\Delta$. There exists a pair $(a, b) \in B \setminus A$; since $B \subseteq T \vee A$, there exists a $T \cup A$-proof form a to b. Let n be the minimal positive integer such that there exists a $T \cup A$-proof $a_0, \ldots, a_n$ with $(a_0, a_n) \in B \setminus A$ and let us fix one such $T \cup A$-proof $a_0, \ldots, a_n$. It is evident that $n \geqq 3$, n is odd, $(a_{i-1}, a_i) \in T \setminus A$ if i is odd and $(a_{i-1}, a_i) \in A \setminus T$ if i is even. For every $i \in \{0, \ldots, n\}$ define a non-negative integer $k(i)$ and an element $u_i \in V \cup \Delta_0$ by $a_i = F^{k(i)} u_i$.

Suppose $T \nsubseteq E_\Delta$. Then $T = (U \times U) \cup 1_{W_\Delta}$ for a full subset U of W_Δ. Since $(a_0, a_1) \in T$ and $a_0 \neq a_1$, we have $a_0 \in U$. Quite similarly, $a_n \in U$. Hence $(a_0, a_n) \in T \cap B \subseteq A$, a contradiction.

Hence $T \subseteq E_\Delta$ and so either (2) or (3) is satisfied.

Suppose that either $u_0 \in V$ or $u_0 = u_1 = \ldots = u_n \in \Delta_0$. Evidently, there exists an $m_1 > 0$ such that $(a_0, F^{im_1} a_0) \in T$ for all $i \geqq 0$; there exists an $m_2 > 0$ such that $(a_0, F^{im_2} a_0) \in B$ for all $i \geqq 0$; there exists an $m_3 > 0$ such that $(a_n, F^{im_3} a_n) \in B$ for all $i \geqq 0$; since either (2) or (3) is satisfied, there exists an $m_4 > 0$ such that $(a_n, F^{im_4} a_n) \in T$ for all $i \geqq 0$. Put $m = m_1 m_2 m_3 m_4$. If $i \geqq 0$ then $(a_0, F^{im} a_0) \in B \cap T \subseteq A$, $(a_n, F^{im} a_n) \in B \cap T \subseteq A$, so that $(F^{im} a_0, F^{im} a_n) \in B \setminus A$. The sequence $F^{im} a_0, \ldots, F^{im} a_n$ is evidently a $T \cup A$-proof. Let us fix an $i \geqq 0$ such that $im \geqq k(1) - k(0)$ and $im \geqq k(1) - k(2)$. Then $(F^{im+k(0)} u_0, F^{im+k(0)+k(2)-k(1)} u_2) \in A$ and $(F^{im+k(0)+k(2)-k(1)} u_2, F^{im+k(2)} u_2) \in T$. Hence the sequence $F^{im} a_0$, $F^{im+k(0)+k(2)-k(1)} u_2, F^{im} a_2, \ldots, F^{im} a_n$ is a $T \cup A$-proof, too; however, the pair

$(F^{im}a_0, F^{im+k(0)+k(2)-k(1)}u_2)$ belongs to A and so there exists a shorter $T \cup A$-proof, which contradicts the minimality of n.

We get $u_0 \notin V$. Similarly, $u_n \notin V$. Evidently, it is enough to consider the case $u_0, \ldots$ $\ldots, u_n \notin V$. We have $a_0, \ldots, a_n \in C$. If $C \times C$ is a block of T then $(a_0, a_n) \in T \cap$ $\cap B \subseteq A$, a contradiction. In the opposite case (3) is satisfied and so $u_0 = u_1 = \ldots$ $\ldots = u_n \in \Delta_0$; however, this was already proved to be impossible.

This completes the proof of Theorem 4.2.

5. MODULAR ELEMENTS IN THE LATTICE OF EQUATIONAL THEORIES OF A LARGE TYPE

If T is an equational theory of type Δ, we denote by U_T the set of all the terms a such that there exists a term b with $(a, b) \in T$ and $b \neq \bar{p}(a)$ for any permutation p of var (a); for every term a we denote by $G_T(a)$ the set of all the permutations p of var (a) such that $(a, \bar{p}(a)) \in T$, so that $G_T(a)$ is a subgroup of $S_{\mathrm{var}(a)}$.

5.1. Theorem. *Let Δ be a large type and T an equational theory of type Δ. Then T is a modular element of $\mathscr{L}_\Delta$ iff the following nine conditions are satisfied:*

(1) *U_T is a full subset of W_Δ;*

(2) *if $u, v \in U$ and* var $(u) =$ var (v) *then $(u, v) \in T$;*

(3) *for every $t \in W_\Delta$, the group $G_T(t)$ is a modular element of the subgroup lattice of $S_{\mathrm{var}(t)}$;*

(4) *if $a, b \in W_\Delta$,* var $(a) =$ var $(b) = \{x_1, x_2, x_3\}$ *and $G_T(a) = G_T(b) = P_1$, then either $a \leqq b$ or $b \leqq a$;*

(5) *if $a, b \in W_\Delta$,* var $(a) =$ var $(b) = \{x_1, x_2, x_3\}$, *$G_T(a) = P_1$ and $G_T(b) = A_{\{x_1,x_2,x_3\}}$, then $a < b$;*

(6) *if $a, t \in W_\Delta$,* var $(a) = \{x_1, x_2, x_3\}$, *$G_T(a) = P_1$,* var $(t) = \{x\}$ *for some $x \in V$, $t \neq x$ and if x has a single occurrence in t, then there exists a positive integer k with $G_T(t^{(k)}[a]) = S_{\{x_1,x_2,x_3\}}$;*

(7) *if $a, b \in W_\Delta$,* var $(a) =$ var $(b) = \{x_1, x_2, x_3, x_4\}$ *and $G_T(a) = G_T(b) = R_1$, then either $a \leqq b$ or $b \leqq a$;*

(8) *there exist no two terms $a, b \in W_\Delta$ such that* var $(a) =$ var $(b) = \{x_1, x_2, x_3, x_4\}$, *$G_T(a) = R_1$ and $G_T(b) = A_{\{x_1,x_2,x_3,x_4\}}$;*

(9) *if $a, t \in W_\Delta$,* var $(a) = \{x_1, x_2, x_3, x_4\}$, *$G_T(a) = R_1$,* var $(t) = \{x\}$ *for some $x \in V$, $t \neq x$ and if x has a single occurrence in t, then there exists a positive integer k with $G_T(t^{(k)}[a]) = S_{\{x_1,x_2,x_3,x_4\}}$.*

Notice that in the case of a large type Δ containing neither nullary nor unary symbols the two most complicated of these nine conditions, namely (6) and (9), are empty.

The proof of this theorem will be divided into the following six sections. In these sections let Δ be a large type and let T be an equational theory of type Δ; put $U = U_T$.

6. DIRECT IMPLICATION: PRELIMINARIES

6.1. Lemma. *Let $a \in U$. Then there exists a term b such that $(a, b) \in T$, $b \nleqq a$ and* $\operatorname{var}(a) = \operatorname{var}(b)$.

Proof. Since $a \in U$, there exists a term c such that $(a, c) \in T$ and $c \neq \bar{p}(a)$ for any permutation p of $\operatorname{var}(a)$. Consider first the case $\operatorname{var}(a) \neq \operatorname{var}(c)$. Then there exist a term $d \in \{a, c\}$ and a variable x such that $x \in \operatorname{var}(d)$ and $x \notin \operatorname{var}(a) \cap \operatorname{var}(c)$. Let us take a non-nullary symbol $F \in \Delta$ and define a substituion f by $f(y) = y$ for all $y \in \operatorname{var}(a) \cap \operatorname{var}(c)$ and $f(y) = F(a, a, \ldots, a)$ for all the remaining variables y. It is evident that the term $b = f(d)$ has the desired properties. Now let $\operatorname{var}(a) = \operatorname{var}(c)$. If $c \nleqq a$, we can put $b = c$. If $c < a$, then $a = t_{(x)}[c]$ for a variable x and a term t with a single occurrence of x; it is easy to see that the term $b = t_{(x)}[a]$ has the desired properties.

6.2. Lemma. *Let $F \in \Delta$ be a symbol of arity $n \geqq 1$. Let $E \subseteq W_\Delta \times W_\Delta$ be such that if $(u, v) \in E$ then $v = F(u, w_2, \ldots, w_n)$ for some terms $w_2, \ldots, w_n$. Let $(a, v_0) \in E$ be such that if $(u, v) \in E$ then either $u = a$ or $u \nleqq a$. Let a' be a term such that (a, a') is a consequence of E. Then there exist a non-negative integer k and terms $t_2^1, \ldots, t_n^1, t_2^2, \ldots, t_n^2, \ldots, t_2^k, \ldots, t_n^k$ such that*

$$a' = F(\ldots F(F(a, t_2^1, \ldots, t_n^1), t_2^2, \ldots, t_n^2), \ldots, t_2^k, \ldots, t_n^k)\,.$$

Proof. Denote by H the set of all the terms of the form $F(\ldots F(F(a, t_2^1, \ldots, t_n^1), t_2^2, \ldots, t_n^2), \ldots, t_2^k, \ldots, t_n^k)$. It is enough to prove that if $b \in H$ and (b, c) is an immediate consequence of an equation from $E \cup E^{-1}$ then $c \in H$. Let

$$b = F(\ldots F(F(a, t_2^1, \ldots, t_n^1), t_2^2, \ldots, t_n^2), \ldots, t_2^k, \ldots, t_n^k) \in H$$

and let (b, c) be an immediate consequence of an equation $(u, v) \in E \cup E^{-1}$. There exists a substitution f such that $f(u)$ is a subterm of b and c results from b by substituting $f(v)$ for one occurrence of $f(u)$. If the occurrence of $f(u)$ is contained in some t_i^j then it is evident that $c \in H$. Let the occurrence of $f(u)$ be not contained in any t_i^j. Then it follows from the properties of E and a that $f(u) = F(\ldots F(F(a, t_2^1, \ldots$ $\ldots, t_n^1), t_2^2, \ldots, t_n^2), \ldots, t_2^m, \ldots, t_n^m)$ for some $m \in \{0, \ldots, k\}$ and if $(u, v) \in E^{-1}$ then $m \neq 0$. If $(u, v) \in E$ then $v = F(u, w_2, \ldots, w_n)$ for some $w_2, \ldots, w_n$ and we have

$$c = F(\ldots F(F(a, t_2^1, \ldots, t_n^1), \ldots, t_2^m, \ldots, t_n^m), f(w_2), \ldots, f(w_n)),$$
$$t_2^{m+1}, \ldots, t_n^{m+1}), \ldots, t_2^k, \ldots, t_n^k) \in H\,.$$

If $(u, v) \in E^{-1}$ then $u = F(v, w_2, \ldots, w_n)$ for some $w_2, \ldots, w_n$ and we have

$$c = F(\ldots F(F(a, t_2^1, \ldots, t_n^1), \ldots, t_2^{m-1}, \ldots, t_n^{m-1}), t_2^{m+1}, \ldots, t_n^{m+1}), \ldots, t_2^k, \ldots, t_n^k) \in H .$$

6.3. Lemma. *Let T be modular and $a \in U$. Then $(a, b) \in T$ for a term b such that* $\operatorname{var}(a) = \operatorname{var}(b)$ *and a is a proper subterm of b.*

Proof. Let us fix a symbol $F \in \Delta$ of arity $n \geqq 1$. By 6.1 there exists a term c such that $(a, c) \in T$, $c \nleqq a$ and $\operatorname{var}(a) = \operatorname{var}(c)$. Denote by A the equational theory generated by $(c, F(c, \ldots, c))$ and by B the equational theory generated by $(a, F(a, \ldots, a))$ and $(c, F(c, \ldots, c))$. We have $A \subseteq B$ and $(a, F(a, \ldots, a)) \in (A \vee T) \cap \cap B = A \vee (T \cap B)$. Hence there exists an $A \cup (T \cap B)$-proof from a to $F(a, \ldots, a)$. Especially, there exists a term $b \neq a$ such that either $(a, b) \in A$ or $(a, b) \in T \cap B$. Since $A \subseteq E_\Delta$ and $B \subseteq E_\Delta$, we have $\operatorname{var}(a) = \operatorname{var}(b)$. Since $c \nleqq a$ and $a \neq b$, we cannot have $(a, b) \in A$; hence $(a, b) \in T \cap B$. Especially, $(a, b) \in T$. Since $(a, b) \in B$, it follows from 6.2 that a is a proper subterm of b.

6.4. Lemma. *Let T be modular; let p, q, r, s be terms such that $p \nleqq r$, $q \nleqq r$, $p \nleqq s$, $q \nleqq s$, $r \nleqq s$, $s \nleqq r$,* $\operatorname{var}(r) = \operatorname{var}(s)$ *and (r, s) is a consequence of $T \cup \cup \{(p, q)\}$. Then $(r, s) \in T$.*

Proof. Denote by A the equational theory generated by (p, q) and by B the equational theory generated by (p, q) and (r, s). We have $A \subseteq B$, $(r, s) \in (A \vee T) \cap \cap B = A \vee (T \cap B)$ and so there exists a term $c \neq r$ such that either $(r, c) \in A$ or $(r, c) \in T \cap B$. Since $p \nleqq r$ and $q \nleqq r$, we cannot have $(r, c) \in A$. Hence $(r, c) \in \in T \cap B$. Now it is enough to prove that if t is a term such that either (r, t) or (s, t) is an immediate consequence of an equation belonging to $\{(p, q), (r, s), (q, p), (s, r)\}$, then either $t = r$ or $t = s$. For the reasons of symmetry it is enough to consider the case of (r, t) being an immediate consequence of an equation from $\{(p, q), (r, s), (q, p), (s, r)\}$. Since $p, q, s \nleqq r$, (r, t) is an immediate consequence of (r, s). There exists a substitution f such that $f(r)$ is a subterm of r and t results from r by replacing the subterm $f(r)$ by $f(s)$. But $f(r) = r$, $f(x) = x$ for all $x \in \operatorname{var}(r) = \operatorname{var}(s)$, $f(s) = s$ and $t = s$.

If F is an n-ary symbol from Δ and $i \in \{1, \ldots, n\}$ then for any term $u \in W_\Delta$ and any sequences $s_1, \ldots, s_k \in W_\Delta^{n-1}$ (where $k \geqq 0$) we define a term $\gamma_{F,i}(u; s_1; \ldots; s_k)$ as follows: if $k = 0$ then $\gamma_{F,i}(u; s_1; \ldots; s_k) = u$; if $k \geqq 1$ then $\gamma_{F,i}(u; s_1; \ldots; s_k) = F(t_1, \ldots, t_{i-1}, \gamma_{F,i}(u; s_1; \ldots; s_{k-1}), t_i, \ldots, t_{n-1})$ where $s_k = (t_1, \ldots, t_{n-1})$.

6.5. Lemma. *Let T be modular. Let $(a, b) \in T$, $b \nleqq a$,* $\operatorname{var}(a) = \operatorname{var}(b)$; *let a be neither a variable nor a nullary symbol from Δ. Let $x \in V \setminus$* $\operatorname{var}(a)$ *and let d be a term such that x has exactly one occurrence in d and $d \neq x$. Let $F \in \Delta$ be a symbol of arity n and let $i \in \{1, \ldots, n\}$ be such that d is not of the form $F(u_1, \ldots, u_n)$ where $u_1, \ldots, u_n \in W_\Delta$ and $x \in$* $\operatorname{var}(u_i)$. *Put $f = \sigma_a^x$ and $g = \sigma_b^x$. Let $k >$* $\operatorname{Max}(\lambda(f(d)), \lambda(g(d)))$. *Let $s_1, \ldots, s_k$ be finite sequences such that:*

(i) *if* $\operatorname{var}(f(d)) \neq \emptyset$ *then* $s_1, \ldots, s_k \in (\operatorname{var}(f(d)))^{n-1}$ *and every variable from* $\operatorname{var}(f(d))$ *is a member of some member of* $s_1, \ldots, s_k$;

(ii) *if* $\operatorname{var}(f(d)) = \emptyset$ *then* $s_1 = \ldots = s_k = (G, \ldots, G)$ *for some nullary symbol* G *contained in* a.

Then $(\gamma_{F,i}(a; s_1; \ldots; s_k), f(d)) \in T$.

Proof. By 6.4 it is enough to prove

$$\gamma_{F,i}(b; s_1; \ldots; s_k) \not\leq \gamma_{F,i}(a; s_1; \ldots; s_k),$$
$$g(d) \not\leq \gamma_{F,i}(a; s_1; \ldots; s_k),$$
$$\gamma_{F,i}(b; s_1; \ldots; s_k) \not\leq f(d),$$
$$g(d) \not\leq f(d),$$
$$\gamma_{F,i}(a; s_1; \ldots; s_k) \not\leq f(d).$$
$$f(d) \not\leq \gamma_{F,i}(a; s_1; \ldots; s_k).$$

All these inequalities except for the second and the last one are clear. Let h be either f or g and suppose that $p(h(d))$ is a subterm of $\gamma_{F,i}(a; s_1; \ldots; s_k)$ for a substitution p. Evidently, $p(h(d))$ is not a subterm of a and $p(h(d))$ is neither a variable nor a nullary symbol. Hence $p(h(d)) = \gamma_{F,i}(a; s_1; \ldots; s_j)$ for some $j \in \{1, \ldots, k\}$. Then $d = F(u_1, \ldots, u_n)$ for some terms $u_1, \ldots, u_n$. By the choice of F, i we have $x \in \operatorname{var}(u_{i_0})$ for some $i_0 \neq i$. Since $p(h(u_{i_0}))$ is either a variable or a nullary symbol G contained in a, we get $u_{i_0} = x$. If $h = g$ then $p(b)$ is either a variable or a nullary symbol contained in a, so that b is either a variable or a nullary symbol contained in a, a contradiction with $b \not\leq a$. If $h = f$ then $p(a)$ is either a variable or a nullary symbol, so that a is either a variable or a nullary symbol, a contradiction.

6.6. Lemma. *Let* T *be modular. Let* $a \in U$ *be neither a variable nor a nullary symbol from* Δ. *Let* $c_1, c_2 \in W_\Delta$, $\operatorname{var}(c_1) = \operatorname{var}(c_2)$ *and let* a *be a proper subterm of both* c_1 *and* c_2. *Then* $(c_1, c_2) \in T$.

Proof. By 6.1 there exists a term b such that $(a, b) \in T$, $b \not\leq a$ and $\operatorname{var}(a) = \operatorname{var}(b)$. Let $x \in V \setminus \operatorname{var}(c_1)$. Put $f = \sigma_a^x$ and $g = \sigma_b^x$. Let d_1 and d_2 be the terms obtained respectively from c_1 and c_2 by replacing exactly one occurrence of the subterm a by x. Evidently, there exists a triple F, n, i such that F is an n-ary symbol from Δ, $i \in \{1, \ldots, n\}$ and d_1 is not of the form $F(u_1, \ldots, u_n)$ where $u_1, \ldots, u_n \in W_\Delta$ and $x \in \operatorname{var}(u_i)$. There exist a number $k > \operatorname{Max}(\lambda(f(d_1)), \lambda(f(d_2)), \lambda(g(d_1)), \lambda(g(d_2)))$ and finite sequences $s_1, \ldots, s_k$ satisfying the conditions (i), (ii) of 6.5 (with d being either d_1 or d_2; we have $f(d_1) = c_1$ and $f(d_2) = c_2$). By 6.5, $(\gamma_{F,i}(a; s_1; \ldots; s_k), c_1) \in T$. If d_2 is not of the form $F(u_1, \ldots, u_n)$ where $x \in \operatorname{var}(u_i)$ then $(\gamma_{F,i}(a; s_1; \ldots; s_k), c_2) \in T$ by 6.5, too, so that $(c_1, c_2) \in T$. Let $d_2 = F(u_1, \ldots, u_n)$ and $x \in \operatorname{var}(u_i)$. Since Δ is a large type, there exists a triple G, m, j such that G is an m-ary symbol from Δ, $j \in \{1, \ldots, m\}$ and $(F, n, i) \neq (G, m, j)$. There exist an

$l > \operatorname{Max}(\lambda(f(d_2)), \lambda(g(d_2)), \lambda(f(\gamma_{F,i}(x; s_1; \dots; s_k))), \lambda(g(\gamma_{F,i}(x; s_1; \dots; s_k))))$ and finite sequences $s'_1, \dots, s'_l$ such that:

(i′) if $\operatorname{var}(c_2) \neq \emptyset$ then $s'_1, \dots, s'_l \in (\operatorname{var}(c_2))^{m-1}$ and every variable from $\operatorname{var}(c_2)$ is a member of some member of $s'_1, \dots, s'_l$;

(ii′) if $\operatorname{var}(c_2) = \emptyset$ then $s'_1 = \dots = s'_l = (H, \dots, H)$ for a nullary symbol H contained in a.

By 6.5 we have $(\gamma_{G,j}(a; s'_1; \dots; s'_l), f(\gamma_{F,i}(x; s_1; \dots; s_k))) \in T$ and $(\gamma_{G,j}(a; s'_1; \dots; s'_l), f(d_2)) \in T$, so that $(\gamma_{F,i}(a; s_1; \dots; s_k), c_2) \in T$ and consequently $(c_1, c_2) \in T$.

6.7. Lemma. *Let T be modular. Let $a \in U$; let $c_1, c_2 \in W_\Delta$, $\operatorname{var}(c_1) = \operatorname{var}(c_2)$ and let a be a proper subterm of both c_1 and c_2. Then $(c_1, c_2) \in T$.*

Proof. If a is neither a variable nor a nullary symbol, this follows from 6.6. Let a be either a variable or a nullary symbol. By 6.3 we have $(a, b) \in T$ for a term b such that $\operatorname{var}(a) = \operatorname{var}(b)$ and a is a proper subterm of b. Evidently, $b \in U$. Denote by c'_1 and c'_2 the terms obtained respectively from c_1 and c_2 by replacing one occurrence of a by b. Then $\operatorname{var}(c'_1) = \operatorname{var}(c'_2)$ and b is a proper subterm of both c'_1 and c'_2; since b is neither a variable nor a nullary symbol, it follows from 6.6 that $(c'_1, c'_2) \in T$. However, we have $(c_1, c'_1) \in T$ and $(c_2, c'_2) \in T$, so that $(c_1, c_2) \in T$.

6.8. Lemma. *Let T be modular. Let $a \in U$; let c be a term such that $\operatorname{var}(a) = \operatorname{var}(c)$ and a is a subterm of c. Then $(a, c) \in T$.*

Proof. It follows from 6.3 and 6.7.

6.9. Lemma. *Let T be modular. Then U is a full subset of W_Δ and if $u, v \in U$ and $\operatorname{var}(u) = \operatorname{var}(v)$ then $(u, v) \in T$.*

Proof. Let $a \in U$ and $a \leqq b$, so that $f(a)$ is a subterm of b for a substitution f. It follows from 6.8 that $(a, c) \in T$ for a term c such that $\lambda(c) > \lambda(b)$. Denote by d the term obtained from b by replacing one occurrence of the subterm $f(a)$ by $f(c)$. Then $(b, d) \in T$; since $\lambda(d) > \lambda(b)$, we get $b \in U$. We have proved that U is a full subset of W_Δ. Let $u, v \in U$ and $\operatorname{var}(u) = \operatorname{var}(v)$. Let us distinguish two cases.

Case 1. Δ contains a symbol F of arity $n \geqq 2$. By 6.8 we have $(u, F(u, v, \dots, v)) \in T$ and $(v, F(u, v, \dots, v)) \in T$, so that $(u, v) \in T$.

Case 2. Δ contains no symbol of arity $\geqq 2$. Then $u = s_1(t_1)$ and $v = s_2(t_2)$ for some finite sequences s_1, s_2 of unary symbols from Δ and some t_1, t_2 such that either $t_1 = t_2 \in V$ or t_1, t_2 are nullary symbols. By 6.8, $(s_1(t_1), ms_1(t_1)) \in T$ and $(s_2(t_2), ms_2(t_2)) \in T$ for any finite sequence m of unary symbols from Δ. Since Δ is a large type, there exist two different unary symbols $F, G \in \Delta$. The equation $(Fs_2s_1(t_1), Gs_1s_2(t_2))$ is a consequence of $T \cup \{(FFs_2s_1(t_1), FFs_1s_2(t_2)\}$; evidently, the assumptions of 6.4 are satisfied, so that $(Fs_2s_1(t_1), Gs_1s_2(t_2)) \in T$ by 6.4. Hence $(s_1(t_1), s_2(t_2)) \in T$, i.e. $(u, v) \in T$.

6.10. Lemma. *Let T be modular and let $t \in W_\Delta$. Then the group $G_T(t)$ is a modular element of the subgroup lattice of $S_{\mathrm{var}(t)}$.*

Proof. Suppose Pent $(G_T(t), H, K, M, N)$ for some H, K, M, N in the subgroup lattice of $S_{\mathrm{var}(t)}$. Denote by A and B the equational theories generated by the equations $(t, \bar{p}(t))$ with $p \in H$ and $p \in K$, respectively. We have $A \subseteq B$ and so $(A \vee T) \cap B = A \vee (T \cap B)$. Since $H \vee G_T(t) \supseteq K$, it is evident that $A \vee T \supseteq B$ and so $(A \vee T) \cap B = B$; we get $A \vee (T \cap B) = B$. Let $q \in K \setminus H$. We have $(t, \bar{q}(t)) \in B = A \vee (T \cap B)$ and so there exists an $A \cup (T \cap B)$-proof $u_0, \dots, u_m$ from t to $\bar{q}(t)$. It is easy to prove $u_i = \bar{h}(t)$ for some $h \in H$ by induction on $i \in \{0, \dots, m\}$. Hence $q \in H$, a contradiction.

7. DIRECT IMPLICATION: THREE VARIABLES

Put $r_1 = [x_1, x_2]$, $r_2 = [x_1, x_3]$, $r_3 = [x_2, x_3]$, $r_4 = [x_1, x_2, x_3]$ and $r_5 = [x_1, x_3, x_2] = r_4^{-1}$. We have $P_1 = \{1, r_1\}$ and $A_{\{x_1,x_2,x_3\}} = \{1, r_4, r_5\}$. Put

$$V_1 = \{a \in W_\Delta;\ \mathrm{var}(a) = \{x_1, x_2, x_3\},\ G_T(a) = P_1\},$$

$$V_2 = \{a \in W_\Delta;\ \mathrm{var}(a) = \{x_1, x_2, x_3\},\ G_T(a) = A_{\{x_1,x_2,x_3\}}\}.$$

7.1. Lemma. *Let $a \in V_1$ and let f be a substitution such that $f(a) \notin U$. Then $f(x_1), f(x_2) \in V$ and $f(x_1), f(x_2) \notin \mathrm{var}(f(x_3))$.*

Proof. Let x, y be two different variables not belonging to $\mathrm{var}(f(a))$. Denote by g the substitution with $g(x_1) = f(x_1)$, $g(x_2) = x$, $g(x_3) = y$. We have $(a, \bar{r}_1(a)) \in T$, $(g(a), g\,\bar{r}_1(a)) \in T$. We have $g(a) \notin U$, since otherwise we would have $f(a) \in U$. Hence $g(a) \sim g\,\bar{r}_1(a)$ and there exists an automorphism p of W_Δ with $p\,g(a) = g\,\bar{r}_1(a)$. Hence $p\,g(x_1) = g\,\bar{r}_1(x_1)$, i.e. $p\,f(x_1) = x$ and we get $f(x_1) \in V$. Similarly we can prove $f(x_2) \in V$. Denote by h the substitution with $h(x_1) = f(x_1)$, $h(x_2) = x$, $h(x_3) = f(x_3)$. We have $h(a) \notin U$ and $(h(a), h\,\bar{r}_1(a)) \in T$, so that $h(a) \sim h\,\bar{r}_1(a)$ and $q\,h(a) = h\,\bar{r}_1(a)$ for an automorphism q of W_Δ. Hence $q\,h(x_1) = h\,\bar{r}_1(x_1)$ and $q\,h(x_3) = h\,\bar{r}_1(x_3)$, i.e. $q\,f(x_1) = x$ and $q\,f(x_3) = f(x_3)$, where $f(x_1) \in V$; this implies $f(x_1) \notin \mathrm{var}(f(x_3))$. We can prove $f(x_2) \notin \mathrm{var}(f(x_3))$ quite similarly.

7.2. Lemma. *Let $a \in V_2$ and let f be a substitution such that $f(a) \notin U$. Then $a \sim f(a)$.*

Proof. Let x, y be two different variables not belonging to $\mathrm{var}(f(a)) \cup \{x_1, x_2, x_3\}$. Denote by g the substitution with $g(x_1) = f(x_1)$, $g(x_2) = x$, $g(x_3) = y$. We have $g(a) \notin U$ and $(g(a)\,g\,\bar{r}_4(a)) \in T$, so that $p\,g(a) = g\,\bar{r}_4(a)$ for an automorphism p of W_Δ. Hence $p\,g(x_1) = g\,\bar{r}_4(x_1)$, i.e. $p\,f(x_1) = x$; we get $f(x_1) \in V$. Quite similarly, $f(x_2) \in V$ and $f(x_3) \in V$. Denote by h the substitution with $h(x_1) = f(x_1)$, $h(x_2) =$

$= f(x_2)$, $h(x_3) = x$. We have $h(a) \notin U$ and $(h(a), h\,\bar{r}_4(a)) \in T$, so that $q\,h(a) = h\,\bar{r}_4(a)$ for an automorphism q of W_Δ. Hence $q\,h(x_1) = h\,\bar{r}_4(x_1)$, $q\,h(x_2) = h\,\bar{r}_4(x_2)$ and $q\,h(x_3) = h\,\bar{r}_4(x_3)$, i.e. $q\,f(x_1) = f(x_2)$, $q\,f(x_2) = x$ and $q(x) = f(x_1)$. This yields $f(x_1) \neq f(x_2)$. Similarly $f(x_2) \neq f(x_3)$ and $f(x_3) \neq f(x_1)$. Hence $a \sim f(a)$.

7.3. Lemma. *Let T be modular and $a, b \in V_1$. Then either $a \leqq b$ or $b \leqq a$.*

Proof. Suppose that $a \nleqq b$ and $b \nleqq a$. Denote by A the equational theory generated by $(a, \bar{r}_2(b))$ and by B the equational theory generated by $(a, \bar{r}_2(b))$, $(a, \bar{r}_3(b))$. We have $(a, \bar{r}_1(a)) \in T$, $(\bar{r}_1(a), \bar{r}_5(b)) \in A$, $(\bar{r}_5(b), \bar{r}_3(b)) \in T$ and so $(a, \bar{r}_3(b)) \in (A \vee T) \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_n$ be a minimal $A \cup (T \cap B)$-proof from a to $\bar{r}_3(b)$. Evidently, $\{a, \bar{r}_4(a), \bar{r}_5(a), \bar{r}_1(b), \bar{r}_2(b), \bar{r}_3(b)\}$ is a block of B and $\{a, \bar{r}_2(b)\}$ is a block of A; hence every member of $a_0, \ldots, a_n$ equals either a or $\bar{r}_2(b)$, a contradiction.

7.4. Lemma. *Let T be modular, $a \in V_1$ and $b \in V_2$. Then $a < b$.*

Proof. Suppose first that $a \nleqq b$ and $b \nleqq a$. Denote by A the equational theory generated by (a, b) and by B the equational theory generated by (a, b), $(\bar{r}_1(a), \bar{r}_4(b))$. We have $(\bar{r}_1(a), a) \in T$, $(a, b) \in A$, $(b, \bar{r}_4(b)) \in T$ and so $(\bar{r}_1(a), \bar{r}_4(b)) \in (A \vee T) \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_n$ be an $A \cup (T \cap B)$-proof from $\bar{r}_1(a)$ to $\bar{r}_4(b)$. Evidently, $\{\bar{r}_1(a), \bar{r}_1(b), \bar{r}_4(a), \bar{r}_4(b)\}$ is a block of B and $\{\bar{r}_1(a), \bar{r}_1(b)\}$ is a block of A; hence every member of $a_0, \ldots, a_n$ equals either $\bar{r}_1(a)$ or $\bar{r}_1(b)$, a contradiction.

We have proved that either $a \leqq b$ or $b \leqq a$. Now it remains to derive a contradiction from $b \leqq a$. However, if $b \leqq a$, then $f(b)$ is a subterm of a for a substitution f; by 7.2 we may suppose that f is an automorphism of W_Δ. Let a' be the term obtained from a by replacing the subterm $f(b)$ by $f\,\bar{r}_4(b)$. We have $(a, a') \in T$ and so $a' \in \{a, \bar{r}_1(a)\}$, so that $f\,\bar{r}_4(b) \in \{f(b), \bar{r}_1\,f(b)\}$; this is evidently a contradiction.

7.5. Lemma. *Let f be a substitution such that $f(x_1) \in V$, $f(x_2) \in V$ and $f(x_1), f(x_2) \notin$ var $(f(x_3))$. Let a be a term such that* var $(a) = \{x_1, x_2, x_3\}$ *and $f(a)$ is a constant extension of a. Then $a = f(a)$.*

Proof. Suppose that there is a term a such that var $(a) = \{x_1, x_2, x_3\}$, $f(a)$ is a constant extension of a and $a \neq f(a)$; let us take such a term a of minimal length. Since each of the terms $f(x_1), f(x_2), f(x_3)$ contains at most two variables, a is not a subterm of any of the terms $f(x_1), f(x_2), f(x_3)$. Hence $a = f(d)$ for a subterm d of a; since $a \neq f(a)$, d is a proper subterm of a. There exist a variable x and a term t with a single occurrence of x such that $a = t_{(x)}[d]$. Since $\lambda(d) < \lambda(a)$, it follows from the minimality of $\lambda(a)$ that a is not a constant extension of d; hence there exists a variable $y \in$ var (d) different from x. But then $f(y)$ is a term containing no variable; since $f(x_1) \in V$ and $f(x_2) \in V$, we get $y = x_3$. We get var $(f(a)) = \{f(x_1), f(x_2)\}$, a contradiction.

7.6. Lemma. *Let T be modular. Let $a \in V_1$. Let $x \in V$, $t \in W_\Delta$,* $\operatorname{var}(t) = \{x\}$, *$t \neq x$ and let x have a single occurrence in t. Then there exists a positive integer k with $G_T(t^{(k)}[a]) = S_{\{x_1,x_2,x_3\}}$.*

Proof. Suppose that there is no such k. Denote by A the equational theory generated by $(a, t[\bar{r}_2(a)])$ and by B the equational theory generated by $(a, t[\bar{r}_2(a)])$, $(a, \bar{r}_4(a))$. Put

$$Z = \{t^{(i)}[\bar{p}(a)];\ p \in \{1, r_4, r_5\},\ i \geqq 0,\ i \text{ even}\} \cup$$

$$\cup \{t^{(i)}[\bar{p}(a)];\ p \in \{r_1, r_2, r_3\},\ i \geqq 1,\ i \text{ odd}\}.$$

We have $Z \cap U = \emptyset$. Let us prove that if $d \in Z$ and e is a term such that either (d, e) or (e, d) is an immediate consequence of one of the equations $(a, t[\bar{r}_2(a)])$ and $(a, \bar{r}_4(a))$, then $e \in Z$. There exists a substitution f such that either $f(a)$ or $f(t[\bar{r}_2(a)])$ or $f(a)$ or $f\,\bar{r}_4(a)$ is a subterm of d and e results from d by replacing one occurrence of this subterm by $f(t[\bar{r}_2(a)])$ or $f(a)$ or $f\,\bar{r}_4(a)$ or $f(a)$. If $f(a)$ is a subterm then it follows from 7.1 that $f(x_1) \in V$, $f(x_2) \in V$ and $f(x_1), f(x_2) \notin \operatorname{var}(f(x_3))$; applying 7.5 we see that the restriction of f to $\{x_1, x_2, x_3\}$ is a permutation; this implies that $e \in Z$. In the remaining three cases we similarly obtain $e \in Z$, too. Put

$$Y = \{t^{(i)}[a];\ i \geqq 0,\ i \text{ even}\} \cup \{t^{(i)}[\bar{r}_2(a)];\ i \geqq 1,\ i \text{ odd}\}.$$

We can prove similarly that if $d \in Y$ and e is a term such that either (d, e) or (e, d) is an immediate consequence of $(a, t[\bar{r}_2(a)])$, then $e \in Y$. We have $(a, \bar{r}_4(a)) \in (A \vee T) \cap B = A \vee (T \cap B)$ and so there exists an $A \cup (T \cap B)$-proof $a_0, \ldots, a_n$ from a to $\bar{r}_4(a)$. By induction on i we see that $a_i \in Y$ for all $i \in \{0, \ldots, n\}$; for $i = n$ we get a contradiction.

8. DIRECT IMPLICATION: FOUR VARIABLES

Define r_1, r_2, r_3, r_4, r_5 in the same way as in Section 7. Put

$$V_3 = \{a \in W_\Delta;\ \operatorname{var}(a) = \{x_1, x_2, x_3, x_4\},\quad G_T(a) = R_1\},$$

$$V_4 = \{a \in W_\Delta;\ \operatorname{var}(a) = \{x_1, x_2, x_3, x_4\},\quad G_T(a) = A_{\{x_1,x_2,x_3,x_4\}}\}.$$

8.1. Lemma. *Let $a \in V_3$ and let f be a substitution such that $f(a) \notin U$. Then $a \sim f(a)$.*

Proof. For every integer m denote by $c(m)$ the number from $\{1, 2, 3, 4\}$ congruent with m modulo 4. Let $i \in \{1, 2, 3, 4\}$. Let x be a variable not belonging to $\operatorname{var}(f(a)) \cup \cup \{x_1, x_2, x_3, x_4\}$. Denote by p the extension of $[x_1, x_2, x_3, x_4]$ to an automorphism of W_Δ; denote by g the substitution with $g(x_i) = x$ and $g(x_j) = f(x_j)$ for all $j \in \in \{1, 2, 3, 4\} \setminus \{i\}$. We have $g(a) \notin U$ and $(g(a), g\,p(a)) \in T$, so that $q\,g(a) = g\,p(a)$

for an automorphism q of W_4. Hence $q(x) = f(x_{c(i+1)})$, $q f(x_{c(i-1)}) = x$, $q f(x_{c(i+1)}) = f(x_{c(i+2)})$, $q f(x_{c(i+2)}) = f(x_{c(i-1)})$. Hence it follows that $f(x_{c(i-1)})$ is a variable, $f(x_{c(i-1)}) \neq f(x_{c(i+1)})$ and $f(x_{c(i-1)}) \neq f(x_{c(i+2)})$. Since $i \in \{1, 2, 3, 4\}$ was arbitrary, we see that $f(x_1), f(x_2), f(x_3), f(x_4)$ are pairwise different variables, i.e. $a \sim f(a)$.

8.2. Lemma. *Let $a \in V_4$ and let f be a substitution such that $f(a) \notin U$. Then $a \sim f(a)$.*

Proof. Let x, y, z be three different variables not belonging to $\operatorname{var}(f(a)) \cup \cup \{x_1, x_2, x_3, x_4\}$. Denote by g the substitution with $g(x_1) = f(x_1)$, $g(x_2) = x$, $g(x_3) = y$, $g(x_4) = z$. We have $g(a) \notin U$ and $(g(a), g\,\bar{r}_4(a)) \in T$, so that $p\,g(a) = g\,\bar{r}_4(a)$ for an automorphism p of W_4. Hence $p\,g(x_1) = g\,\bar{r}_4(x_1)$, i. e. $p f(x_1) = x$; we get $f(x_1) \in V$. Similarly $f(x_2), f(x_3), f(x_4) \in V$. Denote by h the substitution with $h(x_1) = f(x_1)$, $h(x_2) = f(x_2)$, $h(x_3) = x$, $h(x_4) = y$. We have $h(a) \notin U$ and $(h(a), h\,\bar{r}_4(a)) \in T$, so that $q\,h(a) = h\,\bar{r}_4(a)$ for an automorphism q of W_4. Hence $q\,h(x_1) = h\,\bar{r}_4(x_1)$ and $q\,h(x_2) = h\,\bar{r}_4(x_2)$, i.e. $q f(x_1) = f(x_2)$ and $q f(x_2) = x$. This implies that $f(x_1) \neq f(x_2)$. Similarly $f(x_1) \neq f(x_3)$, $f(x_1) \neq f(x_4)$, $f(x_2) \neq f(x_3)$, $f(x_2) \neq f(x_4)$, $f(x_3) \neq f(x_4)$. Hence $a \sim f(a)$.

8.3. Lemma. *Let T be modular and $a, b \in V_3$. Then either $a \leqq b$ or $b \leqq a$.*

Proof. Suppose that $a \nleqq b$ and $b \nleqq a$. Denote by A the equational theory generated by $(a, \bar{r}_1(b))$ and by B the equational theory generated by $(a, \bar{r}_1(b))$, $(a, \bar{r}_3(b))$. We have $(a, \bar{r}_2(a)) \in T$, $(\bar{r}_2(a), \bar{r}_4(b)) \in A$, $(\bar{r}_4(b), \bar{r}_3(b)) \in T$ and so $(a, \bar{r}_3(b)) \in (A \vee T) \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_n$ be a minimal $A \cup (T \cap B)$-proof from a to $\bar{r}_3(b)$. Evidently $\{a, \bar{r}_4(a), \bar{r}_5(a), \bar{r}_1(b), \bar{r}_2(b), \bar{r}_3(b)\}$ is a block of B and $\{a, \bar{r}_1(b)\}$ is a block of A; hence every member of $a_0, \ldots, a_n$ equals either a or $\bar{r}_1(b)$, a contradiction.

8.4. Lemma. *Let T be modular, $a \in V_3$ and $b \in V_4$. Then either $a \leqq b$ or $b \leqq a$.*

Proof. Suppose that $a \nleqq b$ and $b \nleqq a$. Denote by A the equational theory generated by (a, b) and by B the equational theory generated by (a, b), $(\bar{r}_2(a), \bar{r}_4(b))$. We have $(\bar{r}_2(a), a) \in T$, $(a, b) \in A$, $(b, \bar{r}_4(b)) \in T$ and so $(\bar{r}_2(a), \bar{r}_4(b)) \in (A \vee T) \cap \cap B = A \vee (T \cap B)$. Let $a_0, \ldots, a_n$ be an $A \cup (T \cap B)$-proof from $\bar{r}_2(a)$ to $\bar{r}_4(b)$. Evidently, $\{\bar{r}_2(a), \bar{r}_4(a), \bar{r}_2(b), \bar{r}_4(b)\}$ is a block of B and $\{\bar{r}_2(a), \bar{r}_2(b)\}$ is a block of A, so that every member of $a_0, \ldots, a_n$ equals either $\bar{r}_2(a)$ or $\bar{r}_2(b)$, a contradiction.

8.5. Lemma. *Let T be modular, $a \in V_3$ and $b \in V_4$. Then $a < b$.*

Proof. By 8.4 it is enough to derive a contradiction from $b \leqq a$. However, if $b \leqq a$, then $f(b)$ is a subterm of a for a substitution f; by 8.2 we may suppose $f = \bar{g}$ for a permutation g of $\{x_1, x_2, x_3, x_4\}$. Let a' be the term obtained from a by replacing one occurrence of the subterm $f(b)$ by $f\,\bar{r}_4(b)$. We have $(a, a') \in T$ and so $a' = \bar{p}(a)$ for some $p \in R_1$. Hence $f\,\bar{r}_4(b) = \bar{p}\,f(b)$, $gr_4 = pg$, $gr_4g^{-1} \in R_1$, evidently a contradiction.

8.6. Lemma. *Let T be modular. Then either V_3 or V_4 is empty.*

Proof. Suppose that there exist terms $a \in V_3$ and $b \in V_4$. By 8.1 and 8.5 there exist a variable x, a term t and a permutation $p \in S_{\{x_1,x_2,x_3,x_4\}}$ such that $x \notin \{x_1, x_2, x_3, x_4\}$, x has a single occurrence in t and $b = t_{(x)}[\bar{p}(a)]$. Let us prove $\operatorname{var}(t) = \{x\}$. Suppose, on the contrary, that a variable $y \in \{x_1, x_2, x_3, x_4\}$ belongs to $\operatorname{var}(t)$. There exists a permutation $q \in R_1$ such that $pqp^{-1}(y) \neq y$. We have $(a, \bar{q}(a)) \in T$, $(\bar{p}(a), \bar{p}\,\bar{q}(a)) \in T$, $(t_{(x)}[\bar{p}(a)],\ t_{(x)}[\bar{p}\,\bar{q}(a)]) \in T$ where $t_{(x)}[\bar{p}(a)] = b$ and so $t_{(x)}[\bar{p}\,\bar{q}(a)] = \bar{r}(t_{(x)}[\bar{p}(a)])$ for some $r \in S_{\{x_1,x_2,x_3,x_4\}}$; since $y \in \operatorname{var}(t) \setminus \{x\}$, we get $r(y) = y$; we have $pqp^{-1}(y) = rpp^{-1}(y) = r(y) = y$, a contradiction. Thus $\operatorname{var}(t) = \{x\}$. There exists an odd permutation $s \in G_T(a)$. We have $(a, \bar{s}(a)) \in T$, $(\bar{p}(a), \bar{p}\,\bar{s}(a)) \in T$, $(\bar{p}(a), \bar{p}\bar{s}\bar{p}^{-1}\,\bar{p}(a)) \in T$, $(b, \bar{p}\bar{s}\bar{p}^{-1}(b)) \in T$, $psp^{-1} \in G_T(b)$, so that psp^{-1} is an even permutation, a contradiction, since s is odd.

8.7. Lemma. *Let T be modular. Let $a \in V_3$. Let $x \in V$, $t \in W_\Delta$, $\operatorname{var}(t) = \{x\}$, $t \neq x$ and let x have a single occurrence in t. Then there exists a positive integer k with $G_T(t^{(k)}[a]) = S_{\{x_1,x_2,x_3,x_4\}}$.*

Proof. Suppose that there is no such k, so that $G_T(t^{(k)}[a]) = R_1$ for all $k \geqq 0$. Put $p = [x_1, x_3, x_4]$, $q = [x_1, x_4, x_3]$, $r = [x_1, x_3]$, $s = [x_3, x_4]$. Denote by A the equational theory generated by $(a, t[\bar{p}(a)])$ and by B the equational theory generated by $(a, t[\bar{p}(a)])$, $(a, t[\bar{q}(a)])$. We have $(a, \bar{r}(a)) \in T$, $(\bar{r}(a), t[\bar{s}(a)]) \in A$, $(t[\bar{s}(a)], t[\bar{q}(a)]) \in T$ and so $(a, t[\bar{q}(a)]) \in (A \vee T) \cap B = A \vee (T \cap B)$. Put

$$Z = \{t^{(i)}[a];\ i \geqq 0\} \cup \{t^{(i)}[\bar{p}(a)];\ i \geqq 0\} \cup \{t^{(i)}[\bar{q}(a)];\ i \geqq 0\}\,.$$

We have $Z \cap U = \emptyset$. Similarly as in the proof of 7.6, Z is a block of B. Similarly, the set

$$Y = \{t^{(i)}[a];\ i \geqq 0,\ i \equiv 0 \pmod 3\} \cup \{t^{(i)}[\bar{p}(a)];\ i \geqq 0,\ i \equiv 1 \pmod 3\} \cup$$
$$\cup \{t^{(i)}[\bar{q}(a)];\ i \geqq 0,\ i \equiv 2 \pmod 3\}$$

is a block of A. Let $a_0, \ldots, a_n$ be an $A \cup (T \cap B)$-proof from a to $t[\bar{q}(a)]$. By induction on i we get $a_i \in Y$ for all $i \in \{0, \ldots, n\}$, a contradiction.

9. CONVERSE IMPLICATION: PRELIMINARIES

9.1. Lemma. *Let the equational theory T be such that the conditions* (1) *and* (2) *are satisfied. Then either $T \subseteq E_\Delta$ or $U \times U$ is a block of T.*

Proof. Let $T \nsubseteq E_\Delta$ and $u, v \in U$; it is enough to prove that $(u, v) \in T$. There exist terms a, b and a variable x such that $(a, b) \in T$ and $x \in \operatorname{var}(a) \setminus \operatorname{var}(b)$. We have $(a, \sigma^x_{F(x,\ldots,x)}(a)) \in T$ (where F is an arbitrary non-nullary symbol from Δ) and so $a \in U$. Define four substitutions f, g, h, k as follows: $f(y) = u$ for all $y \in V$; $g(y) = v$ for all $y \in V$; $h(x) = v$; $h(y) = u$ for all $y \in V \setminus \{x\}$; $k(x) = u$; $k(y) = v$ for all $y \in V \setminus \{x\}$. The terms $f(a), g(a), h(a), k(a)$ belong to U by (1). If $\operatorname{var}(a) = \{x\}$ then $(u, f(a)) \in T$ by (2), $(f(a), g(a)) \in T$ evidently and $(g(a), v) \in T$ by (2); hence $(u, v) \in T$. If $\operatorname{var}(a) \neq \{x\}$ then $(u, f(a)) \in T$ by (2), $(f(a), h(a)) \in T$ evidently, $(h(a), k(a)) \in T$ by (2), $(k(a), g(a)) \in T$ evidently and $(g(a), v) \in T$ by (2); hence $(u, v) \in T$ again.

In order to prove the converse implication of Theorem 5.1, we shall suppose that the equational theory T satisfies the conditions (1), ..., (9) and that it is not a modular element of $\mathscr{L}_\Delta$. Hence Pent (T, A, B, C, D) for a quadruple A, B, C, D of elements of $\mathscr{L}_\Delta$; let us fix such a quadruple A, B, C, D. By 9.1, either $T \subseteq E_\Delta$ or $U \times U$ is a block of T. The set U is non-empty, since $U = \emptyset$ would imply $T = 1_{W_\Delta}$ and 1_{W_Δ} is a modular element of $\mathscr{L}_\Delta$.

9.2. Lemma. *There exists a non-empty finite sequence $a_0, \ldots, a_n$ with the following three properties:*

(i) *$a_0, \ldots, a_n$ is a $T \cup A$-proof (i.e. $(a_{i-1}, a_i) \in T \cup A$ for all $i \in \{1, \ldots, n\}$) and $(a_0, a_n) \in B \setminus A$;*

(ii) *if $b_0, \ldots, b_m$ is any $T \cup A$-proof such that $(b_0, b_m) \in B \setminus A$, then $n \leqq m$;*

(iii) *if $b_0, \ldots, b_n$ is a $T \cup A$-proof such that $(b_0, b_n) \in B \setminus A$, then*

$$\operatorname{Card}(\operatorname{var}(a_0) \cup \ldots \cup \operatorname{var}(a_n)) \leqq \operatorname{Card}(\operatorname{var}(b_0) \cup \ldots \cup \operatorname{var}(b_n)).$$

Proof. Since $A \subset B$, there exists an equation $(a, b) \in B \setminus A$; since $B \subseteq T \vee A$, there exists a $T \cup A$-proof from a to b. Now the assertion is evident.

In the following let $a_0, \ldots, a_n$ be one fixed $T \cup A$-proof satisfying the three conditions of 9.2.

9.3. Lemma. *$n \geqq 3$, n is odd, $(a_{i-1}, a_i) \in T \setminus A$ if i is odd and $(a_{i-1}, a_i) \in A \setminus T$ if i is even ($i \in \{1, \ldots, n\}$). Further,* $\operatorname{var}(a_i) \subseteq \operatorname{var}(a_0) \cup \operatorname{var}(a_n)$ *for all $i \in \{0, \ldots, n\}$.*

Proof. It is evident.

For every odd integer $i \in \{1, \ldots, n\}$ such that $a_i \notin U$ we denote by p_i the permutation of $\operatorname{var}(a_{i-1})$ with $a_i = \bar{p}_i(a_{i-1})$; put $q_i = \bar{p}_i$.

9.4. Lemma. *Let $U \times U$ be a block of T. Then* $\operatorname{var}(a_0) = \operatorname{var}(a_1) = \ldots = \operatorname{var}(a_n)$ *and $a_0, a_1, \ldots, a_n \notin U$.*

Proof. If it were $a_0 \in U$ and $a_n \in U$ simultaneously, then $(a_0, a_n) \in T \cap B \subseteq A$, a contradiction with 9.2(i). Hence either $a_0 \notin U$ or $a_n \notin U$. It is enough to consider the case $a_0 \notin U$. We shall prove by induction on $i \in \{0, \ldots, n\}$ that $\operatorname{var}(a_0) = \ldots$

$\ldots = \operatorname{var}(a_i)$ and $a_0, \ldots, a_i \notin U$. This is clear if either $i = 0$ or i is odd. Let $i \geqq 2$ be even. We have $\operatorname{var}(a_0) = \ldots = \operatorname{var}(a_{i-1})$ and $a_0, \ldots, a_{i-1} \notin U$ by induction. If it were $a_i \in U$ then evidently $a_0, \ldots, a_{i-2}, q_{i-1}^{-1}(a_i), a_{i+1}, \ldots, a_n$ would be a $T \cup A$-proof, a contradiction with the minimality of $a_0, \ldots, a_n$. Thus $a_i \notin U$ and it remains to prove $\operatorname{var}(a_{i-1}) = \operatorname{var}(a_i)$. Suppose that there exists a variable $z \in (\operatorname{var}(a_{i-1}) \smallsetminus \operatorname{var}(a_i)) \cup (\operatorname{var}(a_i) \smallsetminus \operatorname{var}(a_{i-1}))$. Take a term $t \in U$. We have either $\sigma_t^z(a_{i-1}) \in U$ and $\sigma_t^z(a_i) = a_i$ or $\sigma_t^z(a_i) \in U$ and $\sigma_t^z(a_{i-1}) = a_{i-1}$. In both cases there evidently exists a term $w \in U$ with $(a_{i-1}, w) \in A$ and $(a_i, w) \in A$. If $i > 2$ then $a_0, \ldots, a_{i-3}, q_{i-1}^{-1}(w), q_{i+1}(w), a_{i+1}, \ldots, a_n$ is a $T \cup A$-proof, a contradiction with the minimality of $a_0, \ldots, a_n$. If $i + 1 < n$ then $a_0, \ldots, a_{i-2}, q_{i-1}^{-1}(w), q_{i+1}(w), a_{i+2}, \ldots, a_n$ is a $T \cup A$-proof, a contradiction again. If $i = 2$ and $i + 1 = n$ then $(q_1^{-1}(w), q_3(w)) \in B \cap T \subseteq A$ and so $(a_0, a_n) \in A$, a contradiction.

9.5. Lemma. *Let $T \subseteq E_\Delta$. Then either $a_0 \notin U$ or $a_n \notin U$.*

Proof. Suppose that $a_0 \in U$ and $a_n \in U$. Then $\operatorname{var}(a_0) \neq \operatorname{var}(a_n)$, since otherwise we would have $(a_0, a_n) \in T \cap B \subseteq A$ by (2). It is enough to consider the case $\operatorname{var}(a_0) \smallsetminus \operatorname{var}(a_n) \neq \emptyset$. For every $i \in \{0, \ldots, n\}$ define a substitution f_i as follows: if $x \in V \smallsetminus (\operatorname{var}(a_0) \smallsetminus \operatorname{var}(a_n))$ then $f_i(x) = x$; if $x \in \operatorname{var}(a_0) \smallsetminus \operatorname{var}(a_n)$ then $f_i(x) = a_i$. If i is odd then $(f_{i-1}(a_0), f_i(a_0)) \in T \cap B \subseteq A$; if i is even then $(f_{i-1}(a_0), f_i(a_0)) \in A$ is even more evident. Hence $(f_{i-1}(a_0), f_i(a_0)) \in A$ for all i and so $(f_0(a_0), f_n(a_0)) \in A$. We have evidently $(a_0, f_0(a_0)) \in T \cap B \subseteq A$ and so $(a_0, f_n(a_0)) \in A$. Further, it is evident that $(f_n(a_0), a_n) \in T$. This shows that $a_0, f_n(a_0), a_n$ is a $T \cup A$-proof, evidently a contradiction.

9.6. Lemma. *Δ contains a symbol of arity $\geqq 2$.*

Proof. By 9.1, 9.4 and 9.5 it is enough to consider the case $a_0 \notin U$. Then $a_1 = \bar{p}_1(a_0)$ where p_1 is a permutation of $\operatorname{var}(a_0)$; since $a_0 \neq a_1$, we get $\operatorname{Card}(\operatorname{var}(a_0)) \geqq 2$ and so Δ contains a symbol of arity $\geqq 2$.

Let us fix a variable $z \notin \operatorname{var}(a_0) \cup \operatorname{var}(a_n)$. Denote by H the set of all the terms u such that $(u, v) \in A$ for a term v with $z \in \operatorname{var}(v)$.

9.7. Lemma. *Let $T \subseteq E_\Delta$. Then either $a_0 \notin H$ or $a_n \notin H$.*

Proof. Suppose $a_0 \in H$ and $a_n \in H$, so that $(a_0, v_0) \in A$ and $(a_n, v_n) \in A$ for some terms v_0, v_n containing z. By 9.4 there exists a term $t \in U$ with $\operatorname{var}(t) = \operatorname{var}(a_0) \cup \operatorname{var}(a_n)$. Define a substitution f as follows: if $x \in \operatorname{var}(a_0) \cup \operatorname{var}(a_n)$ then $f(x) = x$; if $x \in V \smallsetminus (\operatorname{var}(a_0) \cup \operatorname{var}(a_n))$ then $f(x) = t$. We have $(a_0, f(v_0)) \in A$, $(f(v_0), f(v_n)) \in T$, $(f(v_n), a_n) \in A$, evidently a contradiction.

9.8. Lemma. *Let $T \subseteq E_\Delta$ and $a_0 \notin U$. Let $i \in \{1, \ldots, n\}$ be such that* $\operatorname{var}(a_0) = \operatorname{var}(a_1) = \ldots = \operatorname{var}(a_i)$. *Then $a_i \notin U$.*

Proof. Suppose $a_i \in U$; it is enough to consider the case when i is the least integer with $a_i \in U$. Then i is even and $a_0, q_1^{-1}(a_2), \ldots, q_1^{-1}(a_i), a_{i+1}, \ldots, a_n$ is a $T \cup A$-proof of length $n - 1$, a contradiction.

9.9. Lemma. *Let* $T \subseteq E_\Delta$ *and let there exist an* $i \in \{1, \ldots, n\}$ *with* $\operatorname{var}(a_{i-1}) \neq \operatorname{var}(a_i)$. *If* $a_0 \notin U$ *then* $a_0 \in H$; *if* $a_n \notin U$ *then* $a_n \in H$.

Proof. It is enough to prove $a_0 \in H$ under the assumption $a_0 \notin U$. Let i be the least integer with $\operatorname{var}(a_{i-1}) \neq \operatorname{var}(a_i)$. By 9.8, $a_j \notin U$ for all $j \in \{0, \ldots, i - 1\}$. We have $(q_{i-1}q_{i-3} \ldots q_1(a_0), a_i) \in A$, $\operatorname{var}(q_{i-1}q_{i-3} \ldots q_1(a_0)) = \operatorname{var}(a_0)$, $\operatorname{var}(a_i) \neq \operatorname{var}(a_0)$ and so evidently $a_0 \in H$.

9.10. Lemma. *Let* $T \subseteq E_\Delta$. *Then* $\operatorname{var}(a_0) = \operatorname{var}(a_1) = \ldots = \operatorname{var}(a_n)$.

Proof. By 9.5 it is enough to consider the case $a_0 \notin U$. Suppose $\operatorname{var}(a_{i-1}) \neq \operatorname{var}(a_i)$ for some i. By 9.9, $a_0 \in H$. By 9.7, $a_n \notin H$. By 9.9, $a_n \in U$. If $\operatorname{var}(a_0) \subseteq \operatorname{var}(a_n)$ then $a_0, q_1^{-1}(a_2), q_1^{-1}(a_3), \ldots, q_1^{-1}(a_{n-1}), a_n$ is a $T \cup A$-proof of length $n - 1$, a contradiction. Hence there exists a variable $x \in \operatorname{var}(a_0) \setminus \operatorname{var}(a_n)$. Evidently there exists a variable $y \in \operatorname{var}(a_0) \setminus \{x\}$. We have $(\sigma_y^x(a_0), a_n) \in A$, since otherwise $\sigma_y^x(a_0), \ldots, \sigma_y^x(a_n)$ would be a $T \cup A$-proof contradicting 9.2(iii). Since $a_0 \in H$, there is a term u with $(a_0, u) \in A$ and $z \in \operatorname{var}(u)$. Hence $(\sigma_y^x(a_0), \sigma_y^x(u)) \in A$, so that $(a_n, \sigma_y^x(u)) \in A$; we have $z \in \operatorname{var}(\sigma_y^x(u))$ and so $a_n \in H$, a contradiction.

9.11. Lemma. *We have* $\operatorname{var}(a_0) = \operatorname{var}(a_1) = \ldots = \operatorname{var}(a_n)$ *and* $a_0, a_1, \ldots, a_n \notin U$.

Proof. It follows from 9.1, 9.4, 9.10, 9.5, 9.8 and the assertion symmetric to 9.8.

It follows that the permutations p_i of $\operatorname{var}(a_0)$ are defined for every odd $i \in \{1, \ldots, n\}$; we have $q_i = \bar{p}_i$ and $a_i = q_i(a_{i-1})$.

9.12. Lemma. *Let* $i \in \{0, \ldots, n - 3\}$ *be even. Then* $p_{i+1} \notin G_T(a_{i+2})$ *and* $p_{i+3} \notin G_T(a_i)$. *Hence* $G_T(a_i) \nsubseteq G_T(a_{i+2})$ *and* $G_T(a_{i+2}) \nsubseteq G_T(a_i)$.

Proof. Suppose $p_{i+1} \in G_T(a_{i+2})$. Then $p_{i+1}p_{i+3} \in G_T(a_{i+2})$, $(a_{i+2}, q_{i+1}q_{i+3}(a_{i+2})) \in T$, $(q_{i+1}^{-1}(a_{i+2}), a_{i+3}) \in T$ and $a_0, \ldots, a_i, q_{i+1}^{-1}(a_{i+2}), a_{i+3}, \ldots, a_n$ is a $T \cup A$-proof of length $n - 1$, a contradiction. Similarly we can prove that $p_{i+3} \notin G_T(a_i)$.

9.13. Lemma. *Either* $\operatorname{Card}(\operatorname{var}(a_0)) = 3$ *or* $\operatorname{Card}(\operatorname{var}(a_0)) = 4$.

Proof. It follows from 9.12, since if $\operatorname{Card}(M) \notin \{3, 4\}$ and H_1, H_2 are two modular elements of the subgroup lattice of S_M, then either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$ by 3.1.

In this section we shall suppose that the $T \cup A$-proof $a_0, \ldots, a_n$ from Section 9 is such that $\operatorname{var}(a_0) = \{x_1, x_2, x_3\}$. Define $r_1, \ldots, r_5$ in the same way as in Section 7. It follows from 9.11, 9.12 and 3.7 that for every odd $i \in \{1, \ldots, n\}$ we have $G_T(a_{i-1}) = G_T(a_i) \in \{\{1, r_1\}, \{1, r_2\}, \{1, r_3\}, \{1, r_4, r_5\}\}$ and if $i \leqq n - 2$ then $G_T(a_i) \neq G_T(a_{i+2})$.

10.1. Lemma. *Let $i \in \{1, \ldots, n\}$ be odd, $p \in S_{\{x_1,x_2,x_3\}}$ and $(a_i, \bar{p}(a_i)) \in A$. Then $p = 1$.*

Proof. Suppose $p \neq 1$. Put $G = \{q \in S_{\{x_1,x_2,x_3\}};\ (a_i, \bar{q}(a_i)) \in A\}$ and $H = \{q \in S_{\{x_1,x_2,x_3\}};\ (a_i, \bar{q}(a_i)) \in B\}$. We have $(a_0, \bar{r}(a_i)) \in A$ and $(\bar{s}(a_i), a_n) \in A$ for some $r, s \in S_{\{x_1,x_2,x_3\}}$. Hence $(\bar{r}(a_i), \bar{s}(a_i)) \in B \setminus A$ and so G is a proper subgroup of H; since $G \neq \{1\}$, we get $H = S_{\{x_1,x_2,x_3\}}$ by 3.7. Hence $(a_{i-1}, a_i) \in B \cap T \subseteq A$, a contradiction.

10.2. Lemma. *Let $i \in \{1, \ldots, n\}$ be odd. Then $G_T(a_i) \neq \{1, r_4, r_5\}$.*

Proof. Suppose $G_T(a_i) = \{1, r_4, r_5\}$. It is enough to consider the case $i \geqq 3$, since otherwise we would have $i \leqq n - 2$ and the proof would be analogous in that case. We have $G_T(a_{i-2}) \neq \{1, r_4, r_5\}$ and so $G_T(a_{i-2}) = \{1, r\}$ for some $r \in \{r_1, r_2, r_3\}$. We have $p_{i-2} = r$ and $p_i \in \{r_4, r_5\}$. By (5) we have $a_{i-2} < a_{i-1}$. Let $x \in V \setminus \{x_1, x_2, x_3\}$. There exist a substitution f and a term t with a single occurrence of x such that $a_{i-1} = t_{(x)}[f(a_{i-2})]$. By 7.1, two of the terms $f(x_1), f(x_2), f(x_3)$ are variables not contained in the remaining term. If it were $(a_{i-2}, u) \in A$ for some $u \in U$, then evidently $(a_{i-2}, v) \in A$ for some $v \in U$ with $\operatorname{var}(v) = \{x_1, x_2, x_3\}$; then $(a_{i-3}, q_{i-2}(v)) \in A$, $(q_{i-2}(v), q_i(v)) \in T$, $(q_i(v), a_i) \in A$, so that $a_0, \ldots, a_{i-3}, q_{i-2}(v), q_i(v), a_i, \ldots, a_n$ would be a $T \cup A$-proof of length n contradicting 9.3. Hence there is no $u \in U$ with $(a_{i-2}, u) \in A$. We have $(a_{i-2}, t_{(x)}[f(a_{i-1})]) \in A$ and so $t_{(x)}[f(a_{i-1})] \notin U$; since $(t_{(x)}[f(a_{i-1})], t_{(x)}[f\bar{r}_4(a_{i-1})]) \in T$, there exists a $p \in S_{\{x_1,x_2,x_3\}}$ with $\bar{p}(t_{(x)}[f(a_{i-1})]) = t_{(x)}[f\bar{r}_4(a_{i-1})]$. Hence $\bar{p}f(a_{i-1}) = f\bar{r}_4(a_{i-1})$, $\bar{p}f(x_1) = f(x_2)$, $\bar{p}f(x_2) = f(x_3)$, $\bar{p}f(x_3) = f(x_1)$. This implies that $f(x_1), f(x_2), f(x_3)$ are pairwise different variables and we can assume that $f = \bar{g}$ for some $g \in S_{\{x_1,x_2,x_3\}}$. We have $(t_{(x)}[f(a_{i-2})], t_{(x)}[f(a_{i-3})]) \in T$ and $t_{(x)}[f(a_{i-2})] = a_{i-1}$; hence there exists a permutation $q \in \{1, r_4, r_5\}$ with $\bar{q}(a_{i-1}) = t_{(x)}[f(a_{i-3})]$. Hence $\bar{q}f(a_{i-2}) = f q_{i-2}(a_{i-2})$, $qg = gr$, $q \in \{r_1, r_2, r_3\}$, a contradiction.

10.3. Lemma. *Let $i \in \{1, \ldots, n\}$ be odd. Then there is no u with $(a_{i-1}, u) \in A$ and $(u, \bar{r}_4(u)) \in T$.*

Proof. Suppose that there is such a term u. It is enough to suppose $i \leqq n - 2$. By 10.2, $p_{i+2}p_i \in \{r_4, r_5\}$. We have $(a_{i+2}, q_{i+2}\, q_i(u)) \in A$ and $(u, q_{i+2}\, q_i(u)) \in T$; hence $a_0, \ldots, a_{i-1}, u, q_{i+2}\, q_{i+1}(u), a_{i+2}, \ldots, a_n$ is a $T \cup A$-proof contradicting 9.3.

Let us fix an odd number $i \in \{1, \ldots, n-2\}$. It follows from 10.1 that the terms a_i, a_{i+1} are not similar; by (4), it follows from 10.2 that either $a_i < a_{i+1}$ or $a_{i+1} < a_i$. We shall assume $a_i < a_{i+1}$; in the other case we could proceed similarly. Let x be a variable not belonging to $\{x_1, x_2, x_3\}$. There exist a substitution f and a term t with a single occurrence of x such that $a_{i+1} = t_{(x)}[f(a_i)]$ and $f(y) = y$ for all $y \in V \setminus \{x_1, x_2, x_3\}$.

10.4. Lemma. *f is an automorphism of W_Δ and* $\operatorname{var}(t) = \{x\}$.

Proof. There exists a unique triple (y_1, y_2, y_3) such that $\{y_1, y_2, y_3\} = \{x_1, x_2, x_3\}$, $p_i = [y_1, y_2]$ and $p_{i+2} = [y_2, y_3]$. By 7.1, $f(y_1)$ and $f(y_2)$ are variables not contained in $f(y_3)$. We have $(a_{i+1}, t_{(x)}[f(a_{i+1})]) \in A$ and $(t_{(x)}[f(a_{i+1})],$ $t_{(x)}[f\, q_{i+2}(a_{i+1})]) \in T$, so that by 10.3 there is a permutation $p \in S_{\{x_1,x_2,x_3\}} \setminus \{r_4, r_5\}$ with $\bar{p}(t_{(x)}[f(a_{i+1})]) = t_{(x)}[f q_{i+2}(a_{i+1})]$. We have $\bar{p} f(a_{i+1}) = f\, q_{i+2}(a_{i+1})$, $\bar{p} f(y_1) = f(y_1)$, $\bar{p} f(y_2) = f(y_3)$, $\bar{p} f(y_3) = f(y_2)$. Hence $f(y_1), f(y_2), f(y_3)$ are three pairwise different variables and f is an automorphism. We have $(t_{(x)}[f(a_i)],$ $t_{(x)}[f\, q_i(a_i)]) \in T$; there exists a $q \in \{1, p_{i+2}\}$ with $\bar{q}(t_{(x)}[f(a_i)]) = t_{(x)}[f\, q_i(a_i)]$; evidently $q \neq 1$ and so $q = p_{i+2}$; hence $q_{i+2} f = f q_i$. We get $q_{i+2} f(y_3) = f(y_3)$ and so $f(y_3) = y_1$. From $q_{i+2}(t_{(x)}[f(a_i)]) = t_{(x)}[f\, q_i(a_i)]$ we get $y_2, y_3 \notin \operatorname{var}(t)$. If it were $y_1 \in \operatorname{var}(t)$ then $\bar{p}(t_{(x)}[f(a_{i+1})]) = t_{(x)}[f\, q_{i+2}(a_{i+1})]$ would imply $\bar{p}(y_1) =$ $= y_1$, $p = p_{i+2}$, $p_{i+2} f(y_3) = f\, p_{i+2}(y_3)$, $y_1 = f(y_2)$, a contradiction.

10.5. Lemma. *There exists no positive integer k with $G_T(t^{(k)}[a_i]) = S_{\{x_1,x_2,x_3\}}$.*

Proof. Suppose that k is such a positive integer. Evidently, $(t^{(m)}[a_i], \bar{r}_4(t^{(m)}[a_i])) \in$ $\in T$ for every $m \geqq k$. There exists an m with $m \geqq k$ and $f^m = 1$. Evidently $(a_i, t^{(m)}[f^m(a_i)]) \in A$ (this is true for all non-negative integers m, proof by induction on m), $(a_i, t^{(m)}[a_i]) \in A$; hence $(a_{i-1}, q_i(t^{(m)}[a_i])) \in A$, $(a_{i+2}, q_{i+2}(t^{(m)}[a_i])) \in A$, $(q_i(t^{(m)}[a_i]), q_{i+2}(t^{(m)}[a_i])) \in T$. Hence $a_0, \ldots, a_{i-1}, q_i(t^{(m)}[a_i]), q_{i+2}(t^{(m)}[a_i])$, $a_{i+2}, \ldots, a_n$ is a $T \cup A$-proof contradicting 9.3.

10.6. Lemma. *The identity* $\operatorname{var}(a_0) = \{x_1, x_2, x_3\}$ *does not hold.*

Proof. It follows from 10.5 and (6).

11. CONVERSE IMPLICATION: FOUR VARIABLES

In this section we shall suppose that the $T \cup A$-proof $a_0, \ldots, a_n$ from Section 9 is such that $\operatorname{var}(a_0) = \{x_1, x_2, x_3, x_4\}$.

11.1. Lemma. *If $i \in \{1, \ldots, n\}$ is odd then $G_T(a_i) \in \{R_1, R_2, R_3\}$. If $i \in$ $\in \{1, \ldots, n-2\}$ is odd then $G_T(a_i) \neq G_T(a_{i+2})$.*

Proof. It follows from 9.11, 9.12, 3.8 and from the condition (8).

11.2. Lemma. *We have* $a_0 \sim a_1 \sim \ldots \sim a_n$.

Proof. Suppose, on the contrary, that there exists an odd $i \in \{1, \ldots, n-2\}$ such that the terms a_i, a_{i+1} are not similar. Using the condition (7), we obtain from 11.1 that either $a_{i-1} < a_{i+1}$ or $a_{i+1} < a_{i-1}$; it is enough to consider the case $a_{i-1} < a_{i+1}$. By 8.1, there exist a permutation $p \in S_{\{x_1,x_2,x_3,x_4\}}$, a variable x and a term t with a single occurrence of x such that $a_{i+1} = t_{(x)}[\bar{p}(a_{i-1})]$; we have $t \neq x$. Similarly as in the proof of 8.6 we get var $(t) = \{x\}$. By (9) there is a positive integer k with $G_T(t^{(k)}[a_{i-1}]) = S_{\{x_1,x_2,x_3,x_4\}}$. There exist permutations $q, r \in S_{\{x_1,x_2,x_3,x_4\}}$ such that $(a_{i-1}, t^{(k)}[\bar{q}(a_{i-1})]) \in A$, $(t^{(k)}[\bar{q}(a_{i-1})], t^{(k)}[\bar{r}(a_{i-1})]) \in T$, $(t^{(k)}[\bar{r}(a_{i-1})], a_{i+2}) \in A$. Hence $a_0, \ldots, a_{i-1}, t^{(k)}[\bar{q}(a_{i-1})], t^{(k)}[\bar{r}(a_{i-1})], a_{i+2}, \ldots, a_n$ is a $T \cup A$-proof contradicting 9.3.

11.3. Lemma. *The identity* var $(a_0) = \{x_1, x_2, x_3, x_4\}$ *does not hold.*

Proof. Put $G = \{p \in S_{\{x_1,x_2,x_3,x_4\}};\ (a_0, \bar{p}(a_0)) \in A\}$ and $H = \{p \in S_{\{x_1,x_2,x_3,x_4\}};\ (a_0, \bar{p}(a_0)) \in B\}$. By 11.2 we have $a_n = \bar{q}(a_0)$ for some $q \in S_{\{x_1,x_2,x_3,x_4\}}$ and $q \in H \setminus G$. Hence G is a proper subgroup of H. Evidently $G \nsubseteq G_T(a_0)$; from this and from the fact that $G_T(a_0)$ is a modular and maximal element of the subgroup lattice of $S_{\{x_1,x_2,x_3,x_4\}}$ we get $G \vee (H \cap G_T(a_0)) = H$. Hence $q = f_1 f_2 \ldots f_k$ for an odd number $k \geqq 1$, $f_i \in G$ if i is odd and $f_i \in H \cap G_T(a_0)$ if i is even. Put $g_0 = 1$ and $g_i = g_{i-1} f_i$ for all $i \in 1, \ldots, k\}$. Thus $g_k = q$. If $i \in \{1, \ldots, k\}$ is odd then $(\bar{g}_{i-1}(a_0), \bar{g}_i(a_0)) \in A$; if $i \in \{1, \ldots, k\}$ is even then $(\bar{g}_{i-1}(a_0), \bar{g}_i(a_0)) \in B \cap T \subseteq A$ as well. Hence $(\bar{g}_0(a_0), \bar{g}_k(a_0)) \in A$, i.e. $(a_0, a_n) \in A$. We get a contradiction.

The contradiction induced by Lemmas 9.13, 10.6 and 11.3 proves the converse implication of Theorem 5.1. Theorem 5.1 is thus proved.

Bibliography

[1] *A. D. Bol'bot:* O mnogoobrazijach Ω-algebr. Algebra i logika *9/4* (1970), 406—414.

[2] *S. Burris:* On the structure of the lattice of equational classes $L(\tau)$. Algebra Universalis *1* (1971), 39—45.

[3] *G. Grätzer:* Universal algebra, second edition. (To appear.)

[4] *E. Jacobs* and *R. Schwabauer:* The lattice of equational classes of algebras with one unary operation. Amer. Math. Monthly *71* (1964), 151—155.

[5] *J. Ježek:* Primitive classes of algebras with unary and nullary operations. Colloq. Math. *20* (1969), 159—179.

[6] *J. Ježek:* Principal dual ideals in lattices of primitive classes. Comment. Math. Univ. Carolinae *9* (1968), 533—545.

[7] *J. Ježek:* On atoms in lattices of primitive classes. Comment. Math. Univ. Carolinae *11* (1970), 515—532.

[8] *J. Ježek:* The existence o upper semicomplements in lattices of primitive classes. Comment. Math. Univ. Carolinae *12* (1971), 519—532.

[9] *J. Ježek:* Upper semicomplements and a definable element in the lattice of groupoid varieties. Comment. Math. Univ. Carolinae *12* (1971), 565—586.

[10] *J. Ježek:* Intervals in the lattice of varieties. Algebra Universalis *6* (1976), 147—158.
[11] *J. Kalicki:* The number of equationally complete classes of equations. Indag. Math. *17* (1955), 660—662.
[12] *R. McKenzie:* Definability in lattices of equational theories. Annals of Math. Logic *3* (1971), 197—237.
[13] *G. McNulty:* The decision problem for equational bases of algebras. Annals of Math. Logic 10 (1976), 193—259.
[14] *G. McNulty:* Undecidable properties of finite sets of equations. J. Symbolic Logic (1977).
[15] *G. McNulty:* Structural diversity in the lattice of equational theories. (To appear.)
[16] *G. Pollák:* On the existence of covers in lattices of varieties. 235—247 in: Contributions to general algebra. Proc. of the Klagenfurt Conference, May 25—28, 1978. Verlag Johannes Heyn, Klagenfurt 1979.
[17] *A. Tarski:* Equational logic and equational theories of algebras. 275—288 in: H. A. Schmidt, K. Schütte and H. J. Thiele, eds., Contributions to Mathematical Logic, North-Holland, Amsterdam 1968.
[18] *W. Taylor:* Equational logic. Houston J. of Math. (To appear.)
[19] *A. N. Trachtman:* O pokryvajuščich elementach v strukture mnogoobrazij algebr. Matem. Zametki 15 (1974), 307—312.

Author address: 186 00 Praha 8 - Karlín, Sokolovská 83, ČSSR (Matematicko-fyzikální fakulta UK).