Can. J. Math., Vol. XLI, No. 6, 1989, pp. 961–1004

ON THE WORD PROBLEM FOR ORTHOCOMPLEMENTED MODULAR LATTICES

MICHAEL S. RODDY

(0.1) *Introduction.* In [**16**] Freese showed that the word problem for the free modular lattice on 5 generators is unsolvable. His proof makes essential use of McIntyre's construction of a finitely presented field with unsolvable word problem [**30**]. (We follow Cohn [**7**] in calling what is commonly called a division ring a field, and what is commonly called a field a commutative field.) In this paper we will use similar ideas to obtain unsolvability results for varieties of modular ortholattices. The material in this paper is fairly wide ranging, the following are recommended as reference texts. Burris and Sankappanavar, [**6**], for universal algebra, for a short discussion of word problems and for references. Crawley and Dilworth [**12**], Grätzer [**17**], for lattice theory, and the survey paper of Day [**13**], for our approach to coordinatization. The only reasonably comprehensive texts on *rings, as far as I know, are Berberian [**1**] and Herstein [**21**], but the material presented here is elementary and one could survive with a good undergraduate algebra text, e.g. [**8**]. For ortholattice theory the standard reference is Kalmbach [**26**]. Finally, the ring constructions used in this paper are drawn entirely from Cohn [**7**] and [**9**]. I have attempted to make the paper reasonably self contained and accessible. For this reason some proofs, definitions or observations have been included which to the specialist in the particular field might seem trivial or unnecessary.

(0.2) *Modular Ortholattices.* (cf. [**26**], [**40**]). An *orthocomplementation*, abbreviated OC, on a bounded lattice $(L; \vee, \wedge, 0, 1)$ is a function

$$\begin{aligned} ' : L &\longrightarrow L \\ x &\longrightarrow x' \end{aligned}$$

satisfying, for all $a, b \in L$

(i) (Complementation laws)

$$a \vee a' = 1$$
$$a \wedge a' = 0$$

(ii) (deMorgan's laws)

$$(a \vee b)' = a' \wedge b'$$
$$(a \wedge b)' = a' \vee b'$$

Received September 25, 1987 and in revised form October 18, 1988. This paper is dedicated to the memory of Evelyn Nelson.

(iii)

$$(a')' = a.$$

A perhaps more intuitive condition than de Morgan's laws, although not an equation, is

(iv) (antimonotonicity)

$$a \leqq b \Rightarrow b' \leqq a'$$

for all $a, b \in L$. It is easy to show that, with the other conditions, (ii) and (iv) are equivalent.

A bounded lattice together with an orthocomplementation is called an *orthocomplemented lattice* or *ortholattice*, abbreviated OL. If the lattice reduct of an OL, L, is modular then L is called a *modular* ortholattice, abbreviated MOL. More formally, an *ortholattice* is an algebra

$$(L; \vee, \wedge, ', 0, 1)$$

where $(L; \vee, \wedge, 0, 1)$ is a bounded lattice with OC, $' : L \longrightarrow L$. L is a *modular ortholattice* in case $(L; \vee, \wedge)$ is modular.

Example 1. Boolean algebras are the best known variety of orthocomplemented lattices. They are the distributive ortholattices.

Example 2. The prototypical examples, for us, come from Hermitian forms on finite dimensional vector spaces. The simplest examples of these go as follows. Let F be a commutative field. A *Hermitian form* on F then is an n-tuple $(\alpha_1, \ldots, \alpha_n) \in F^n$ so that for all $(a_1, \ldots, a_n) \in F^n$

$$\sum_{i=1}^{n} a_i \alpha_i a_i = 0$$

implies for all i,

$$a_i = 0.$$

Let $L = L(F_F^n)$ be the lattice of all (right) vector subspaces of F^n. We will use the Hermitian form $(\alpha_1, \ldots, \alpha_n)$ to define an OC on L. Let V be a subspace of F and set

$$V' := \{(u_1, \ldots, u_n) \in F^n : \sum_{i=1}^{n} v_i \alpha_i u_i = 0, \quad \text{for all } (v_1, \ldots, v_n) \in V\}.$$

It is easy to show (cf. [**4**]) that $'$ is an OC on L. A familiar situation is when the Hermitian form consists entirely of 1's and the field is the real numbers.

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

In this case the OC is the orthogonal complement derived from the usual inner product. These examples are prototypical in the sense that the OC for every 'coordinatizable' MOL can be derived from a more general notion of a Hermitian form, as we will see.

(0.3) *Word Problems.* (cf. [**6**], [**14**]). Let $\mathcal{V}$ be a variety of algebras, G a finite set and *Rel* a finite set of equations of the type of $\mathcal{V}$ involving only elements of G. The pair (G, Rel) is called a *finite presentation.* Considering the elements of G as extra constants and the elements of *Rel* as extra identities we obtain the variety $\hat{\mathcal{V}}$. The free algebra on the empty set in $\hat{\mathcal{V}}$ is said to be *finitely presented* in $\mathcal{V}$ with *finite presentation* (G, Rel), this algebra will be written $\mathcal{V}(G, Rel)$. The *word problem for* $\mathcal{V}(G, Rel)$ asks for an algorithm which will determine whether or not a given equation will hold in this algebra. If such an algorithm exists then it is a *solution* to the word problem and the word problem for $\mathcal{V}(G, Rel)$ is said to be *solvable.* The *word problem for* $\mathcal{V}$ asks whether there is a solution to the word problem for each finite presentation on $\mathcal{V}$ (the distinction between this definition and the existence of a uniform solution for the variety should be noted, see [**35**]). Finally, if we ask only for a solution to the word problem when *Rel* is empty we are considering the *free word problem* because then $\mathcal{V}(G, Rel)$ is just a free algebra in $\mathcal{V}$, on G.

Example 1. Boolean algebras and distributive lattices have solvable word problem because every word can be reduced to one in 'normal form'. This reduction process is a solution to the word problem, cf. page 133 [**17**].

Example 2. Ortholattices and lattices have solvable free word problem. Both have an algorithm which compares words in free algebras, Whitman's algorithm [**44**] for free lattices, and a modification of it by Bruns [**5**] for ortholattices. They both also share Evans' embeddability property [**14**] via the MacNeille completion, so their general word problems are also solvable. An explicit solution for the ortholattice case is given in [**26**].

Example 3. Groups and semigroups both have solvable free word problem, normal forms for free algebras are easily visualized, but neither have a solvable word problem in general. The existence of a finitely presented semigroup with unsolvable word problem was established by Post [**39**], this marked the starting point of such investigations. This was used by Novikov [**38**] to find a finitely presented group with unsolvable word problem, a major technical achievement. An excellent presentation of this material is given in [**41**].

Example 4. For modular lattices the existence of a finitely presented modular lattice with unsolvable word problem was established by Hutchinson [**25**], and Lipshitz [**29**]. As mentioned, a negative solution for the free case was given by Freese [**16**], for 5 generators. His method was ingeneously adapted by Herrmann [**20**] to the case of 4 generators.

The number of generators allowed is critical in determining solvability. The

critical jump for modular lattices is from three to four. For us it is from two to three.

THEOREM (0.3.1) ([**27**]). *The free* MOL *on two generators is finite.*

It follows that the word problem is solvable for any two generated MOL. For this reason we will concern ourselves primarily with the case of three generators.

(0.4) *Motivation.* The negative solutions listed above all have in common the fact that they are based on Post's original construction and will be, at least indirectly, used in this paper. There are many other examples of unsolvability, some based on Post's construction, some not. One remarkable thing about Post's original result and about many of its derivatives is that these algebras have all arisen naturally from sources where it is not obvious à priori that unsolvability will occur. Unsolvability is therefore not always expected, and its occurrence anywhere is of some interest. The ability to adapt the original semigroup presentation to these other varieties of algebras also shows how, in some sense, these disparate equational theories are woven together. For MOL's there are other and perhaps less esoteric reasons for interest.

Quantum mechanical systems have associated with them an algebra of propositions, cf. [**22**], [**36**] or [**26**]. The interpretation of the operations of such an algebra is exactly the same as the classical Boolean case for 'compatible' or 'commuting' propositions, (see the references listed above). For 'noncompatible' or 'noncommuting' propositions it is not exactly clear how to interpret the operations $\wedge$ and $\vee$. In fact, it is not even agreed that such operations should exist on a purely syntactic level, cf. [**36**] for example. However in the classical models, the projection (ortho)lattices of Hilbert spaces, these operations are defined. This was first emphasized by Birkhoff and vonNeumann in their 1936 paper 'On the logic of quantum mechanics', [**4**]. This paper has led to a well developed theory of, particularly, the orthomodular lattices. (Still the best account of the passage from the Hilbert space to the ortholattice setting is given in [**22**].) It is this interpretation of ortholattices as propositional logics that makes the solution of the word problem an important goal for varieties of ortholattices.

In fact, the algebras Birkhoff and vonNeumann proposed for study were modular ortholattices, or more accurately the *n-distributive* MOLs; the ones arising from projective geometries. It is thus tempting to overstate the importance of the results in this paper. But modularity only holds when the Hilbert space is finite dimensional and even Birkhoff later admitted the need for infinitely many dimensions, [**3**]. Even so, the finite dimensional case is not completely without interest. I also believe there may be applications of the techniques developed here to wider classes of algebras which do include the infinite dimensional Hilbert space examples.

1. Coordinatization of modular ortholattices.

(1.1) *Multiplicative Structures with Involution.* Let $(S, \cdot)$ be a semigroup. An

involution on $(S, \cdot)$ is a map

$$^* : S \longrightarrow S$$

satisfying for all $a, b \in S$,

$$(a \cdot b)^* = b^* \cdot a^*,$$

and

$$(a^*)^* = a.$$

We may consider the involution as an extra operation. A **semigroup*, or *semigroup with involution*, is an algebra $(S; \cdot, ^*)$, where * is an involution on the semigroup $(S; \cdot)$. Other structures with a semigroup reduct may admit an involution, however it is usual to insist that the involution be compatible with the other operations.

Example 1. Let $(G; \cdot, ^{-1}, e)$ be a group, and let * be an involution on the semigroup $(G; \cdot)$. * is automatically compatible with the other operations as the following two computations show. The identity element of a group is unique as even a one sided identity, and for any $g \in G$ we have

$$g \cdot e^* = ((e^*)^* \cdot g^*) = (e \cdot g^*)^* = (g^*)^* = g.$$

Therefore, $e^* = e$. For any $g \in G$, g^{-1} is unique as a left inverse of g, and

$$g^* \cdot (g^{-1})^* = (g^{-1} \cdot g)^* = e^* = e.$$

Therefore $(g^*)^{-1} = (g^{-1})^*$. Thus a **group* or *group with involution* is an algebra $(G; \cdot, ^*, ^{-1}, e)$ where * is an involution on the group $(G; \cdot, ^{-1}, e)$.

For any group taking inverses produces an involution but for our purposes it is not one of much interest.

Example 2. Let $(R; +, \cdot, -, 0, 1)$ be a ring with unit. An *involution* on $(R; +, \cdot, -, 0, 1)$ is an involution * on the semigroup $(R; \cdot)$ which is compatible with addition, ie., for all $s, t \in R$,

$$(a + b)^* = a^* + b^*.$$

Compatibility with the constants is easy to establish. Hence a **ring*, or, *ring with involution*, is an algebra $(R; +, \cdot, -, ^*, 0, 1)$, where * is an involution on the ring $(R; +, \cdot, -, 0, 1)$. A **field* is a *ring which is also a field.

In connection with this last example we consider a semigroup S with 0. An involution * on S is *nondegenerate* is case for all s

$$s^* \cdot s = 0 \text{ implies } s = 0.$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

The involution is *degenerate* in case it is not nondegenerate. An involution on a ring is *degenerate* or *nondegenerate* according to whether it is as an involution on the multiplicative semigroup of the ring. We will not be interested in degenerate involutions so let us adopt the convention of assuming that the involution on a *ring is nondegenerate unless it is specified that it may be degenerate. We will soon see the intimate connection between nondegenerate involutions on certain rings and OC's on MOLs.

Finally, observe that it is relatively easy to build a categorical framework which handles both involutions on multiplicative structures and polarities on ordered structures, of which OC's are the 'nondegenerate' case. This viewpoint was taken in an earlier draft of this paper, but was cumbersome since our intents here are technical and fairly specific. The basic necessity for such a treatment is the concept of an opposite, or dual, structure; in this case the 'opposite' of a semigroup and the 'dual' ordering of a partially ordered set. See [**11**] for a categorical treatment of structures with involution.

(1.2) *Canonical Frames.* The next few sections are devoted to recalling enough coordinatization theory to understand and exploit the links between certain MOLs and regular rings with involution. We start with some notation and definitions which apply to all rings.

Let R be a ring and let $n \in \mathbf{N}$. For any right R-module M we define the following two ordered structures.

(i) $L(M_R)$ is the (modular) lattice of all right R-submodules of M.

(ii) $\hat{L}(M_R)$ is the subpartially ordered set of $L(M_R)$ consisting of all finitely generated right R-submodules of M.

In general $\hat{L}(M_R)$ is not a sublattice of $L(M_R)$, not even when M_R is itself finitely generated which is the case we will be interested in. In fact we will usually only be interested in right R-modules of the form R_R^n, $n \in \mathbf{N}$. Let us establish some notation for this situation. Fix R and n. As usual, for $x \in R^n$ the right R-submodule of R^n generated by x is xR. For $i \leqq n$ let e_i be the vector consisting of a 1 in the i'th place and 0's elsewhere. Let e_{n+1} be the vector with a 1 in every place. The $(n+1)$-tuple $(e_1R, \ldots, e_{n+1}R)$ is called the *canonical n-frame* of $L(R_R^n)$, or, of $\hat{L}(R_R^n)$, depending on context.

(1.3) *An Isomorphism.* For a ring R and $n \in \mathbf{N}$ let R_n be the ring of $n \times n$ matrices over R. There is a fundamental, obvious, isomorphism between $L(R_R^n)$ and $L(R_{nR_n})$. Define

$$\Psi : L(R_R^n) \longrightarrow L(R_{nR_n})$$

by

$$M \longrightarrow \{(a_{ij} \mid (a_{1j}, \ldots, a_{nj}) \in M, j = 1, \ldots, n\}$$

and

$$\Phi : L(R_{nR_n}) \longrightarrow L(R_R^n)$$

by

$$A \longrightarrow \{(a_1, \ldots, a_n) \in R^n \mid (a_1, \ldots, a_n) \text{ is the column of a matrix in } A\}.$$

THEOREM (1.3.1). (Proposition 14, [**42**]). *Φ and Ψ are inverse lattice isomorphisms. Furthermore, finitely generated right submodules and finitely generated right ideals correspond to one another under each of these maps.*

(1.4) *Frames*, (cf. [**13**]). We have already introduced the canonical n-frame in the lattice of right R-submodules of R^n. If L is a bounded modular lattice then a *spanning n-frame* in L is an $(n+1)$-tuple $(x_1, \ldots, x_{n+1})$ of elements of L satisfying, for all $i, j, k \in \{1, \ldots, n\}$,

$$\text{(i)} \quad \bigvee_{i \neq j} x_i = \bigvee x_i,$$

$$\text{(ii)} \quad x_i \wedge \bigvee_{i \neq j \neq k \neq i} x_k = 0.$$

and

$$\text{(iii)} \quad \bigvee x_i = 1.$$

If $(x_1, \ldots, x_{n+1})$ satisfies (i) and (ii) but not necessarily (iii) then it is called an *n-frame*. If L is in addition an MOL then a (spanning) n-frame in L is *orthogonal* in case for all $i \neq j$ with $1 \leqq i, j \leqq n$, $x_i \leqq x_j'$.

(1.5) *Regular Rings*. In this section we recall some basic facts about regular rings. Our main concern will be to provide enough information to prove the main theorem. A slightly more comprehensive version of this section, which is consistent with the notation used here, is given in [**40**] and that in turn is taken mainly from the original [**43**], see also [**42**]. Let R be a ring. An element $e \in R$ is an *idempotent* in case $e = e^2$. We recall some facts about idempotents.

OBSERVATION (1.5.1) ([**43**]). (1) *e is an idempotent if and only if $1 - e$ is an idempotent.*

(2) *$eR = \{a \in R \mid ea = a\}$, where e is an idempotent.*

(3) *eR and $(1 - e)R$ are complements in $L(R_R)$, where e is an idempotent.*

(4) *Conversely, if two right ideals I and J are complements in $L(R_R)$ then there exists an idempotent $e \in R$ with $I = eR$ and $J = (1 - e)R$.*

THEOREM (1.5.2) ([**43**]). *For a ring R the following conditions are equivalent.*

(i) *Every principal right ideal has a complement in $L(R_R)$.*

(ii) *For every $a \in R$ there exists an idempotent $e \in R$ with $eR = aR$.*

(iii) *For every $e \in R$ there exists $r \in R$ with $ara = a$.*

A ring R is *regular* in case it possesses one, hence all, of the above properties. Usually (iii) is used as the definition of a regular ring because of its obvious left-right symmetry.

THEOREM (1.5.3) ([**43**]). *For a regular ring R, $\hat{L}(R_R)$ is a complemented modular lattice; it is a sublattice of $L(R_R)$.*

THEOREM (1.5.4) ([**43**]). *Let R be a ring and let $n \in \mathbf{N}$. R is regular if and only if R_n is regular.*

(1.6) OC's *and Involutions*. A **regular ring* is a *ring which is also regular. A *projection* of a *regular ring R is an idempotent $e \in R$ with $e = e*$. The set of all projections of R is written $Pr(R)$. As its idempotents describe the structure of the lattice of finitely generated right ideals of a regular ring, so the projections describe the structure of the ortholattice induced by the involution when R is a *regular ring. A regular ring is of *order n* in case $\hat{L}(R_R)$ contains an n-frame.

THEOREM (1.6.1) ([**43**]). (*a*) *If R is *regular then the map*

$$aR \longrightarrow \{r \in R \mid a^*r = 0\}$$

defines an OC, $'$, *on $\hat{L}(R_R)$. The involution * is said to generate the* OC $'$. *Conversely, if R is of order $n, n \geqq 3$, then each* OC *on $\hat{L}(R_R)$ is generated by a unique involution on R.*

(*b*) *If $e \in Pr(R)$ then $(eR)' = (1 - e)R$.*

(1.7) *Coordinatization of Modular Lattices*. We recall the basic coordinatization theorem for complemented modular lattices. Let L and M be modular lattices containing, not necessarily spanning, n-frames, $(x_1, \ldots, x_{n+1})$ and $(y_1, \ldots, y_{n+1})$ respectively. A *frame preserving homomorphism* is a lattice homomorphism from L to M which maps x_i to y_i, for each $i, 1 \leqq i \leqq n + 1$. Of course, a frame preserving homomorphism is frame preserving with respect to two specific frames, context will usually specify these.

COORDINATIZATION THEOREM (1.7.1) ([**43**], see also Theorem 5, [**13**]). *Let L be a complemented modular lattice containing a spanning n-frame, $n \geqq 4$, $(x_1, \ldots, x_{n+1})$. Then there exists a regular ring R and a frame preserving isomorphism sending $(x_1, \ldots, x_{x+1})$ to the canonical frame of $\hat{L}(R_R^n)$.*

The theorem is proved by coding the operations of the ring as lattice polynomials. Our final objective is to use these operations to obtain unsolvability in an MOL, so it is worth our while spending some time here understanding the operations. There are several slightly different but equivalent ways of doing this. We are following the approach of Day [**13**], as opposed to, for example, that of [**16**], or [**19**].

(1.8) *The Arithmetic of Frames*, (cf. [**13**]). Let $(x_1, \ldots, x_{n+1})$ be an n-frame, $n \leqq 3$, in a bounded modular lattice L. Then standard modular arguments show

that (x_1, x_2, x_3, t) is a 3-frame in L, where

$$t := \left(\bigvee_{4 \leqq i \leqq n+1} x_i \right) \wedge (x_1 \vee x_2 \vee x_3).$$

Let $w := (x_1 \vee t) \wedge (x_2 \vee x_3)$. The *diagonal* is

$$D := \{d \in L : w \wedge d = w \wedge x_1 \text{ and } w \vee d = w \vee x_1\}.$$

Define,

$$\oplus : D \times D \longrightarrow D$$

by

$$a \oplus b := (x_1 \vee t) \wedge (x_2 \vee ((x_3 \vee a) \wedge (((x_3 \vee x_1) \wedge (x_2 \vee b)) \vee w))),$$

$$\ominus : D \longrightarrow D$$

by

$$\ominus a := (t \vee x_1) \wedge [x_3 \vee ((x_1 \vee x_2) \wedge (w \vee [(x_1 \vee x_3) \wedge (x_2 \vee a)])],$$

and

$$\otimes : D \times D \longrightarrow D$$

by

$$a \otimes b := (x_1 \vee t) \wedge (x_2 \vee ((x_3 \vee b) \wedge (x_1 \vee ((x_3 \vee t) \wedge (x_2 \vee a))).$$

It is instructive to do the calculations which show that these operations in fact do what they should in a submodule lattice. That is, if $L = \hat{L}(R_R^3)$ then

$$D = \{(1, r, r)R : r \in R\},$$

and if $r, s \in R$ then

$$(1, r, r)R \oplus (1, s, s)R = (1, r + s, r + s)R,$$
$$(1, r, r)R \otimes (1, s, s)R = (1, rs, rs)R,$$

and

$$\ominus(1, r, r)R = (1, -r, -r)R.$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

THEOREM 1.8.1 ([**43**], see also Theorem 3, [**13**]). *If L is a complemented modular lattice with n-frame $(x_1, \ldots, x_{n+1})$, $n \geqq 4$, then $(D; \oplus, \otimes, \ominus, x_1, t)$ is a regular ring with unit t and zero x_1.*

As a result the full coordinatization theorem can be restated as follows. Let R be the ring $(D; \oplus, \otimes, \ominus, x_1, t)$ and suppose $(x_1, \ldots, x_{n+1})$ spans L. Then there exists a unique frame preserving isomorphism, f, from L to $\hat{L}(R_R^n)$, with the canonical frame, so that $f(a) = (1, a, a, 0, \ldots, 0)R$ for all $a \in D$. Calculations using (1.8.1) also provide us with the following observation:

PROPOSITION (1.8.1). *Let R be a regular ring and define $(D; \oplus, \otimes, \ominus, x_1, t)$ in terms of the canonical frame of $\hat{L}(R_R^n)$. Then the map*

$$\hat{f} : R \longrightarrow D$$

given by

$$\hat{f}(r) = (1, r, r, 0, \ldots, 0)R$$

is a ring isomorphism.

(1.9) *Hermitian Forms on *Regular Rings.* The isomorphism of (1.3.1) can be used to translate from involutions on R_n to Hermitian forms on R. This was first done for the special case of fields in [**4**] and later extended by F. Maeda [**31**].

THEOREM (1.9.1) ([**31**]). *If $'$ is an* OC *on $\hat{L}(R_R^n)$ and if the canonical frame is orthogonal then there exist invertible $\alpha_2, \ldots, \alpha_n \in R$ and an involution $*$ on R so that for each i,*

$$\alpha_i = \alpha_i^*$$

and for $M \in \hat{L}(R_R^n)$,

$$M' = \{(a_1, \ldots, a_n) \mid a_1^* m_1 + a_2^* \alpha_2 m_2 + \cdots + a_n^* \alpha_n m_n = 0, \text{ for all } (m_1, \ldots, m_n) \in M\}.$$

The $(n+1)$-tuple $(1, \alpha_2, \ldots, \alpha_n; *)$ is called a *Hermitian form* associated with the OC, $'$, (we follow [**31**] in this choice of terminology).

In general, a *Hermitian form* on a regular ring R is an $(n+1)$-tuple $(\alpha_1, \ldots, \alpha_n; *)$ where $*$ is an involution on R each α_i is invertible, *self-adjoint*, i.e., $\alpha_i = \alpha_i^*$, and the form is *nondegenerate*, i.e., for $a_1, \ldots, a_n \in R$,

$$a_1^* \alpha_1 a_1 + \cdots + a_n^* \alpha_n a_n^* = 0$$

implies

$$a_i = 0, \quad \text{for each } i.$$

THEOREM (1.9.2) ([**31**]). *If* $(\alpha_1, \ldots, \alpha_n;^*)$ *is a Hermitian form on the regular ring* R *then the map on* $\hat{L}(R_R^n)$ *defined by*

$$M \to M' :=$$
$$\{(a_1, \ldots, a_n) \mid a_1^* \alpha_1 m_1 + a_2^* \alpha_3 m_2 + \cdots + a_n^* \alpha_n m_n = 0,$$
$$\text{for all } (m_1, \ldots, m_n) \in M\}$$

is an OC *on* $\hat{L}(R_R^n)$.

We will always work with Hermitian forms whose first element is 1, (1.9.1) shows us that this is no restriction. By (1.6.1) the involution on R_n is unique, for $n \geqq 3$. But the uniqueness of the Hermitian form associated with the OC on $\hat{L}(R_R^n)$ via the isomorphism of (1.3.1) has to be qualified. It depends on the choice of orthogonal frame and on the fact that $\alpha_1 = 1$. However, elementary calculations show that with these provisions the Hermitian form is also unique.

There is another observation that belongs here. Suppose $\beta_1, \ldots, \beta_n$ are invertible elements of the *regular ring R and that $(\alpha_1, \ldots, \alpha_n;^*)$ is a Hermitian form on R. If, for $a_1, \ldots, a_n \in R$,

$$a_1^* \beta_1^* \alpha_1 \beta_1 a_1 + \cdots + a_n^* \beta_n^* \alpha_n \beta_n a_n = 0,$$

then $\beta_i a_i = 0$ for each i. But since each β_i is invertible this means that $a_i = 0$, for each i. We have proved,

PROPOSITION (1.9.3). *If* $(\alpha_1, \ldots, \alpha_n;^*)$ *is a Hermitian form on* R *then so too is* $(\beta_1^* \alpha_1 \beta_1, \ldots, \beta_n^* \alpha_n \beta_n;^*)$.

(1.10) *More arithmetic.* Let $\hat{L}(R_R^n)$ be an MOL with orthogonal canonical frame and an associated Hermitian form $(1, \alpha_2, \ldots, \alpha_n;^*)$. Our objective is to show that for each $k, 2 \leqq k \leqq n$, $(1, \alpha_k, \alpha_k, 0, \ldots, 0)R$ and $(1, \alpha_k^{-1}, \alpha_k^{-1}, 0, \ldots, 0)R$ can be expressed as ortholattice polynomials on elements on the canonical frame. A consequence of this will be that any ring relation between the elements of the Hermitian form can be expressed as an ortholattice relation between the elements of the canonical frame using the operations of (1.8.1). We will show this via a sequence of lemmas whose proofs consist of calculations in the submodule lattice. These calculations will not be done and the lemmas will be formulated only for $k = 3$ and $k = 4$. The argument for $k = 2$ follows the argument for $k = 3$ and the arguments for all other values of k follow the argument for $k = 4$. This is done to avoid the notational inconvenience of a general argument, a typical calculation is given for (1.10.8). Here the canonical frame is $(x_1, \ldots, x_{n+1})$ and t is as defined in section (1.8). Let D_α be the subring of D, from (1.8), contained in the subortholattice of $\hat{L}(R_R^n)$ generated, as an ortholattice, by the elements of the canonical frame.

LEMMA (1.10.1).

$$(1, 0, -\alpha_3^{-1}, 0, \ldots, 0)R = (x_1 \vee x_3) \wedge t'.$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

LEMMA (1.10.2). *For any* $a \in R$,

$$(1, a, a, 0, \ldots, 0)R = (t \vee x_1) \wedge ((1, 0, a, 0, \ldots, 0)R \vee x_2),$$

and

$$(1, 0, a, 0, \ldots, 0)R = (x_1 \vee x_3) \wedge ((1, a, a, 0, \ldots, 0)R \vee x_2).$$

COROLLARY (1.10.3).

$$(1, \alpha_3^{-1}, \alpha_3^{-1}, 0, \ldots, 0)R \in D_\alpha$$

and

$$(1, -\alpha_3^{-2}, -\alpha_3^{-2}, 0, \ldots, 0)R \in D_\alpha.$$

LEMMA (1.10.4).

$$(1, 0, \alpha_3, 0, \ldots, 0)R = (x_1 \vee x_3) \wedge ((1, -\alpha_3^{-2}, -\alpha_3^{-2}, 0, \ldots, 0)R)'.$$

COROLLARY (1.10.5).

$$(1, \alpha_3, \alpha_3, 0, \ldots, 0)R \in D_\alpha.$$

The calculations for $k = 4$ are similar, except we need a slightly more complex translation process.

LEMMA (1.10.6). *For* $a \in R$,

$$(1, a, a, 0, \ldots, 0)R = (t \vee x_1) \wedge ((1, 0, 0, -a, 0, \ldots, 0)R \vee (0, 1, 1, 1, 0, \ldots, 0)R)$$

and

$$(0, 1, 1, 1, 0, \ldots, 0)R = (x_2 \vee x_3 \vee x_4) \wedge \left(\bigvee_{i \neq 2,3,4} x_i \right).$$

Also,

$$(1, 0, 0, a, 0, \ldots, 0)R = (x_1 \vee x_4) \wedge ((1, -a, -a, 0, \ldots, 0)R \vee (0, 1, 1, 1, 0, \ldots, 0)R).$$

LEMMA (1.10.7).

$$(1, 0, 0, -\alpha_4^{-1}, 0, \ldots, 0)R = (x_1 \vee x_4) \wedge x'_{n+1}$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

and

$$(1,0,0,\alpha_4,0,\ldots,0)R = (x_1 \vee x_4) \wedge ((1,0,0,-\alpha_4^{-2},0,\ldots,0)R)'.$$

COROLLARY (1.10.8).

$$(1,\alpha_4^{-1},\alpha_4^{-1},0,\ldots,0)R \in D_\alpha$$

and

$$(1,\alpha_4,\alpha_4,0,\ldots,0)R \in D_\alpha.$$

Proof. We will outline a proof of the second part of the claim, since it is probably the most involved of the calculations in this section. From the first part we have

$$(1,\alpha_4^{-1},\alpha_4^{-1},0,\ldots,0)R \in D.$$

Squaring this, using $\otimes$, we obtain

$$(1,\alpha_4^{-2},\alpha_4^{-2},0,\ldots,0)R \in D.$$

From (1.10.6) we obtain, $(1,0,0,-\alpha_4^{-2},0,\ldots,0)R$. Now,

$$(1,0,0,\alpha_4,0,\ldots,0)R = (x_1 \vee x_4) \wedge ((1,0,0,-\alpha_4,0,\ldots,0)R)',$$

applying (1.10.6) again, and using $\ominus$ we obtain $(1,\alpha_4,\alpha_4,0,\ldots,0)R$.

This sequence of lemmas (for general k) proves,

PROPOSITION (1.10.9). *Let R_α be the subring of R generated by the elements of the Hermitian form and their inverses and let D_α be the subring of D defined above. Then,*

$$\hat{f}(R_\alpha) \subseteq D_\alpha,$$

where $\hat{f}$ is the ring isomorphism provided by (1.8.2).

It is actually quite easy to see that $\hat{f}(R_\alpha) = D_\alpha$ but we will not prove it here.

(1.11) *The free* MOL *on an Orthongonal n-Frame with Relations.* A spanning orthogonal n-frame is an example of a finite presentation in the variety of MOL's. The finitely presented MOL whose presentation is the spanning orthogonal n-frame is called the *free* MOL *on a spanning orthogonal n-frame*, written $Frm(n)$. If $n \geqq 4$ then, by (1.7.1), $Frm(n)$ can be coordinatized.

Let Φ be a finite set of ring relations on the letters $\alpha_2,\ldots,\alpha_n,\alpha_2^{-1},\ldots,\alpha_n^{-1}$. Let R be a regular ring with Hermitian form $(1,\alpha_2,\ldots,\alpha_n;^*)$. Then by (1.10.9),

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

there exists a finite set of ortholattice relations, Φ_0, involving only elements of the orthogonal frame of $\hat{L}(R_R^n)$ (with OC induced by the Hermitian form $(\alpha_2, \ldots, \alpha_n;^*)$), which correspond via the isomorphism $\hat{f}$ with the relations Φ, i.e., the relations Φ hold in R if and only if the relations Φ_0 hold in the MOL $\hat{L}(R_R^n)$.

Let $Frm(n, \Phi)$ be the free MOL on the orthogonal n-frame, $n \geqq 4$, satisfying the relations Φ_0, i.e., the finitely presented MOL on the presentation obtained by adjoining the relations Φ_0 to the presentation for an orthogonal n-frame, let R_Φ be the coordinatizing ring of $Frm(n, \Phi)$ and let $(1, \Omega_1, \ldots, \Omega_n;^*)$ be the associated Hermitian form. Then we have:

LEMMA (1.11.1). *Let R be a *regular ring with Hermitian form $(1, \ldots, \alpha_n;^*)$, let Φ be a set of *ring relations involving only form elements which hold in R. Then there exist unique homomorphisms*

$$f : Frm(n, \Phi) \longrightarrow \hat{L}(R_R^n),$$
$$\hat{f} : R_\Phi \longrightarrow R,$$

so that for all $r \in R_\Phi$,

$$f((1, r, r, 0, \ldots, 0)R_\Phi) = (1, \hat{f}(r), \hat{f}(r), 0, \ldots, 0)R,$$

and

$$\hat{f}(\Omega_i) = \alpha_i, \quad 2 \leqq i \leqq n.$$

Proof. The existence of the frame preserving ortholattice homomorphism, f, follows from the universality properties of $Frm(n, \Phi)$. Its 'extension' to the ring homomorphism $\hat{f}$ is accomplished via (1.8.1) and (1.8.2). The final part of the claim follows from the uniqueness of the Hermitian form, cf. the comments below (1.9.2).

It was shown in [**34**], see also [**20**], that any MOL generated by an orthogonal n-frame is generated by 3 elements. To obtain a finitely presented 3-generated MOL with unsolvable word problem we will encode unsolvability in the multiplicative group of a *field in terms of the elements of a Hermitian form and pull this unsolvability back into the free MOL on a spanning orthogonal n-frame with a certain set of relations. The construction of the *field and the mechanics of the proof will occupy the rest of this paper.

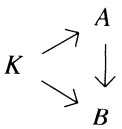
2. *Ring constructions.

(2.1) *Amalgamated Coproducts*, (cf. page 92, [**7**]). Let $\mathcal{C}$ be a category and let K be an object of $\mathcal{C}$. The *comma category* $(K, \mathcal{C})$ has, as objects, $\mathcal{C}$-morphisms of the form

$$K \longrightarrow A$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

and as morphisms, commutative triangles of the form



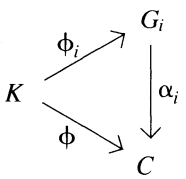
Coproducts in this category are called $\mathcal{C}$-*coproducts amalgamating*, or, *over* K. More explicitly, if

$$\phi_i : K \longrightarrow G_i, \quad i \in I$$

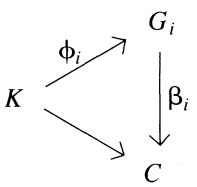
is a family of $\mathcal{C}$-morphisms then its *coproduct over* K is an object of $(K, \mathcal{C})$,

$$\phi : K \longrightarrow G$$

along with a family of morphisms of $(K, \mathcal{C})$



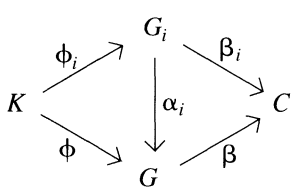
so that for any family of morphisms of $(k, \mathcal{C})$,



there exists a unique $\mathcal{C}$-morphism

$$\beta : G \longrightarrow C$$

so that for all $i \in I$,



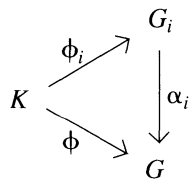
commutes.

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

(2.2) *Coproducts of Multiplicative Structures with Involution.* Our construction will require taking amalgamated coproducts of *structures (where 'structure' means ring, semigroup or group) over a sub-*structure in the category under consideration. We start this section with a simple lemma which often allows us to do this by just taking the coproduct in the underlying category without the involution, and then defining an involution on it. Again, we formulate the lemma only generally enough to cover present needs.

Let $\mathcal{V}$ be one of the varieties of algebras with semigroup reduct given in (1.1), and let ${}^*\mathcal{V}$ be the corresponding variety of structures with involution. For A an object in $\mathcal{V}$ let A^{opp} be the *opposite* of A, i.e., A^{opp} has the same underlying set and operations except the multiplication is reversed.

LEMMA (2.2.1). *Let $\phi_i : K \to G_i$, $i \in I$, be a set of homorphisms in ${}^*\mathcal{V}$ and suppose that the amalgamated coproduct of the G_i over K,*

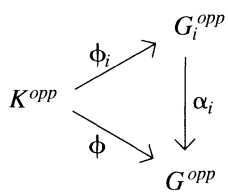


exists in $\mathcal{V}$. Then it is contained in (the reduct of) ${}^*\mathcal{V}$; in fact, it is the coproduct of the G_i over K in ${}^*\mathcal{V}$.

Proof. There are two parts to the proof. We will show first that the $\mathcal{V}$ coproduct, if it exists, is in (the reduct of) ${}^*\mathcal{V}$. Then we will show that it is also the coproduct in ${}^*\mathcal{V}$. We begin with a simple observation. If $\beta : A \to B$ is in $\mathcal{V}$ then $\beta : A^{opp} \to B^{opp}$, the same underlying set map, is also in $\mathcal{V}$. To see this let us use juxtaposition for the multiplication in A and B, and $\odot$ for the opposite multiplication. Then for $x, y \in A$, we have

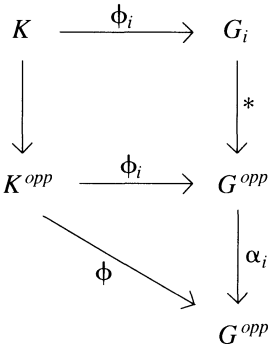
$$\beta(x \odot y) = \beta(yx) = \beta(y)\beta(x) = \beta(x) \odot \beta(y).$$

It follows that

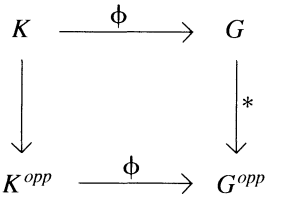


is a coproduct as well.

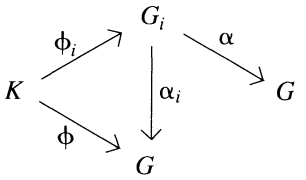
For each $i \in I$, we have



commutative. This induces a morphism $^* : G \longrightarrow G^{opp}$, with

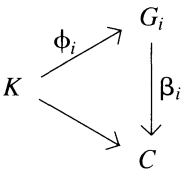


commutative. Trivially, $id_G : G \longrightarrow G$ is the unique morphism completing,

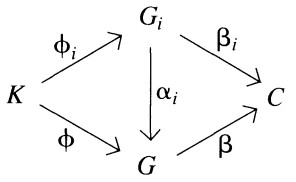


to a commutative diagram. But $^*\circ^* : G \longrightarrow G$ also completes this diagram, hence $^*\circ^* = id_G$. It follows that * is an involution, and the first part of the proof is complete.

Let



$i \in I$, be a set of morphisms in $(K, {}^*\mathcal{V})$. Then there exists a unique morphism β in $(K, \mathcal{V})$ so that



https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

commutes for all $i \in I$. We need to show that β is in ${}^*\mathcal{V}$. Now, for $a \in G_i$, we have

$$\beta_i(a^*) = \beta(\alpha_i(a^*)) = \beta(\alpha_i(a)^*)$$

and this implies

$$\beta(\alpha_i(a)) = \beta_i(a) = (\beta_i(a^*))^* = (\beta(\alpha_i(a)^*))^*.$$

This computation and the uniqueness of β mean that β equals the composition, ${}^* \circ \beta \circ {}^*$, which in turn implies $\beta(g)^* = \beta(g^*)$, for all $g \in G$. In other words β is in ${}^*\mathcal{V}$ and the second part of the proof is complete.

We will use the symbol $\coprod_C$ to denote an amalgamated coproduct over the object C. Context will make it clear which variety of algebras we are dealing with if this isn't explicitly stated. The last result allows us to obtain new *structures from old ones by taking coproducts, but there is also a standard coproduct construction allowing one to obtain *structures from structures which may not have an involution. For $A \in \mathcal{V}$ we define the *center* of A as

$$C(A) := \{c \in A : ca = ac, \text{ for all } a \in A\}.$$

We can form the coproduct of A with A^{opp} amalgamating any substructure, C, of $C(A)$, to obtain the structure $A \coprod_C A^{opp}$.

LEMMA (2.2.2). *The identity map from A to A^{opp} extends to an involution on $A \coprod_C A^{opp}$.*

Proof. By considering the coproduct as the union of the presentations of the factors (cf. page 94 [7], for example) it is clear that, in general, the opposite of the coproduct $A \coprod_C B$ is $A^{opp} \coprod_{C^{opp}} B^{opp}$. Applying this observation to the present situation we observe that the maps id_a and $id_{A^{opp}}$ extend to a homomorphism

$$* : A \coprod_{C(A)} A^{opp} \longrightarrow \left(A \coprod_{C(A)} A^{opp} \right)^{opp}$$

and easy uniqueness arguments show that

$$* \circ * = id_{A \coprod_{C(A)} A^{opp}}.$$

Note, however, that there is no claim here that the coproduct is well behaved (cf. (2.4)), or even nontrivial.

There are two applications of this lemma which we will include here, even though they will not be used until Section 3. For a set G let $FD(G)$ be the free group on G and let $F^*G(G)$ be the free *group on G. Consider the group homomorphism

$$FG(G) \longrightarrow FG(G)^{opp}$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

induced by mapping the generators identically. By (2.2.2) this map induces an involution on the coproduct $FG(G) \coprod FG(G)^{opp}$ (here C is just the trivial subgroup consisting of the unit). To emphasize the involution let us relabel the elements of the generating set of $FG(G)^{opp}$ and the set itself by superscripting * to them. The isomorphism which acts identically on the generators becomes,

$$(1) \qquad * : FG(G) \longrightarrow FG(G^*), \quad x \longrightarrow x^*$$

and its inverse,

$$* : FG(G^*) \longrightarrow FG(G), \quad x \longrightarrow x^*.$$

LEMMA (2.2.3). *As a *group* $FG(G) \coprod FG(G^*)$ *is free on* G.

Proof. There is a unique group homomorphism

$$h : FG(G) \coprod FG(G^*) \longrightarrow F^*G(G)$$

mapping G identically and mapping G^* to the image of G under the involution of $F^*G(G)$ in the manner corresponding to (1) above. We will use the same trick again to show that h is a *group homomorphism. Replace h with the group homomorphism

$$k = * \circ h \circ *$$

obtained by composing h on either side with the appropriate involution. Then for $x \in G$ we have

$$k(x) = (h(x^*))^* = (x^*)^* = x$$

and for $x^* \in G^*$ we have

$$k(x^*) = (h(x^{**})^* = (h(x))^* = x^*.$$

The uniqueness of h implies that $h = k$ and this implies that h is a *group homomorphism. The freeness of $F^*G(G)$ implies that h is an isomorphism.

For a set Rel of *group relations on G let $F^*G(G \mid Rel)$ be the free *group on the presentation $(G \mid Rel)$. Here we will restrict attention to the special case where Rel is a set of group relations on G. Let $FG(G \mid Rel)$ be the free group on the corresponding group presentation. Observe that

$$FG(G \mid Rel)^{opp} \cong FG(G \mid Rel^{opp}),$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

where Rel^{opp} is the set of relations obtained by reversing the multiplication. Again, this time in anticipation, we will write this group $FG(G^* \mid Rel^*)$. From (2.2.2) we know that

$$FG(G \mid Rel) \coprod FG(G^* \mid Rel^*)$$

is a * group. We will prove that it is free on the *group presentation $(G \mid Rel)$. Using (2.2.3) we know that there exist unique *group homomorphisms f, g and a unique group homomorphisms h so that

$$\begin{array}{ccc} F^*G(G) & \xrightarrow{\ j\ } & FG(G) \amalg FG(G^*) \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ F^*G(G \mid Rel) & \xleftarrow{\ h\ } & FG(G \mid Rel) \amalg FG(G^* \mid Rel^*) \end{array}$$

commutes.

LEMMA (2.2.4). *As a *group $FG(G \mid Rel) \coprod FG(G^* \mid Rel^*)$ is free on the presentation $(G \mid Rel)$.*

Proof. If we can establish that h is a *group homomorphism then it follows immediately from the universality properties of $F^*G(G \mid Rel)$ that h is an isomorphism. The argument we use is similar to that used in (2.2.3). Let us replace h with the group homomorphism

$$k = * \circ h \circ *,$$

obtained by composing h on either side with the appropriate involution. Then for any $a \in FG(G)$ we have

$$k(f(j(a)) = (h(f(j(a))^*))^* = (h(f(j(a^*))))^* = g(a^*)^* = g(a).$$

The uniqueness of h implies that $h = k$ and this implies that h is a *group homomorphism.

(2.3) *R-Fields.* Let R be a ring, an *R-field* is a field K together with a ring homomorphism from R to K. K is a *field of fractions* for R when this homomorphism is an embedding. The relevant setting for the study of R-fields, for a fixed R, is the category of R-fields with *specializations*, (see page 388, [**9**]). K is a *universal* R-field in case it is universal, page 389 [**9**], in this category. There is no real need for us to go into the definition of a specialization. But there are some things we should note.

(1) Specializations are equivalence classes of partial functions rather than functions, but each isomorphism forms an equivalence class on its own and hence can be thought of as a specialization (page 388, [**9**]). Actually more can

be said. Any isomorphism between two rings extends to a unique isomorphism between their universal fields of fractions if these exist, see page 89, [7].

(2) A stricter version of 'field of fractions' of a ring is illustrated by the embedding of the integers in the rationals. That is, every element of the field can be written as a quotient of elements from the ring. We will call such a field a *rational* field of fractions. A rational field of fractions is a universal field of fractions, and when it exists it is unique, up to isomorphism, as a field of fractions, cf. Theorem 8.6 and Corollary 8.7, page 38, [9].

LEMMA (2.3.1). *Let R be a *ring. If $\alpha : R \longrightarrow K$ is an R-field then*

$$\alpha \circ {}^* : R \longrightarrow K^{opp}$$

is an R-field, and, if $\beta : K \longrightarrow K^{opp}$ is a specialization then $\beta : K^{opp} \longrightarrow K$ is an R^{opp}-field specialization.

Proof. The first part is entirely trivial. The second follows directly from the definition of a specialization (page 388, [9]).

(2.4) *Coproducts of *Fields.* In this section we will recall some of the information we need about fields, we'll then modify this material to obtain some *fields. If we consider the category of 2.2 to be the category of rings with ring homomorphisms then amalgamated coproducts always exist. It is much harder to guarantee that the coproduct is

(i) *faithful*; each α_i is an embedding, and

(ii) *separating*; for each distinct $i, j \in I$,

$$\alpha_i(G_i) \cap \alpha_j(G_j) = \alpha_i \circ \phi_i(K).$$

These are both desirable properties which do hold in the more common settings of groups and semigroups.

THEOREM (2.4.1). (Bergman [2], cf. Theorem 5.1.2, Theorem 5.3.2, [7]) *The ring coproduct of a family of fields over a given field is faithful and separating. The resulting ring is a fir and hence has a universal field of fractions. This field of fractions is by definition the field coproduct of the family.*

PROPOSITION (2.4.2). *The universal field of a *ring is a *field, or, more precisely, the involution on the *ring extends to a unique involution on the universal field.*

Proof. From the universality property of K we know that there exists a unique specialization (not necessarily a full homomorphism) $^* : K \longrightarrow K^{opp}$ completing

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & K \\ {\scriptstyle *}\downarrow & & \\ R^{opp} & \xrightarrow{\alpha} & K^{opp} \end{array}$$

to a commutative diagram. Now, ${}^*\circ{}^*$ and id_K (by remark (1) of (2.3)) both

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

uniquely complete the trivial

$$\begin{array}{ccc} R & \xrightarrow{\alpha} & K \\ {\scriptstyle id_R}\downarrow & & \\ R & \xrightarrow{\alpha} & K \end{array}$$

to a commutative diagram. So $^*\circ^* = id_K$. This implies that $^* : K \longrightarrow K^{opp}$ is an isomorphism of period two and hence an involution.

Actually we have a bit more here. If

$$\alpha : R \longrightarrow S$$

is a *ring isomorphism and R and S have universal fields of fractions, K and L respectively, then it follows from (1) of (2.3) that α extends to a unique field isomorphism, $\hat{\alpha}$ from K to L. A uniqueness argument analogous to the uniqueness argument first used in (2.2.1) and similar to the one used just above can be used to show that $\hat{\alpha}$ is a *field isomorphism.

PROPOSITION (2.4.3). *If $\alpha : R \longrightarrow S$ is a *ring isomorphism and if K and L are universal fields of R and S respectively then α extends uniquely to a *field isomorphism $\hat{\alpha} : K \longrightarrow L$.*

We also have,

PROPOSITION (2.4.4). *The field coproduct of *fields with amalgamated sub*field is a *field.*

Proof. The field coproduct is, by definition, the universal field of fractions of the ring coproduct which by (2.2.1), applied to the variety of rings is the *ring coproduct. The result now follows from (2.4.2).

(2.5) *Power Series Fields* (cf. page 526, [**9**]). The material in this section is drawn mainly from [**9**], [**7**] and [**28**], and the notation used in each of these differs. As a result my choice of notation is a, sometimes sorry, compromise and care should be taken when consulting the references. Let G be a group and let K be a field. The *group ring*, $K(G)$, of G over K is the set of elements of K^G which have finite support, i.e., are nonzero in only finitely many places. Multiplication of two group ring elements a, b is given by

$$ab(g) := \sum_{uv=g} a(u)b(v) \tag{2}$$

and addition is defined componentwise,

$$(a+b)(g) := a(g) + b(g).$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

An *ordering* on a group G is a total ordering, $\leqq$ of the underlying set of the group which is preserved by the multiplication of the group. That is, if $x, y, s, t \in G$ with $x \leqq y$ and $s \leqq t$ then $xs \leqq yt$. The definition of the product of two group ring elements given above does not make sense for arbitrary elements of K^G, because in general the sum in (2) above will not be finite. However, if G is ordered, i.e., admits an ordering, then one can consider those elements of K^G with well ordered support. This set forms a field under the same operations (cf. [**37**]), called the *power series field of G over K*, which we shall write $K((G))$.

PROPOSITION (2.5.1). *If G is a *group and K is a *field then the group ring admits an involution $\clubsuit$ given by*

$$f^{\clubsuit}(g) := f(g^*)^*.$$

(We have used the symbol '*' both for the involution on G and for the involution on K. The use of the symbol '$\clubsuit$' will be restricted to the statement and proof of this proposition after which we will revert to the use of '*' for all involutions.)

Proof. Let $a, b \in K(G)$. Then, for $g \in G$,

$$\begin{aligned}(a^{\clubsuit} + b^{\clubsuit})(g) &= a^{\clubsuit}(g) + b^{\clubsuit}(g)\\ &= a(g^*)^* + b(g^*)^* = (a(g^*) + b(g^*))^*\\ &= ((a+b)(g^*))^* = (a+b)^{\clubsuit}(g).\end{aligned}$$

Also,

$$\begin{aligned}(ab)^{\clubsuit}(g) &= [ab(g^*)]^*\\ &= \left[\sum_{uv=g^*} a(u)b(v)\right]^*\\ &= \sum_{uv=g^*} [a(u)b(v)]^*,\\ &= \sum_{uv=g^*} b(v)^* a(u)^*\\ &= \sum_{v^*u^*=g} b(v^{**})^* a(u^{**})^*\\ &= \sum_{v^*u^*=g} b^{\clubsuit}(v^*)a^{\clubsuit}(u^*)\\ &= b^{\clubsuit}a^{\clubsuit}(g).\end{aligned}$$

This operation can be defined on all of K^G and it is easy to see that the propoerties of an involution hold whenever multiplication is defined and associative.

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

For an infinite group the power series field does not admit this involution. If it did then the '*' of a well ordered subset of G would again be well ordered. It is relatively easy to show that there are always well ordered sets whose '*' is not well ordered, just manufacture an element of the group which is positive, $> e$, but whose '*' is negative (this is a simple exercise) and take powers of it. However, this naive approach does give some insight into the situation. The involution yields a second ordering of the group,

$$s <_* t \quad \text{if and only if} \quad s^* < t^*.$$

We can construct a power series field using this ordering. If the constructions with respect to these two different orderings are isomorphic (over the group ring) then one can try to define an involution on the power series field by first applying the involution and then the inverse of the isomorphism. There is no reason to believe that such an isomorphism will exist in general. But if G is a free group then such an isomorphism does exist, at least for the subfield generated by $K(G)$, which is what we are interested in. This follows easily from the main theorem of [**23**], see the comment on page 343 of [**28**]. And from this it is fairly easy to establish that the map described above is an involution. The argument presented here does not explicitly use this device, even though this is what is going on behind the scenes. We will use a cleaner but perhaps less illuminating proof based on universality arguments. These come from an updated version of Lewin's Theorem 2 of [**28**]. Bergman's work on coproducts over noncommutative fields allows us to state the theorem more generally. Let $K[x, x^{-1}]$ be the free K ring on $\{x, x^{-1}\}$ satisfying the identities,

$$xk = kx, \text{ for all } k \in K$$
$$xx^{-1} = x^{-1}x = 1.$$

LEMMA (2.5.2). *$K(G) \cong \coprod_K (K[x, x^{-1}] \mid x \in X)$, where G is free on X.*

Proof. $K[x, x^{-1}]$ is a principal (left and right) ideal domain (this follows easily from the fact that the polynomial ring $K[x]$ is) and hence a fir, cf. 2.2 of [**9**]. Hence, $R := \coprod_K (K[x, x^{-1}])$ is a fir, cf. 5.3.2 of [**7**]. Every $r \in R$ can be written,

$$r = \sum_{i=1}^{n} k_i g_i$$

for some $k_1, \ldots, k_n \in K$, $g_1, \ldots, g_n \in G$, $n \in \mathbf{N}$, as can every element of $K(G)$. The freeness of G and elementary calculations show that

$$\sum_{i=1}^{n} k_i g_i \in K(G) \rightarrow \sum_{i=1}^{n} k_i g_i \in R$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

is a ring homomorphism and the universality properties of R guarantee that its an isomorphism.

THEOREM (2.5.3). *Let K be a field and let G be a free group then G can be ordered and the subfield of $K((G))$ generated by $K(G)$ is isomorphic to the universal field of fractions of $K(G)$.*

Proof. This is precisely Theorem 2 of [**28**] except the restriction to commutative fields has been lifted. In [**28**] the commutativity of the underlying field is used essentially in only four places. Once it is used to assert that $K(F)$ is a fir, where F is a free group, and hence has a universal field of fractions (line 12, page 340, [**28**]). It is used again in the proof of lemma 1 to again obtain that $K(G)$ is a fir, where G is a subgroup of a free group and hence free itself, this time so that the full matrices over $K(G)$ are closed under the formation of diagonal sums. It is used in the proof of Lemma 4, but again it is only used to establish that $K(H_i)$, $i = 1, 2$ are firs for the free groups H_1, H_2. Finally it is used in the proof of Proposition 6, again all that is needed is that $K(G)$ is a fir. But (2.5.2) allows us to make these assertions for noncommutative K as well.

PROPOSITION (2.5.4). *Let K be a *field and let $G = \prod_{i=1}^{n} G_i$ be a product of *groups each of whose group reduct is free, (hence G can be ordered by ordering each G_i and using the lexicographic ordering, cf.* [**7**]). *Then the involution which exists on $K(G)$ by virtue of* (2.5.1) *extends to an involution on the subgroup of $K((G))$ generated by $K(G)$.*

Proof. Before beginning the proof proper let us make some key observations. First,

$$K\left(\prod_{i=1}^{k} G_i\right) \subseteq K(G)$$

naturally, and hence

$$K\left(\left(\prod_{i=1}^{k} G_i\right)\right) \subseteq K((G)),$$

naturally as well, for each $k \leqq n$. More generally, if F is a subfield of $K((\prod_{i=1}^{k} G_i))$ then $F(G_{k+1}) \subseteq K((G))$ naturally, and hence $F((G_{k+1})) \subseteq K((G))$ naturally as well. Formally, 'naturally' means that the inclusion extends the usual inclusions of the groups under consideration into products of which they are factors.

For $k \leqq n$ let

$$K_0 := K,$$
$$K_k := K_{k-1}\langle G_k \rangle,$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

where $K_{k-1}\langle G_k\rangle$ is the subfield of $K_{k-1}((G_k))$ generated by $K_{k-1}(G_k)$. By (2.5.3), K_k is a universal field of fractions for $K_{k-1}(G_k)$ which sits naturally inside $K((G))$. Our hypothesis is that the involution on $K(G)$ restricted to $K(\prod_{i=1}^{k-1} G_i)$ extends uniquely to one on K_{k-1}.

By (2.5.1), any involutions on K_{k-1} and G 'lift' uniquely to one on $K_{k-1}(G_k)$, and it is easily seen that if we take the involutions to be the ones provided by, for K_{k-1}, the inductive hypothesis and, for G_k, the statement of the theorem, that this involution agrees with the restriction of the involution on $K(G)$ to $K(\prod_{i=1}^{k} G_i)$. Since K_k is universal for $K_{k-1}(G_k)$ it follows by (2.4.2) that K_k admits a unique involution extending the one on $K_{k-1}(G_k)$. If we take $k = 1$ and interpret $\prod_{i=1}^{0}(G_i)$ as the empty product we obtain the one element group. The hypothesis is then trivially true, for it says that the involution induced on K by the restriction of the involution on $K(G)$ to K extends uniquely to an involution on K.

We have to show more than this. Let us call the subfield of $K((G))$ generated by $K(G)$, $K\langle G\rangle$. We must show that L, the subfield of $K\langle G\rangle$ generated by $K(H)$ is a sub*field of $K\langle G\rangle$, where H is an arbitrary sub*group of G. The existence of an involution on $K\langle G\rangle$ makes this proof easy but it does not appear to follow from any universality arguments. Let A be an arbitrary subset of $K\langle G\rangle$ and define,

$$\begin{aligned} A^{-1} &:= \{a^{-1} : a \in A\}, \\ A^{*} &:= \{a^{*} : a \in A\}, \\ A^{2} &:= \{ab : a, b \in A\}, \\ 2A &:= \{a + b : a, b \in A\}. \end{aligned}$$

LEMMA (2.5.5). *If* $A = A^*$ *then*

$$\begin{aligned} 2A &= (2A)^*, \\ A^2 &= (A^2)^*, \end{aligned}$$

and

$$A^{-1} = (A^{-1})^*.$$

Proof. Only the last part even requires comment. The fact that inverses are unique in a field implies that in any *field the 'identity' $x^{-1*} = x^{*-1}$, holds.

We shall build L recursively:

Definition (2.5.6). Let

$$L_0 := K(H)$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

and

$$L_{i+1} := (2L_i)^2 \cup ((2L_i)^2)^{-1}.$$

LEMMA (2.5.7). *For each i, the support of L_i is contained in H and $L_i = L_i^*$.*

Proof. This is obviously true for L_0. If $L_i = L_i^*$ then by (2.5.4), $L_{i+1}^* = L_{i+1}$. The elements of $K\langle G\rangle$ with support in H form a field. Since the definition of L_{i+1} only involves closing L_i under the operations of this field, the support of L_{i+1} is contained in H whenever the support of L_i is.

THEOREM (2.5.8). *The subfield of $K\langle G\rangle$, L, generated by $K(H)$ is a sub*field of $K\langle G\rangle$, for any sub*group H of G.*

Proof. Clearly $L = \bigcup_{i=1}^{\infty} L_i$.

(2.6) *Skew Polynomial Rings* (cf. pages 52, 53 [**9**]). Let F be a field and σ an automorphism of F. The *skew polynomial ring* $F[t;\sigma]$ has as underlying set the set of all formal power series in t, i.e., all expressions of the form

$$\sum_{i=1}^{n} f_i t^i, \quad f_i \in F, n \in \mathbf{N}.$$

Addition is defined as usual, and multiplication with t by an element of F from the left is as well. However, if $f \in F$ then

$$tf := \sigma(f)t.$$

One multiplies two power series together in the normal way using this rule to bring occurrences of t to the right end of products. The following result is stated at the bottom of page 53 of [**9**].

THEOREM (2.6.1). *The skew polynomial ring $F[t;\sigma]$ has a rational field of fractions $F(t;\sigma)$, called the skew polynomial field.*

PROPOSITION (2.6.2). *If F is a *field and σ is a *automorphism of F then the involution on F extends to one on $F(t;\sigma)$ by sending t to t^{-1}.*

Proof. This result is similar to Proposition (2.5.1). The skew polynomial field is constructed in essentially the same manner as the power series field of the group ring of an ordered group, cf. [**9**]. One allows not just finite series but also infinite series with only finitely many negative coefficients i.e., all series of the form,

$$a = \sum_{i=-n}^{\infty} a_i t^i.$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

Here again there is an obvious candidate for the '*' of such a series,

$$\sum_{i=-n}^{\infty} \sigma^{-1}(a_i^*)t^{-i}.$$

And again, this is not an element of the field. By remark (2) of (2.3) we know that $F(t;\sigma)$ is the universal field of fractions of $F[t;\sigma]$ and formally we will use a universality argument to extend an involution on a ring, A, containing $F[t;\sigma]$, to one on $F(t;\sigma)$. But of course the induced underlying isomorphism, over A, implements the natural involution just as it does for the power series field. The intermediate ring we will consider is the ring consisting of all finite series, allowing negative as well as positive powers of t, i.e.,

$$A := \left\{ \sum_{i=-n}^{n} a_i t^i : a_i \in F, n \in \mathbf{N} \right\}.$$

It is clear in general that if $B \subseteq A \subseteq K$ are rings and if K is rational field of fractions for B then K is a rational field of fractions for A. Hence by (2.4.2) any involution on A will extend to one on $F(t;\sigma)$. For $a \in A$ as above define,

$$a^* := \sum_{i=-n}^{n} \sigma^{-i}(a_i^*)t^{-i}.$$

We need only show that * is an involution on A to prove the result. First let us show that $*\circ* = id_A$. We have,

$$\begin{aligned} a^{**} &= \left(\sum_{i=-n}^{n} \sigma^{-1}(a_i^*)t^{-i} \right)^* \\ &= \sum_{i=-n}^{n} \sigma^{-(-i)}(\sigma^{-i}(a_i^{**}))t^{-(-i)} = a. \end{aligned}$$

Compatibility with addition is also easy to establish, let

$$b = \sum_{i=-n}^{n} b_i t^i,$$

then

$$\begin{aligned} (a+b)^* &= \sum_{i=-n}^{n} ((a_i + b_i)t^i)^* \\ &= \sum_{i=-n}^{n} \sigma^{-i}((a_i + b_i)^*)t^{-i} \\ &= \sum_{i=-n}^{n} (\sigma^{-i}(a_i^*) + \sigma^{-i}(b_i^*))t^{-i} \\ &= \sum_{i=-n}^{n} \sigma^{-i}(a_i^*)t^{-i} + \sum_{i=-n}^{n} \sigma^{-i}(b_i^*)t^{-i} \\ &= a^* + b^*. \end{aligned}$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

It remains to show that for $a, b \in A$ we have

$$(ab)^* = b^*a^*.$$

The commutation rule $tm = \sigma(m)t$ gives,

$$\sigma^{-1}(m)t^{-1} = t^{-1}[t\sigma^{-1}(m)]t^{-1} = t^{-1}[mt]t^{-1} = t^{-1}m.$$

Let

$$ab := \sum_{i=-2n}^{2n} c_i t^i.$$

Direct computation gives

$$c_k t^k = \sum_{i+j=k} a_i t^i b_j t^j = \sum_{i+j=k} a_i \sigma^i(b_j) t^k$$

and so,

$$c_k = \sum_{i+j=k} a_i \sigma^i(b_j).$$

Hence,

$$c_k^* = \sum_{i+j=k} \sigma^i(b_j^*) a_i^*$$

and

$$(ab)^* = \sum_{k=2n}^{-2n} t^{-k} c_k^* = \sum_{k=2n}^{-2n} \sigma^{-k}(c_k^*) t^{-k}$$

so the $-k$'th coefficient of $(ab)^*$ is

$$\begin{aligned}\sigma^{-k}(c_k^*) &= \sigma^{-k}\left(\sum_{i+j=k} \sigma^i(b_j^*) a_i^*\right) \\ &= \sum_{i+j=k} \sigma^{i-k}(b_j^*)\sigma^{-k}(a_i^*).\end{aligned}$$

Now,

$$a^* = \sum_{i=-n}^{n} (a_i^*) t^{-i},$$

$$b^* = \sum_{j=-n}^{n} (b_j^*) t^{-j}.$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

and let

$$b^*a^* = \sum_{i=-2n}^{2n} d_i t^i$$
$$= \left(\sum_{j=-n}^{n} \sigma^{-j}(b_j^*)t^{-j}\right)\left(\sum_{i=-n}^{n} \sigma^{-i}(a_i^*)t^{-i}\right).$$

Then,

$$d_{-k}t^{-k} = \sum_{j+i=k} \sigma^{-j}(b_j^* t^{-j}\sigma^{-i}(a_i^*)t^{-i})$$
$$= \sum_{j+i=k} \sigma^{-j}(b_j^*)\sigma^{-j-i}(a_i^*).$$

And so the $-k$'th coefficient of b^*a^* is

$$\sum_{j+i=k} \sigma^{-j}(b_j^*)\sigma^{-i-j}(a_i^*)$$
$$= \sum_{j+i=k} \sigma^{i-k}(b_j^*)\sigma^{-k}(a_i^*)$$

which is what we wished to prove.

(2.7) *Hermitian Forms on *Fields.* In this section we will give methods of creating Hermitian forms for *fields. The notation is the hardest thing about the proofs of the two results in this section.

THEOREM (2.7.1). *Let R be a *ring and suppose F is a rational R-field, then F is a *field and any nondegenerate Hermitian form on R extends to a nondegenerate Hermitian form on F.*

Proof. The involution on R extends to one on F by (2.4.2). Let $(\alpha_i, \ldots, \alpha_n;^*)$ be a form on R and suppose there exist $a_1, \ldots, a_n \in F$ so that

$$\sum_{i=1}^{n} a_i^* \alpha a_i = 0.$$

We will prove that there exist $b_i, \ldots, b_n \in R$ so that

$$\sum_{i=1}^{n} b_i^* \alpha_i b_i = 0,$$

and so that $b_i = 0$ if and only if $a_i = 0$. This will be done by proving the following statement inductively.

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

For each $k, 0 \leqq k \leqq n$, *there exists a sequence* $b(k)_1, \ldots, b(k)_n \in F$ *so that*

$$(i) \quad \sum_{i=1}^{n} b(k)_i^* \alpha_i b(k)_i = 0,$$

$$(ii) \quad b(k)_i = 0 \text{ if and only if } a(k)_i = 0,$$

$$(iii) \quad b(k)_1, \ldots, b(k)_k \in R.$$

Proof. The sequence $a_1, \ldots, a_n$ works for $k = 0$. Suppose $b(k)_1, \ldots, b(k)_n$ satisfies (i), (ii), (iii). Since F is rational there exist $p, q \in R$ with $q \neq 0$ and $b(k)_{k+1} = pq^{-1}$. Now define,

$$b(k+1)_i := b(k)_i q.$$

Clearly (ii) and (iii) are satisfied. For (i) we have,

$$\begin{aligned} &\sum_{i=1}^{n} b(k+1)_i^* \alpha_i b(k+1)_i \\ &= \sum_{i=1}^{n} q^* b(k)_i^* \alpha_i b(k)_i q \\ &= q^* \left(\sum_{i=1}^{n} b(k)_i^* \alpha_i b(k)_i \right) q = 0. \end{aligned}$$

Given a field E the polynomial ring in (the indeterminate α) is written $E[\alpha]$. If E is a *field then assigning $\alpha^* = \alpha$ induces a unique nondegenerate involution on $E[\alpha]$. For the remainder of this section we shall refer to $E[\alpha]$ as a *ring with this understanding. The construction we are interested in here is the transcendental extension of a *field. We can write $E[\alpha]$ as $E[\alpha; id_E]$ then the *transcendental extension* of E in α is, by definition, the skew polynomial field $E(\alpha) = E(\alpha; id_E)$.

LEMMA (2.7.2). *Let E be a field and let $(\alpha_1, \ldots, \alpha_k; ^*)$ be a Hermitian form on E. Then * extends to an involution * on $E(\alpha)$ and $(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha; ^*)$ is a hermitian form on $E(\alpha)$.*

Proof. By (2.6.2) and (2.7.1) it is enough to show that $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n; ^*)$ is a nondegenerate form on $E[\alpha]$. Assume $a_1, \ldots, a_n \in E[\alpha]$ with

$$\sum_{i=1}^{n-1} a_i^* \alpha_i a_i + a_n \alpha a_n = 0.$$

Each a_i is a polynomial in α with coefficients in E. Let m be the maximum degree of the polynomials $a_i, 1 \leqq i \leqq n$. There are two cases to consider. First we will assume that the degree of a_n is less than m and that $m > 0$. Let

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

$i(1), \ldots i(k)$ be the indices for which the degree m is attained, and let $b_{i(j)}$ be the coefficient of α^m in $a_{i(j)}$. Then the coefficient of α^{2m} in

$$\sum_{i=1}^{n-1} a_i^* \alpha_i a_i$$

is

$$b := \sum_{j=1}^{k} b_{i(j)}^* \alpha_{i(j) b_i(j)}.$$

But the highest degree attainable by the polynomials $a_n^* \alpha a_n$ is $2(m-1)+1 < 2m$. We can therefore conclude that $b = 0$. But since the form is nondegenerate on $E, b_{i(j)} = 0$ for each j, contrary to our assumption that the degree m is attained.

The second possibility is that the degree of a_n is m. (This includes the case $m = 0$, i.e., each a_i is constant.) In this case we observe that the degree of

$$\sum_{i=1}^{n-1} a_i^* \alpha_i a_i$$

is less than or equal to $2m$. But the degree of $a_n^* \alpha a_n$ is $2m + 1$. It is therefore not possible for these two polynomials to add together to give 0.

We now wish to apply this lemma to a transcendental extension of higher dimension. Formally, we will consider a *k-dimensional transcendental extension* to be the composition of k, 1-dimensional transcendental extensions. This, with (2.5.2) yields the following.

COROLLARY (2.7.3). *Let $F := E(\alpha_2, \ldots, \alpha_n)$ be an $n-1$ dimensional transcendental extension of a *field E. Then the involution on E extends to one on F so that $(1, \alpha_2, \ldots, \alpha_n; ^*)$ is a nondegenerate form on F.*

3. The main theorem.

(3.1) *A *Group proposition.* The objective of this subsection is to demonstrate the existence of a special six generated, thirty six relator, *group with an unsolvable word problem. We start by recalling some notation. Let (G, Rel) be a group presentation. The corresponding presented group is written $FG(G \mid Rel)$. If $Rel = \emptyset$ then we just omit it and if G and Rel are listed we may omit the set brackets. We may also consider the free *group on the same presentation which we will write $F^*G(G \mid Rel)$. The result we will prove is

PROPOSITION (3.1.1). *There exists a finitely presented *group*

$$G_* = F^*G(x_1, \ldots, x_6 \mid u_1, \ldots, u_{36})$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

*so that the finitely presented *group*

$$G_{**} = F^*G(x_1^*x_1, \ldots, x_6^*x_6 \mid u_1, \ldots, u_{36})$$

*embeds in G_*, and so that G_{**} has an unsolvable word problem. (Of course, this necessarily means that each u_j is a *group word on the *groups words $x_1^*x_1, \ldots, x_6^*x_6$.)*

The peculiarity of this presentation is the fact that the generators of G_{**} are of the form x^*x, $x \in G_*$. It is this that will allow us to use (1.9.3) to code the unsolvability of G_{**} into the elements of a Hermitian form.

Let $FG(n)$, $n \leqq \omega$, be the free group on n generators. The commutator subgroup of $FG(2)$ is isomorphic to $FG(\omega)$ and is normal. If N is a normal subgroup of $FG(n)$ then the normal subgroup, N_0, of $FG(\omega)$ generated by N has the property that $N_0 \cap FG(n) = N$. It follows from this that if $FG(n)/N$ has unsolvable word problem then, considering N_0 as a subgroup of $FG(2)$, we can conclude that $FG(2)/N_0$ also has an unsolvable word problem. Since there exists a finitely generated twelve relator group with unsolvable word problem [**10**], we can conclude:

LEMMA (3.1.2). *There exists a two generated, twelve relator group with unsolvable word problem.*

Let this group be $FG(x_1, x_2 \mid r_1, \ldots, r_{12})$. We give a simple application of Lemma 12.52, page 344, of [**41**].

LEMMA (3.1.3). *Let $E = FG(S \mid D)$ be a finitely presented group and let*

$$\hat{E} := FG(S, t \mid D, t^{-1}x_i t x_i^{-1}, i \in I),$$

where the x_i are words on S. Let w be a word on S. If $t^{-1}wt = w$ in $\hat{E}$ then the group element of E determined by w is in the subgroup of E generated by the x_i.

LEMMA (3.1.4). *The group $G := FG(x_1, x_2, t \mid U)$ has an unsolvable word problem where U consists of the relations;*

$$(U_1) \quad x_i^{-1}r_j x_i r_j^{-1} (= 1), \quad i = 1, 2, j = 1, \ldots, 12,$$

and

$$(U_2) \quad t^{-1}r_j t r_j^{-1} (= 1), \quad j = 1, \ldots, 12.$$

Proof. There exists a group homomorphism

$$FG(x_1, x_2 \mid U_1) \longrightarrow FG(x_1, x_2 \mid r_1, \ldots, r_{12})$$

whose kernel corresponds to the normal subgroup, N, generated by $\{r_1, \ldots, r_{12}\}$. But since each r_i is central in $FG(x_1, x_2 \mid U_1)$, N is just the subgroup of $FG(x_1, x_2 \mid U_1)$ generated by $\{r_1, \ldots, r_{12}\}$. Let w be a group word on the letters x_1, x_2, then $w = 1$ in $FG(x_1, x_2 \mid r_1, \ldots, r_{12})$ if and only if $w \in N$ in $FG(x_1, x_2 \mid U_1)$. We will apply (3.1.3) to $E = FG(x_1, x_2 \mid U_1)$. Hence consider the group $\hat{E} = FG(x_1, x_2, t \mid U)$, and group word w on x_1, x_2. Then,

$$w = 1 \text{ in } FG(x_1, x_2 \mid r_1, \ldots, r_{12})$$

implies

$$w \in N \text{ in } E = FG(x_1, x_2 \mid U_1)$$

implies

$$t^{-1}wt = w \text{ in } \hat{E} = FG(x_1, x_2, t \mid U).$$

Conversely, by (3.1.3),

$$t^{-1}wt = w \text{ in } \hat{E} = FG(x_1, x_2, t \mid U)$$

implies

$$w \in N \text{ in } E = FG(x_1, x_2 \mid U_1)$$

implies

$$w = 1 \text{ in } FG(x_1, x_2 \mid r_1, \ldots, r_{12}).$$

A solution to the word problem for $FG(x_1, x_2, t \mid U)$ would therefore yield a solution to the word problem for $FG(x_1, x_2 \mid r_1, \ldots, r_{12})$, which does not exist.

To ease notation let us rename the generators of G, s_1, s_2, s_3 and define $S := \{s_1, s_2, s_3\}$. Let $G^{opp} = (S^* \mid U^*)$ (the *'s are, for now, just suggestive) be the opposite group of G and let

$$G_0 := G \coprod G^{opp} = FG(S \cup S^* \mid U \cup U^*).$$

Before going on with the construction let us note:

LEMMA (3.1.5). *G_0 is a *group and as a *group has presentation*

$$F^*G(S \mid U).$$

Proof. This is an application of (2.2.4).

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

For $i = 1, 2, 3$ let $F_i := FG(a_i, b_i, c_i, d_i)$ and let $\langle s_i, s_i^* \rangle_{G_0}$ be the subgroup of G_0 generated by $\{s_i, s_i^*\}$. Define

$$\phi_i : \langle s_i, s_i^* \rangle_{G_0} \longrightarrow F_i$$

by

$$s_i \longrightarrow a_i c_i b_i d_i$$
$$s_i^* \longrightarrow b_i d_i a_i c_i.$$

For this to make sense we must first establish that $\langle s_i, s_i^* \rangle_{G_0}$ is free on $\{s_i, s_i^*\}$. Since all the relations in U are commutators we know that there is a homomorphism from G onto the free abelian group on 3 generators. Symmetrically, there is a homomorphism from G^{opp} onto the free abelian group on 3 generators. Hence there is a homomorphism from G_0 into the coproduct of the free abelian group on 3 generators with itself. The image of $\langle s_i, s_i^* \rangle_{G_0}$ is the free group on $\{s_i, s_i^*\}$ and it follows that $\langle s_i, s_i^* \rangle_{G_0}$ is also free on $\{s_i, s_i^*\}$. This establishes that ϕ_i exists as a group homomorphism. Now any nontrivial group relation (one not following from the group axioms) between the elements of

$$\langle a_i c_i b_i d_i, b_i d_i a_i c_i \rangle_{F_i}$$

would be a nontrivial relation holding between the elements of F_i, because for neither of the generators is it the case that when one is multiplied by itself, the other, or the other's inverse, does any cancellation takes place. It follows that

$$\langle a_i c_i b_i d_i, b_i d_i a_i c_i \rangle_{F_i}$$

is free on $a_i c_i b_i d_i, b_i d_i a_i c_i$, and we have

LEMMA (3.1.6). *Each ϕ_i is a group embedding.*

Definition (3.1.7). Define

$$G_1 := G_0 \coprod_{\phi_1} F_1,$$
$$G_2 := G_1 \coprod_{\phi_2} F_2,$$
$$G_3 := G_2 \coprod_{\phi_3} F_3.$$

Replace the elements of the generating set $S \cup S^*$ of G with the generators a_i, b_i, c_i, d_i, of $F_i, i = 1, 2, 3$, and make the appropriate substitutions in the relations $U \cup U^*$ to obtain the presentation

$$(\{a_i, b_i, c_i, d_i \mid i = 1, 2, 3\} \mid U \cup U^*).$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

(The notation $\coprod_{\phi_i}$ means to amalgamate the subgroup $\langle s_i, s_i^* \rangle_{G_0}$, identifying it with its image under the embedding ϕ_i.)

LEMMA (3.1.8).

$$G_3 = FG(\{a_i, b_i, c_i, d_i, i = 1, 2, 3\} \mid U \cup U^*) \tag{3}$$

and the map

$$a_i \longrightarrow c_i,$$
$$b_i \longrightarrow d_i$$

extends to an involution on G_3. *As a* **group*

$$G_3 = F^*G(a_1, a_2, a_3, b_1, b_2, b_3 \mid U). \tag{4}$$

Proof. A presentation of G_1 is

$$FG(a_1, b_1, c_1, d_1, s_2, s_3, s_2^*, s_3^* \mid U \cup U^*),$$

where each occurrence of s_1 in U is replaced by $a_1c_1b_1d_1$ and each occurrence of s_1^* is replaced by $b_1d_1a_1c_1$. Similarly G_2 is obtained by making the appropriate subscript 2 substitutions, and G_3 by making the appropriate subscript 3 substitutions. This gives

$$G_3 = FG(\{a_i, b_i, c_i, d_i, \quad i = 1, 2, 3\} \mid U \cup U^*),$$

where each occurrence of s_i in U is replaced by $a_ic_ib_id_i$ and each occurrence of s_i^* is replaced by $b_id_ia_ic_i$. Thus (3) is a presentation of G_3. To prove the second part we make two observations. First (3.1.5) gives us a presentation of G_0 as a *group, and (2.2.3) gives us a presentation of each F_i as a *group (since the free group on 4 generators can be thought of as the coproduct of the free group on 2 generators with its opposite). Secondly, Lemma (2.2.1) applied to the variety of groups lets us put these presentations together to obtain the *group presentation (4).

Proof (of (3.1.1)). We let G_* be the *group G_3 defined above, (4), with $x_1 := a_1$, $x_2 := b_2$, $x_3 := a_2$, $x_4 := b_2$, $x_5 := a_3$, and $x_6 := b_3$. Then G_{**} is G_0 as a *group, cf. (3.1.5). The unsolvability of G and the fact that G embeds as a group in G_0 implies that the word problem for G_{**} is unsolvable.

Let us close this section by making two minor observations. We only use the fact that the elements of U are all commutators and hence, Lemmas (3.1.3), (3.1.4), in order to establish that ϕ_i is an embedding for each i, which we really do need. Perhaps there is an easier way to do this but I can't see how to do it. Let me emphasize that this fact is not used directly anywhere else. Secondly,

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

we have explicitly calculated the number of generators, 6, and relations, 36, which are at present required. This will not effect the number of generators the final finite MOL presentation will have, but it will effect the number of relations in this presentation, and this will be of importance in situations to be handled in a second paper. Any reduction in the number of relations needed for an unsolvable group word problem, or an obviation of Lemma (3.1.4), could significantly reduce this number.

(3.2) *The Construction.* In this section we will mimic McIntyre's construction, as presented in Section 6.5 of [7], in the *field setting.

Definition (3.2.1). Let

$$F_X := F^*G(x_1, \ldots, x_6), F_Y := F^*G(y_1, \ldots, y_6),$$

$$G := F_X \times F_Y,$$

and let

$$F_{X^*X} := FG(x_1^*x_1, \ldots, x_6^*x_6), F_{Y^*Y} := FG(y_1^*y_1, \ldots, y_6^*y_6),$$
$$G_0 := F_{X^*X} \times f_{Y^*Y}.$$

Let U be a finite subset of F_{X^*X} (obstensibly, U is the set of relations defining the *group of Proposition (3.1.1)), and let H be the sub*group of $G_0 \subseteq G$ generated by the words

$$x_1^*x_1, y_1^*y_1, \ldots, x_6^*x_6, y_6^*y_6,$$

and U. Let N be the normal (as a subgroup) sub*group of G_0 generated by U.

LEMMA (3.2.2). $N = F_{X^*X} \cap H$.

Proof. Observe that N is the normal subgroup of F_{X^*X} generated by $U \cup U^*$. With this in mind the lemma is just Lemma 6.5.1 of [7].

Since

$$F^*G(x_1, \ldots, x_6) \cong FG(x_1, \ldots, x_6, x_1^*, \ldots, x_6^*),$$

and since every free group can be ordered, cf. page 22, [7], F_X can be ordered. By the same token F_Y can be ordered, and hence G can be ordered lexicographically. So we can form $\mathbf{Q}((G))$, the power series field of the group ring $\mathbf{Q}(G)$, of G over the rational numbers. From (2.5.4) we know that the subfield of $\mathbf{Q}((G))$ generated by $\mathbf{Q}(G)$ is a *field. Call this *field K. Let L be the *subfield of K generated by $\mathbf{Q}(H)$ which exists and whose support is contained in H by (2.5.5). We take the field coproduct of $\mathbf{Z}$ copies of K, amalgamating L, to obtain the field D. By (2.4.4), D is a *field. Mapping the i'th copy of K to the $(i+1)$'st

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

identically, for all i, induces an automorphism σ of D, and by (2.4.3) and the definition of the field coproduct,

LEMMA (3.2.4). *σ is a *automorphism of D.*

We form the skew polynomial ring $D[t;\sigma]$ and its field of fractions $D(t;\sigma)$. From (2.6.2) we know that $D(t;\sigma)$ admits an involution extending that of D and sending t to t^{-1}. Let E be a thirteen dimensional transcendental extension of $D(t;\sigma)$ in the indeterminates $\beta_2,\ldots,\beta_{14}$. Note that F_{X^*X} is 'embedded' in E via the following list of 'containments',

$$(5) \qquad f_{X^*X} \subseteq F_X \subseteq G \subseteq K_0 \subseteq D(t;\sigma) \subseteq E.$$

LEMMA (3.2.5). *For $w \in F_{X^*X} \subseteq E$;*

$$w \in N$$

if and only if

$$wt = tw \in D(t;\sigma) \subseteq E.$$

Proof. In light of our (3.2.2) this is just 6.5.2 of [7].

We want to disguise t as an element of the form x^*x as well, so we define $\tau := t + 1$.

LEMMA (3.2.6). *For $w \in F_{X^*X}$ in E;*

$$w \in N$$

if and only if

$$w\tau^*\tau = \tau^*\tau w \text{ in } E.$$

Proof. We will shown that for any $k \in K_0$,

$$k\tau^*\tau = \tau^*\tau k$$

implies

$$kt = tk.$$

This with (3.2.5) gives one direction; the other direction of the implication follows immediately from (3.2.5).

$$k\tau^*\tau = k(t + t^{-1} + 2) \quad \text{and} \quad \tau^*\tau k = (t + t^{-1} + 2)k.$$

If these are equal then $k(t+t^{-1}) = (t+t^{-1})k$ and

$$\sigma(k)t + \sigma^{-1}(k)t^{-1} = kt + kt^{-1}.$$

Or, multiplying on the right by t and rearranging,

$$(\sigma(k) - \sigma^{-1}(k))t^2 = k - \sigma^{-1}(k).$$

This implies that $k = \sigma^{-1}k$ or that $\sigma k = k$, from which it follows that $kt = tk$.

From (2.7.3) we know that $(1, \beta_2, \ldots, \beta_{14}; ^*)$ is a Hermitian form for an OC on $\hat{L}(E_E^{14})$. This is not the Hermitian form that we want though. The MOL generated by the corresponding frame does not capture enough. We modify the form to capture more.

Definition (3.2.8). Define $\alpha_2, \ldots, \alpha_{14}$ by setting

$$\alpha_i := \beta_i x_{i/2}^* x_{i/2}, \text{ for } i \text{ even}, 2 \leqq i \leqq 12,$$
$$\alpha_i := \beta_i y_{(i-1)/2}^* y_{(i-1)/2}, \text{ for } i \text{ odd}, 3 \leqq i \leqq 13,$$

and

$$\alpha_{14} := \beta_{14} \tau^* \tau.$$

PROPOSITION (3.2.9). *$(1, \alpha_2, \ldots, \alpha_{14}; ^*)$ is a Hermitian form on E. The *group generated by the form elements $\alpha_2, \ldots, \alpha_{13}$, as a sub*group of the multiplicative group of E, is isomorphic to $G_0 \subseteq D(t; \sigma)$. The isomorphism is defined by the obvious association of generators given above, explicitly,*

$$(6) \qquad x_i^* x_i \longrightarrow \alpha_{2i}$$
$$y_i^* y_i \longrightarrow \alpha_{2i+1}.$$

*Furthermore, if w is a *group word on the generators of G_0 then w commutes with t in G_0 if and only if the image of w under this isomorphism commutes with α_{14}.*

Proof. The first part follows directly from (1.9.3). Before starting the second part let us make two simple observations. If a subgroup of a *group contains along with each generator its '*', then it is a sub*group. Secondly, if two *groups are isomorphic as groups, and if the '*' of each element of a generating set of the first *group is sent to the '*' of its image in the second then the isomorphism is a *group isomorphism. These facts will be used below without comment.

Let $E^\times$ be the multiplicative *group of E, and let G_β be the sub*group of $E^\times$ generated by $\beta_2, \ldots, \beta_{14}$, and consider the copy of G_0 sitting inside $E^\times$, cf. (5). The sub*group of $e^\times$ generated by these *groups is isomorphic to the

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

product $G_\beta \times G_0$. This is because the field extensions are transcendental. Now, the relations.

$$x_i^* x_i y_j^* y_j = y_j^* y_j x_i^* x_i, \quad i,j = 1,\dots,6$$

are the relations of a presentation of the *group G_0 and these translate via the map (6) to the relations

$$\alpha_i \alpha_j = \alpha_j \alpha_i,$$

for i even and j odd, $2 \leqq i, j \leqq 13$, which are easily seen to hold because the β_i's are all central. Thus the map (6) extends to a *group homomorphism. Its inverse is given by the restriction of the projection from $G_\beta \times G_0$ onto G_0, to the *group generated by $\alpha_2,\dots,\alpha_{13}$. The final part of the claim follows from the centrality of the β_i's and from (3.2.6).

(3.3) *The Proof of the Main theorem.* We have observed in Section (1.10) that the free MOL on an orthogonal n-frame, $Frm(n)$, is three generated. We begin by giving three sets of ring relations which hold between the elements of the Hermitian form of (3.2.9).

$$(\Phi_1) \quad \alpha_i \alpha_j = \alpha_j \alpha_i, \quad i \text{ even}, j \text{ odd}, 2 \leqq i, j \leqq 13.$$

Let $v_1,\dots,v_{36}$ be the words obtained by substituting each occurrence of $x_j^* x_j$ with α_{2j} in the words $u_1,\dots,u_{36}$ of Proposition (3.1.1) and define,

$$(\Phi_2) \quad v_i \alpha_{14} = \alpha_{14} v_i$$

and

$$(\Phi_3) \quad \alpha_{2j}\alpha_{2j+1}\alpha_{14} = \alpha_{14}\alpha_{2j}\alpha_{2j+1}, \quad j = 1,\dots,6.$$

We let $\Phi := \Phi_1 \cup \Phi_2 \cup \Phi_3$.

THEOREM (3.3.1). *$Frm(14,\Phi)$ has an unsolvable word problem.*

Proof. The proof is essentially Freese's (2.6) of [**16**]. Let R_Φ be the coordinatizing ring of $Frm(14,\Phi)$, cf. (1.10.1), and $(1,\Omega_2,\dots,\Omega_{14};^*)$ the associated Hermitian form. Since the ring E together with the form of (3.2.9) satisfy the relations Φ there are, by (1.10.1), unique homomorphisms,

$$f : Frm(14,\Phi) \longrightarrow \hat{L}(E_E^{14}),$$
$$\hat{f} : R_\Phi \longrightarrow E,$$

so that for all $r \in R_\Phi$,

$$f((1,r,r,0,\dots,0)R_\Phi) = 1(1,\hat{f}(r),\hat{f}(r),0,\dots,0)E,$$

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

and

$$\hat{f}(\Omega_i) = \alpha_i, \quad 2 \leqq i \leqq 14.$$

The relations Φ_0 are the defining relations of the (isomorphic copy of the) group G_0, cf. (3.2.9). Therefore the restriction of $\hat{f}$ to the multiplicative group generated by $\Omega_2, \ldots, \Omega_{14}$ in R_Φ is a *group isomorphism.

Define F, H and N in R_Φ analogously to F_{X^*X}, H and N of (3.2.1) via the isomorphism given in (3.2.9) and the one given above. We claim that for $w \in F$ in R_Φ we have,

$$w \in N$$

if and only if

$$w\Omega_{14} = \Omega_{14}w.$$

If $w \in N$ then it is easily seen that $w \in H$, cf. (2.1) of [**16**] and (3.2.2). Now, from Φ_1, Φ_2 of Φ and the definition of H, for any $h \in H$,

$$h\Omega_{14} = \Omega_{14}h.$$

Hence, $w\Omega_{14} = \Omega_{14}w$. Conversely, if

$$w\Omega_{14} = \Omega_{14}w \quad \text{in } R_\Phi$$

then

$$w\alpha_{14} = \alpha_{14}w \quad \text{in } \hat{f}(R_\Phi).$$

Then, using the group isomorphism of (3.2.9), we have

$$wt = tw \quad \text{in } E.$$

It follows from (3.2.5) that

$$w \in N \quad \text{in } E.$$

But we have gone from the *group F in R_Φ to the *group F_{X^*X} in E via the composition of two *group isomorphisms, and since $N \subseteq F$ in R_Φ was also defined via this composition we can conclude that $w \in N$ in R_Φ as well.

A solution to the word problem for $Frm(14, \Phi)$ would therefore yield a solution to the word problem for the *group $G_{**} \cong F/N$, of (3.1.1), which does not exist.

https://doi.org/10.4153/CJM-1989-044-8 Published online by Cambridge University Press

THEOREM (3.2.2). *There exists a* 3*-generated finitely presented* MOL *with unsolvable word problem.*

(3.4) *Concluding remarks.* It is relatively easy to see that this construction will work, and Theorem (3.2.2) hold, for any variety of MOL's, which captures the orthocomplemented projective geometries of a sufficiently high dimension, (here 14). However, in the situation of varieties generated by projective geometries we can prove more, namely that the free word problem is unsolvable. Though this is quite easy it requires the development of further techniques and will be done in a second paper. (Roughly, we have to mimic the second half of Freese's proof [**16**] by finding a projective configuration with which we can 'pull unsolvability' back into a free algebra.) Unfortunately I have been unable to adapt the argument to the free MOL, the problems with this will also be discussed. It should also be noted that the argument for four generators is significantly easier than the three generator case we have presented here. One can take the McIntyre-Cohn construction, more or less, as it stands because the extra generator means one doesn't have to code all the information into the elements of a Hermitian form. For dimension-generator counting reasons this construction will be of use in the n-distributive case and we will also outline this argument in the second paper.

The variety of algebras which replaced the MOLs as the most promising setting for 'quantum logic' are the *orthomodular lattices*, abbreviated OML, introduced by Husimi [**24**]. Although there is a *semigroup coordinatization theorem for OMLs, Foulis [**15**], it seems unlikely that the techniques developed here will yield unsolvability in this variety. But, there are also varieties with reasonable equational bases which capture the Hilbert space examples more tightly than the OMLs. For example, the orthoarguesian identities, [**26**], [**18**], and equations which are related to the existence of states, [**33**], [**32**], describe such varieties. It is not inconceivable that there exists a tractable variety of ortholattices which contains the Hilbert space examples and for which the techniques above can be applied. Unsolvability would then exist in all the varieties between this variety and the modular algebras, and that would be an important negative result. Let me close by listing the two open problems mentioned in this paragraph.

Problem 1. Is the free word problem for MOLs solvable?

Problem 2 (cf. problem 25, [**26**]). Is there a variety of OML's which contains the classical Hilbert space examples and for which a strong enough coordinatization theory exists that the above techniques can be adapted to yield an unsolvable word problem?

Acknowledgements. These results were mainly obtained in the academic year 1985–86 while the author held an N.S.E.R.C. postdoctoral fellowship at TH Darmstadt, West Germany. I would especially like to thank C. Herrmann for many conversations and useful suggestions.

References

1. S. K. Berberian. *Baer *rings*, Grundl. math. Wiss. *195* (Springer, 1972).
2. G. M. Bergman. *Modules over coproducts of rings*, Trans. Amer. Math. Soc. *200* (1974), 1–32.
3. G. Birkhoff, *Lattices in applied mathematics*, in *Lattice theory*, Proceedings of symp. pure math. A.M.S., Providence (1961), 155–184.
4. G. Birkhoff and J. von Neumann, *The logic of quantum mechanics*, Annals of Math. *37* (1936), 823–843.
5. G. Bruns, *Free ortholattices*, Can. J. Math. *28* (1976), 977–985.
6. S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics *78* (Springer-Verlag, 1981).
7. P. M. Cohn, *Skew field constructions*, London Math. Soc. Lecture Note Series *27* (Cambridge University Press, 1977).
8. ——— *Algebra*, vols. 1 and 2, 2nd ed. (Wiley, 1982).
9. ——— *Free rings and their relations*, L.M.S. Monographs *19* (Academic Press, 1985).
10. D. J. Collins, *A simple presentation of a group with unsolvable word problem*, Illinois J. of Math. *30* (1986), 230–234.
11. W. H. Cornish, *Antimorphic action*, Research and Exposition in Mathematics *12* (Heldermann Verlag, Berlin, 1986).
12. P. Crawley and R. P. Dilworth, *Algebraic theory of lattices* (Prentice Hall, 1973).
13. R. A. Day, *Geometrical applications in modular lattices*, in *Universal algebra and lattice theory*, Proceedings, Puebla (1972), 111–141.
14. T. Evans, *Word problems*, Bull. Amer. Math. Soc. *84* (1978), 789–802.
15. D. J. Foulis, *Baer *semigroups*, Proc. Amer. Math. Soc. *11* (1963), 889–894.
16. R. Freese, *Free modular lattices*, Trans. Amer. Math. Soc. *261* (1980), 81–91.
17. G. Grätzer, *Lattice theory* (Freeman, 1971).
18. R. J. Greechie and R. Godowski, *Some equations related to states on orthomodular lattices*, Demonstratio Math. *17* (1984), 241–250.
19. C. Herrmann, *On the word problem for the modular lattice with four free generators*, Math. Ann. *265* (1983), 513–527.
20. ——— *Rahmen un erzeugende quadrupel in modularen verbanden*, Algebra Universalis *14* (1982), 357–387.
21. I. Herstein, *Rings with involution* (Chicago University Press, 1976).
22. S. S. Holland Jr., *The current interest in orthomodular lattices*, in *Trends in lattice theory* (van Nostrand, 1970), 41–126.
23. I. Hughes, *Division rings of fractions for group rings*, Communications in Pure and Applied Mathematics *13* (1970), 181–188.
24. K. Husimi, *Studies on the foundations of quantum mechanics I*, Proc. of the Physicomath. Soc. of Japan *19* (1937), 766–789.
25. G. Hutchinson, *Recursively unsolvable word problems for modular lattices and diagram chasing*, J. Algebra *26* (1973), 385–399.
26. G. Kalmbach, *Orthomodular lattices* (Academic Press, 1983).
27. J. Kotas, *An axiom system for the modular logic*, Studia Logica *21* (1967), 17–38.
28. J. Lewin, *Fields of fractions for group algebras of free groups*, Trans. Amer. Math. Soc. *192* (1974), 339–346.
29. L. Lipshitz, *The undecidability of the word problem for projective geometries and modular lattices*, Trans. Amer. Math. Soc. *193* (1974), 171–180.
30. A. MacIntyre, *The word problem for division rings*, J. Symb. Logic *38* (1973), 428–436.
31. F. Maeda, *Representations of orthocomplemented modular lattices*, J. Sci. Hiroshima Univ. *14* (1950), 93–96.
32. R. Mayet, *Equational bases for some varieties of orthomodular lattices related to states*, Algebra Universalis, preprint.
33. ——— *Varieties of orthomodular lattices related to states*, Algebra Univesalis *20* (1985), 368–396.

34. R. Mayet and M. Roddy, *N-distributivity in ortholattices*, in *Contributions to general algebra 5*, Proceedings of the Salzburg conference, Mai 29 – June 1, 1986 (1987), 285–294.
35. A. Meckler, E. Nelson and S. Shelah, *A variety with solvable, but not uniformly solvable, word problem*, preprint (1987), 1–62.
36. P. Mittlestaedt, *Quantum logic* (Reidel, Dordrecht, 1978).
37. B. H. Neumann, *On ordered division rings*, Trans. Amer. Math. Soc. *66* (1949), 202—252.
38. P. S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov *44* (1955).
39. E. Post, *Recursive unsolvability of a problem of thue*, J. Symb. Logic *12* (1947), 1–11.
40. M. Roddy, *Varieties of modular ortholattices*, Order *3* (1987), 405–426.
41. J. J. Rotman, *Theory of groups*, 3rd ed. (Wm. C. Brown, 1988).
42. L. A. Skornyakov, *Complemented modular lattices and regular rings*, (Oliver and Boyd, 1964).
43. J. von Neumann, *Continuous geometry* (Princeton University Press, 1960).
44. P. M. Whitman, *Free lattices I*, Ann. of Math. *42* (1941), 325–330.

Brandon University,
Brandon, Manitoba