THE ISOMORPHISM PROBLEM FOR SOME CLASSES OF MULTIPLICATIVE SYSTEMS

BY
TREVOR EVANS

1. **Introduction.** We give here a solution of the isomorphism problem for finitely presented algebras in various classes of multiplicative systems. That is, we describe an algorithm for deciding whether two loops (quasigroups, groupoids, inverse property loops, etc.) given by finite sets of generators and defining relations are isomorphic. We give the details only for loops but with trivial changes, the procedure described here applies also to a number of other systems with a non-associative multiplication which have been extensively discussed in the literature.

The basic ideas used are those of an incomplete algebra [2; 4] and of a minimal incomplete algebra [6; 7]. With a finitely presented loop, we associate a finite minimal incomplete loop which freely generates the loop and we prove that two finitely presented loops are isomorphic if and only if the associated finite minimal incomplete loops are isomorphic. In other words, a finitely presented loop has (to within isomorphism) a unique finite minimal incomplete loop, which we call a *basis* of the loop, which freely generates the loop and, furthermore, a basis can be constructed in a finite number of steps from the generators and defining relations of the loop. Clearly, this solves the isomorphism problem for loops.

In §2, we recall from [4] those properties of loops freely generated by incomplete loops needed in the rest of the paper. In §3, the crucial properties of minimal incomplete loops are derived and then used, in §4, to give a solution of the isomorphism property for loops. In the final section, we discuss the changes which have to be made to apply the ideas of this paper to the other multiplicative systems mentioned above. In addition, we obtain some results on the structure of finitely presented loops which follow from the properties of minimal incomplete loops. For example, a finitely presented loop which does not have a free loop as a free factor has only a finite number of automorphisms.

Comparatively little is known about the isomorphism problem for various classes of algebras. It is solvable, of course, for finitely presented abelian groups and recently it has been shown to be unsolvable for finitely presented semigroups and groups. At the time the results of this paper were originally obtained [6], the author felt that similar methods could probably be applied to other varieties of algebras. In particular, it seemed plausible that the isomorphism problem could be solved, using the same ideas, for varieties satisfying the condition that incomplete

Presented to the Society, December 29, 1954, under the title The isomorphism problem for multiplicative systems; received by the editors October 27, 1962.

algebras in the variety can be embedded, and that possibly there might be some underlying result applicable to general varieties of algebras as is the case for the word problem [2;3]. Although the author was unsuccessful in obtaining any general results the solution given here for multiplicative systems may be of interest in view of the recent paper by Gluhov [7], who used the same ideas to obtain a solution of the isomorphism problem for lattices. This gives added weight to the conjecture that the isomorphism problem can be solved for varieties of algebras satisfying the embeddability condition mentioned above or, more generally, that if the word problem is solvable for a variety of algebras, then the isomorphism problem is also solvable for the variety (we refer, of course, to the finitely presented algebras in the variety).

2. **Preliminaries.** We will assume a knowledge of the ideas of [4] and [5] but give, in this section, a brief review of these ideas. A loop is a nonempty set, and three binary operations, multiplication ($\cdot$), left division ($\backslash$), right division ($/$), with respect to which the set is closed. These operations satisfy

$$\begin{aligned} x \cdot (x \backslash y) &= y, \qquad (x/y)\cdot y = x, \\ x \backslash (x \cdot y) &= y, \qquad (x\cdot y)/y = x, \\ x \backslash x &= y/y, \end{aligned}$$

for all x, y.

This definition is equivalent to requiring that there is a two-sided unit with respect to multiplication and that, for all a, b, the equations $au = b$, $va = b$ are uniquely solvable for u, v. In fact, $u = a \backslash b$, $v = b/a$.

An *incomplete loop* is a nonempty set and three partial binary operations $\cdot, \backslash, /$ such that

(i) for any elements x, y, z, if one of $x \cdot y = z$, $x \backslash z = y$, $z/y = x$ holds, then the other two hold also,

(ii) if $\circ$ is any one of the three partial operations, then, for no elements x, y, z, z' do we have $x \circ y = z$, $x \circ y = z'$ with $z \neq z'$,

(iii) there is an element e such that $e \cdot x = x, x \cdot e = x$ hold.

If $x \cdot y = z$, $x \backslash z = y$, $z/y = x$ hold in an incomplete loop, then these three equations will be called a *triple of relations*. A triple $x \cdot e = x$, $x \backslash x = e$, $x/e = x$ or $e \cdot x = x$, $e \backslash x = x$, $x/x = e$ will be called a *trivial triple* of relations. All others are called *nontrivial*.

An incomplete loop can be embedded in a loop [2; 4], and hence can be embedded in the loop it freely generates. A set of generators and relations for a loop which satisfy the conditions for an incomplete loop will be said to be in *tabular form* (this is an improvement over the terminology *closed form* in [2;4]). If L is a finitely presented loop, then it is possible to construct, in a finite number of steps, a set of generators and relations for L in tabular form [2]. That is, we can find an incomplete loop I which freely generates L. We will write L_I for the loop freely

generated by the incomplete loop I. The loop L_I may be characterized among all loops generated by I by the property that any homomorphism of I into a loop K may be extended to a homomorphism of L_I into K.

A constructive definition of L_I is given in [4] in terms of words in the elements of I and the loop operations. The elements of L_I are equivalence classes of such words and each equivalence class contains a unique word of shortest length which may be obtained from every other word in the class by length-shortening applications of the loop axioms and the relations of I.

If I, J are incomplete loops such that every element of J is an element of I and every relation of J is a relation of I, then we will say that J is included in I and write this as $J \subset I$ or $I \supset J$. If $J \subset I$, then there is a homomorphism $L_J \to L_I$ of L_J into L_I. We will say that I is freely generated by J, and write this as $J \prec\!\!\!\cdot\, I$ or $I \succ\!\!\!\cdot\, J$, if $J \subset I$ and if this inclusion mapping induces an isomorphism of L_J onto L_I. The condition $J \prec\!\!\!\cdot\, I$ is equivalent to the requirement that L_J contains an incomplete loop K isomorphic to I such that $J \subset K \subset L_J$. It is also equivalent to the requirement that any homomorphism of J into a loop can be extended to a homomorphism of I into the loop.

We will need later two results from [2] and [4]. The first is a simple extension of Theorem 3 in [2]. Let L_J be freely generated by the finite incomplete loop J and let S be a finite subset of elements of L_J. Then we can construct, in a finite number of steps, a finite incomplete loop I containing J and all the elements of S, such that I freely generates L_J.

The second result we will need is a special case of the normal form theorem in [4]. If L is a loop given by a set I of generators and relations in tabular form (that is, the loop is freely generated by the incomplete loop I), then no two generators of L are equivalent nor is any word $x \circ y$, where x, y are generators and $(\circ)$ is one of the operations, equivalent to a generator z unless the equation $x \circ y = z$ is one of the defining relations in I. Furthermore, no two words $x \circ y, x' * y'$, where x, y, x', y' are in I and $(\circ), (*)$ are loop operations, are equivalent in L unless there are relations $x \circ y = z, x' * y' = z$ in I.

3. **Minimal incomplete loops.** Let I be a finite incomplete loop and let t be any element other than e in I. Let J be the incomplete loop obtained from I by omitting t and all the relations of I in which t occurs. Then $J \subset I$ and the inclusion map determines a homomorphism of L_J into L_I. We will first answer the question: what conditions must t satisfy in order that we have $J \prec\!\!\!\cdot\, I$, that is, that the homomorphism of L_J into L_I is actually an isomorphism of L_J onto L_I?

DEFINITIONS. An element t in I will be called *redundant* in I if it occurs in exactly one nontrivial triple of relations and this triple does not have the form $t \cdot t = u$, $t \backslash u = t$, $u / t = t$. An element of I will be called *essential* in I if it is not redundant in I.

We note that an element t in I is essential if it is e or if it satisfies one of the following conditions:

(i) t occurs in at least two nontrivial triples of relations,

(ii) t occurs in a triple of relations of the form $t \cdot t = u$, $t \backslash u = t$, $u / t = t$,

(iii) t occurs only in trivial triples of relations.

LEMMA 3.1. *$J \prec I$ if and only if the element t is redundant in I.*

Proof. Let t be essential in I. We have three cases to consider.

(i) t occurs in at least two nontrivial triples, say

$$x_1 \circ y_1 = t, \cdots, \cdots, \qquad x_2 * y_2 = t, \cdots, \cdots,$$

where $(\circ)$, $(*)$ are two of the loop operations.

By the normal form theorem in [4], the words $x_1 \circ y_1, x_2 * y_2$ are not equivalent in L_J but in the homomorphism $L_J \to L_I$ induced by the inclusion mapping $J \subset I$, both are mapped onto t. Hence the mapping is not an isomorphism.

(ii) t occurs in a nontrivial triple $t \cdot t = u, \cdots, \cdots,$.

By the normal form theorem in [4], the only elements x in L_J which satisfy $x \cdot x = u$ are generators in J satisfying the relation $x \cdot x = u$ in J. Now, if the inclusion mapping of J into I determines an isomorphism of L_J onto L_I, since no element of J maps on t, the element w of L_J which maps on t in L_I in this isomorphism is not a generator and yet satisfies $w \cdot w = u$, a contradiction.

(iii) t occurs only in trivial triples.

In this case, the inclusion mapping of J into I is properly into, with no element mapping onto t. Hence, this mapping determines an isomorphism of L_J into L_I but not onto L_I.

Now, let t be a redundant element of I. Let $x \circ y = t, \cdots, \cdots,$ be the nontrivial triple of relations in which t occurs. The mapping which replaces by t any component $x \circ y$ of a word in L_J is an isomorphism.

DEFINITIONS. An incomplete loop in which every element is essential will be called a *minimal incomplete* loop. If I, J are incomplete loops with $J \prec I$ and J minimal, then J will be called a *basis* of I. In particular, if a loop L is freely generated by a minimal incomplete loop J, then J will be called a *basis* of L.

LEMMA 3.2. *A finite incomplete loop has a basis.*

LEMMA 3.3. *A finitely presented loop has a basis.*

We may obtain a basis for a finite incomplete loop simply by removing redundant elements one at a time. For a finitely presented loop, we first obtain a finite incomplete loop which freely generates it and then obtain a basis for this incomplete loop.

The next two lemmas will show that not only can we obtain a basis for a finite

incomplete loop by a succession of removals of redundant elements but that every basis of the incomplete loop may be obtained in this way.

LEMMA 3.4. *Let I, J be finite incomplete loops such that $I \succ J$. Then there is a sequence of incomplete loops*

$$I, I_1, I_2, \cdots, J$$

such that each one following I is obtained from the preceding by the removal of a redundant element and the relations in which the element occurs.

Proof. We use induction on the difference between the numbers of elements in I and J. If this is one, let t be the element in I which is not in J. Then, by Lemma 3.1, t is redundant and we have a sequence I, J of the type described in the lemma.

Assume that the statement of the lemma is true for incomplete loops whose numbers of elements differ by n and consider two incomplete loops I, J satisfying the conditions of the lemma with I containing $n+1$ elements more than J.

Now, there must be an element z in I, not in J such that for some elements x, y in J and operation $(\circ)$, I contains the relation $x \circ y = z$. For, if not, then the inclusion mapping of J into I would determine a homomorphism of L_J properly into and not onto L_I. Furthermore, z cannot occur in any other nontrivial relation in I involving only z and elements of J since, if this were so, and z occurred in another triple $x' * y' = z, \cdots, \cdots$, then $x \circ y$, $x' * y'$ would be equivalent in L_I and not in L_J contradicting the assumption that the inclusion mapping of J into I determines an isomorphism of L_J onto L_I.

Thus, the incomplete loop K consisting of J together with the element z and the three triples of relations, $x \circ y = z, \cdots, \cdots, z \cdot e = z, \cdots, \cdots, e \cdot z = z, \cdots, \cdots$, has z as a redundant element. Since the inclusion mapping of J into I determines an isomorphism of L_J onto L_I and since, by the preceding remark, the inclusion mapping of J into K determines an isomorphism of L_J onto L_K, the inclusion mapping of K into I determines an isomorphism of L_K onto L_I.

Now I contains n elements more than K and hence, by our induction hypothesis, there is a sequence of incomplete loops beginning with I and ending with K, of the type described in the lemma. Combining this sequence with the further transition from K to J by the removal of z, we obtain a sequence from I to J.

LEMMA 3.5. *If J is a basis of the finite incomplete loop I, then there is a sequence of incomplete loops*

$$I, I_1, I_2, \cdots, J$$

such that each one following I is obtained from the preceding by the removal of a redundant element.

Proof. This follows immediately from the preceding lemma.

We have now shown that any basis of a finite incomplete loop may be obtained by a sequence of removals of redundant elements. It remains to investigate the connection between different bases of a finite incomplete loop. For lattices, as Gluhov has shown, a finite incomplete lattice has a unique basis. We will now prove that a finite incomplete loop has a unique basis to within isomorphism.

LEMMA 3.6. *Isomorphic finite incomplete loops have isomorphic bases.*

Proof. Let I, I' be finite incomplete loops and let α be an isomorphism of I onto I'. Let J, J' be incomplete loops obtained from I, I', respectively, by omitting in each a redundant element and the relations on which the elements occur. We will show that either J, J' are isomorphic or there is an incomplete loop K contained in I (and its isomorphic image K' under α contained in I') such that there are sequences

$$I \succ J \succ K, \qquad I' \succ J' \succ K',$$

where K is obtained from J by the removal of a redundant element and the relations in which it occurs (and thus K' is obtained from J' by the removal of a redundant element and the relations in which it occurs).

Let J be obtained from I by the removal of the element a and let J' be obtained from I' by the removal of the element b. We have two cases to consider.

Case 1. No relations of I contain both a and $b\alpha^{-1}$. Then $b\alpha^{-1}$ is redundant in J and $a\alpha$ is redundant in J'. Let K be the incomplete loop obtained from J by the removal of $b\alpha^{-1}$ and let K' be the incomplete loop obtained from from J' by the removal of $a\alpha$. We have

$$I \succ J \succ K, \qquad I' \succ J' \succ K',$$

where K' is the isomorphic image of K under α.

Case 2. There is a triple of relations in I containing both a and $b\alpha^{-1}$. Then $b\alpha^{-1}$ does not occur in any nontrivial relation in J and $a\alpha$ does not occur in any nontrivial relation in J'. Hence, the mapping of J onto J' defined as α for all elements of J except $b\alpha^{-1}$ and which maps $b\alpha^{-1}$ in J onto $a\alpha$ in J' is an isomorphism from J to J'.

We now prove the lemma by induction on the number of elements in I. If this number is one or two, then I is minimal and hence is a basis for itself. Assume the theorem true for incomplete loops containing k or fewer elements and let I be an incomplete loop containing $k+1$ elements. Consider two sequences

$$I \succ I_1 \succ I_2 \succ \cdots \succ I_m,$$

$$I' \succ I'_1 \succ I'_2 \succ \cdots \succ I'_n,$$

obtained by successively removing redundant elements, where I_m, I'_n are minimal. If I_1, I'_1 are isomorphic, then since I_1 contains k elements, I_m, I'_n are isomorphic by our induction hypothesis.

If I_1, I_1' are not isomorphic, then there are isomorphic incomplete loops K, K' such that K, K' are obtained from I_1, I_1', respectively, by removal in each of a redundant element and the relations in which it occurs. Now K contains $k-1$ elements. Hence, all bases of K are isomorphic. Similarly, all bases of K' are isomorphic. But any basis of K is a basis of I_1 and since I_1 contains k elements, all of its bases are isomorphic. Hence, every basis of K is isomorphic to I_m. Similarly, every basis of K' is isomorphic to I_n'. We now apply the inductive hypothesis to K, K' and we conclude that, since any bases for them are isomorphic, I_m and I_n' are isomorphic. The lemma now follows by mathematical induction.

LEMMA 3.7. *Let I, J be finite minimal incomplete loops such that $L_I \cong L_J$. Then $I \cong J$.*

Proof. Let $\alpha: L_I \to L_J$ be the isomorphism of L_I onto L_J. Let S be the subset of L_J consisting of the images under α of all elements of I. Let K be an incomplete loop containing J and S which freely generates L_J.

Now $I\alpha$ is a minimal incomplete loop contained in K which freely generates L_J. Hence, $I\alpha$ is a basis of K. But J is also a basis of K. Hence, by Lemma 3.6, J and $I\alpha$ are isomorphic. That is, I and J are isomorphic.

We can sum up the results of the section in the following theorem.

THEOREM. *Two isomorphic finitely presented loops have isomorphic bases.*

An alternative statement would be: Any two bases of a finitely presented loop are isomorphic.

Since for two isomorphic incomplete loops, the loops they freely generate are isomorphic, we can extend the above theorem to the statement that two finitely presented loops are isomorphic if and only if their bases are isomorphic.

4. **The isomorphism problem.** We now describe a method for deciding whether two finitely presented loops are isomorphic. Let L, M be two loops each given by a finite number of generators and relations. By the algorithm described in [2], we first obtain finite incomplete loops I, J such that I freely generates L and J freely generates M. Next, by the removal of redundant elements, we obtain a basis for I and a basis for J. By Lemma 3.7, the loops L, M are isomorphic if and only if these bases are isomorphic. But to test this is a finite procedure since each basis is a finite incomplete loop. Thus, we have the following theorem.

THEOREM. *The isomorphism problem for loops is solvable.*

We remark that it is possible to obtain an upper bound to the number of steps required in testing two finitely presented loops for isomorphism in terms of the number of generators of the loops and the lengths of the defining relations.

5. **Miscellaneous remarks.** Let I be a finite incomplete loop. We have shown that a basis of I is unique to within isomorphism. Now if L_I does not have a free

loop as a free factor, then in obtaining a basis for I by removing redundant elements, Case 2 of Lemma 3.6 cannot occur and so there is actually a unique basis for I, not merely one unique to within isomorphism. Now an automorphism of L_I maps a basis on a basis and if L_I has only one basis and this in addition contains only a finite number of elements, we may conclude L_I has only a finite number of automorphisms. Thus, we have proved the following:

A finitely presented loop which does not have a free loop as a free factor has only a finite number of automorphisms.

Since a free loop has an infinite number of automorphisms, a loop which has a free loop as a free factor has an infinite number of automorphisms and so the restrictions on the loop in the above theorem are quite essential. In [7] Gluhov obtains a similar theorem for finitely presented lattices but without the restrictions on free factors since any finitely presented lattice has a unique basis.

It was shown in [5] that a loop generated by one element which is not free and which satisfies a finite set of relations has only a finite number of endomorphisms. The methods used were quite different from those of this paper but were sufficient to give a solution of the isomorphism problem for finitely related one-generator loops. The author has not verified, but it seems likely, that a finitely presented loop not having a free loop as a free factor has only a finite number of endomorphisms. A closely connected conjecture is that a finitely presented loop cannot be isomorphic to a proper homomorphic image of itself. Higman has shown [8] that this situation can occur for groups. In [5] the author has given an example, based on a similar one of Neumann's for groups [9], of a one-generator infinitely related loop which is isomorphic to a proper homomorphic image of itself.

We have restricted treatment of the isomorphism problem to loops but, as we remarked earlier, the same methods can be applied to a number of other types of multiplicative systems. A *groupoid* is a set closed with respect to a binary operation. A *quasigroup* is a groupoid in which, for any a, b, the equations $au = b, va = b$ have unique solutions. If the axiom $x \backslash x = x/x$ is omitted from the set of axioms for loops given in §2, we obtain a characterization of quasigroups. The modifications required to obtain systems with one-sided division or a one-sided unit are obvious. For all of these systems only trivial changes are necessary in the definitions and proofs in order to obtain a solution of the isomorphism problem.

Systems with rather more structure are obtained if we require the existence of an inverse rather than divisibility operations. An *inverse property loop* is a groupoid in which every element x has an inverse x^{-1} and such that

$$x(x^{-1}y) = y, \qquad (yx^{-1})x = y, \qquad xx^{-1} = y^{-1}y,$$

for all x, y. These axioms imply the existence of a unit and unique solutions $u = a^{-1}b, v = ba^{-1}$ of the equations $au = b, va = b$. Other properties easy to

prove are $(x^{-1})^{-1} = x$, $(xy)^{-1} = y^{-1}x^{-1}$. An *inverse property quasigroup* is a groupoid in which each element x has a left inverse x^L and a right inverse x^R such that

$$x^L(xy) = y, \qquad (yx)x^R = y,$$

for all x, y. Simple consequences of these axioms are

$$(xy)^R = y^L x^L, \quad (xy)^L = y^R x^R, \quad (x^L)^L = x, \quad (x^R)^R = x.$$

The equations $au = b$, $va = b$ have the unique solutions $u = a^L b$, $v = ba^R$.

A *totally symmetric* loop is an inverse property loop in which $x = x^{-1}$. Such a loop is commutative and $xx = 1$, the unit element. A *totally symmetric quasigroup* is an inverse property quasigroup in which $xx = x$. Such a quasigroup is commutative and $x^L = x^R = x$.

The author has verified that, with the appropriate definitions of incomplete algebra, all the normal form theorems obtained for loops in [4] carry over. The only point worth noting is that in the definition of incomplete algebra, it is convenient to require that if x is in the incomplete algebra, then so are the inverses of x. All of the results of this paper then hold with precisely similar proofs and hence the isomorphism problem can be solved for these systems. We refer to Bruck [1] for a general discussion of the properties of these systems.

We conclude with some remarks justifying the conjectures made in the introduction. In [2], the concept of an incomplete algebra is defined for a general variety of abstract algebras given by a finite set of operations and identities. The idea of a redundant element can be introduced by defining an element in an incomplete algebra to be redundant if the inclusion mapping of the incomplete algebra, obtained by removing the element and the relations in which it occurs, into the original incomplete algebra determines an isomorphism of the algebras which the two incomplete algebras freely generate. A minimal incomplete algebra may then be defined as one with no redundant elements. If the word problem can be solved for the variety of algebras, then it is possible, given a finitely presented algebra of the variety, to construct a minimal incomplete algebra which freely generates it. If the even stronger condition is assumed for the variety that incomplete algebras in it can be embedded, then the minimal incomplete algebra constructed will have the property that no two elements in it are equivalent in the algebra it freely generates. From this point on, however, we meet difficulties if we try to follow through the development of §3. In the crucial Lemma 3.6, redundant elements which occur in the same relations give rise to difficulties which the author has been unable to resolve.

References

1. R.H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

2. T. Evans, *The word problem for abstract algebras*, J. London Math. Soc. **26** (1951), 64–71.

3. ———, *Embeddability and the word problem*, J. London Math. Soc. **28** (1953), 76–80.

4. ———, *On multiplicative systems defined by generators and relations.* I. *Normal form theorems*, Proc. Cambridge Philos. Soc. **47** (1951), 637–649.

5. ———, *On multiplicative systems defined by generators and relations.* II. *Monogenic loops*, Proc. Cambridge Philos. Soc. **49** (1953), 579–589.

6. ———, *The isomorphism problem for multiplicative systems*, Bull. Amer. Math. Soc. **61** (1955), 126.

7. M.M. Gluhov, *On the problem of isomorphism of lattices*, Dokl. Akad. Nauk SSSR **132** (1960), 254–256. (Russian) = Soviet Math. Dokl. **1** (1960), 519–522.

8. G. Higman, *A finitely related group with an isomorphic proper factor group*, J. London Math. Soc. **26** (1951), 59–61.

9. B. H. Neumann, *A two-generator group isomorphic to a proper factor group*, J. London Math. Soc. **25** (1950), 247–248.

EMORY UNIVERSITY,
ATLANTA, GEORGIA