VECTOR LOOPS

BY
J. MARSHALL OSBORN

In this paper we shall study commutative diassociative loops with operators from a division ring (a loop is called *diassociative* if any pair of elements generate a subgroup, or associative subloop). Since these loops offer a generalization of the concept of a vector space, we have called them vector loops. The basic result, from which everything else follows, is the setting up of a one-to-one correspondence between classes of vector loops and certain geometrical systems. This correspondence is a generalization of the usual method of coordinatizing a Desarguesian projective plane by triples of elements from a division ring.

This paper constitutes the essence of a doctoral dissertation prepared under the supervision of Professor A. Adrian Albert. The author would like to express his gratitude to Professor Albert for his continued advice and encouragement.

1. Basic definitions and terminology

We begin with a rigorous definition of a vector loop. Let V be a loop, D any division ring, and suppose that the elements of D induce endomorphisms on V satisfying the three axioms:

(a) $(\alpha x + \beta y) + (\gamma x + \delta y) = (\alpha + \gamma)x + (\beta + \delta)y$, *for all* $x, y \in V$, $\alpha, \beta, \gamma, \delta \in D$.
(b) $\alpha(\beta x) = (\alpha\beta)x$ *for all* $x \in V$, $a, \beta \in D$.
(c) $1x = x$, *where* 1 *is the identity element of* D.

Then V will be called a *vector loop* over the division ring D. As in the associative case, we shall call a subloop of V a *subspace* whenever it is closed under multiplication by D, and we shall call an element x of V a *multiple* of an element y of V if there exists a scalar α in D such that $x = \alpha y$. A set $\{x_i\}$ of elements of a vector loop V will be called a *set of representatives of* V if every nonzero element of V is a multiple of one and only one of the x_i's. Also if $\{x_i\}$ is any set of elements in V, we shall define the subspace S *generated* by the set $\{x_i\}$ to be the intersection of the subspaces containing the set (we shall usually use the symbol $\langle x_i \rangle$ to denote the subspace generated by the set $\{x_i\}$). Whenever no proper subset of the set $\{x_i\}$ generates S, we shall say that $\{x_i\}$ is a *strongly independent* (or just independent) set. If an ordered set $\{x_i\}$ of elements of V satisfies the condition that for no finite subset $x_{i_1}, \cdots, x_{i_n}$ (arranged in ascending order) of $\{x_i\}$ do there exist scalars $\alpha_1, \cdots, \alpha_n$, not all zero, such that $(\cdots ((\alpha_1 x_{i_1} + \alpha_2 x_{i_2}) + \alpha_3 x_{i_3}) \cdots + \alpha_n x_{i_n}) = 0$, then

Received February 22, 1959; received in revised form December 24, 1960.

the set $\{x_i\}$ will be called *weakly independent*. We now define the *upper dimension* of a vector loop to be the maximum number of elements occurring in a weakly independent set, and the *lower dimension* to be the minimum number of elements occurring in a maximal independent set. In those special cases where the upper and lower dimensions are equal, we shall speak simply of the dimension.

The other concept that we would like to define in this section concerns the geometrical systems referred to at the beginning of this paper. Since these systems include all projective and affine geometries as the most important special cases, we shall call them simply geometries. More specifically, we define a *geometry of order c* to be a set of points, lines, and incidence relations between them, satisfying the axioms:

(i) *Any two distinct points determine precisely one line.*
(ii) *The cardinality of points on each line is* $c + 1$.

By a *subgeometry* of a geometry G of order c, we shall mean a subset of the points and lines of G, under the same incidence relations, which themselves form a geometry of order c. And finally, a subset of points $\{p_i\}$ of G will be said to generate a subgeometry H of G if H is the intersection of all subgeometries containing the set $\{p_i\}$.

2. The connection between vector loops and geometries

Let V be a vector loop over a division ring D of cardinality c. Then any element of V that is not the identity generates a subspace of dimension one, and any two such subspaces are either identical or have only the identity in common. Also, if x and y are two independent elements of V, then the set of all elements of the form $\alpha x + \beta y$ is a two-dimensional vector space $\langle x, y\rangle$ over D (by axiom (a)) containing x and y. From vector space theory it is clear that any two independent elements in $\langle x, y\rangle$ will generate it, and that $\langle x, y\rangle$ is a set-theoretic sum of $c + 1$ disjoint one-dimensional subspaces of V.

Now, let G consist of a set of points in one-to-one correspondence with the one-dimensional subspaces of V, a set of lines in one-to-one correspondence with the two-dimensional subspaces of V, and the incidence relations that a given point is on a given line if and only if the subspace corresponding to the point is contained in the subspace corresponding to the line. Then it is clear from the above remarks that G is a geometry of order c. Furthermore, the elements of G corresponding to any subspace of V form a subgeometry of G, and every subgeometry of G corresponds to a unique subspace of V in this way. Since this correspondence preserves inclusion relations, G may be regarded as being the lattice of subspaces of V.

Conversely, given a geometry G of order c and a division ring D of cardinality c, we shall construct a vector loop over D which has a lattice of subspaces isomorphic to G. Consider first the set of pairs (P, α) where P ranges over the points of G, and α ranges over the elements of D. Identifying all

pairs of the form $(P, 0)$ where 0 is the zero element of D, we denote the resulting set by V. The operation of D upon V may now be defined by the relation $\beta(P, \alpha) = (P, \beta\alpha)$, from which the validity of axioms (b) and (c) follows immediately. Now, let H be a two-dimensional vector space over D, and let the set $\{y_j\}$ be a set of representatives of H. Then for each line l of G, we set up a one-to-one correspondence between the set $\{y_j\}$ and the set of symbols of the form $(P, 1)$ where P ranges over the points of l and where 1 is the identitiy element of D. This induces the correspondence $(P, \alpha) \leftrightarrow \alpha y_i$, where y_i is the representative corresponding to P. We now define addition between these (P, α)'s to be that induced by the operation of vector addition between the corresponding elements of H.

If P and P' are distinct points of G, then they lie on exactly one line of G, so that we have uniquely defined the sum $(P, \alpha) + (P', \beta)$ for any α, β in D. On the other hand, the sum $(P, \alpha) + (P, \beta)$ has been defined once for each line passing through P; but in each case the definition yields $(P, \alpha) + (P, \beta) = (P, \alpha + \beta)$. Hence, addition in V is well-defined. To show that V is a loop, and that it satisfies axiom (a), it is only necessary to remark that by construction, any two elements of V can be imbedded in a subsystem which is a two-dimensional vector space over D. Thus, given a geometry of order c and a division ring D of cardinality c, we have shown how to construct from them a vector loop over D, and there remains only the question of how this construction is related to the previous construction of a geometry from a vector loop.

Given a geometry G of order c and a division ring D of cardinality c, let V be a loop constructed from it by the method just described, and let G' be the geometry associated with V at the beginning of this section. We would like to show that G and G' are isomorphic (i.e., that there is a one-to-one correspondence between the points and lines preserving incidence). Given any point P of G, the set of pairs (P, α) with the given point P as first argument (and α ranging over D) form a one-dimensional subspace of V, and thus determine a unique point P' of G'. This sets up a map from the points of G to the points of G' which is clearly one-to-one and onto. Also, if a set of points of G form a line l, then the pairs (P, α) where P ranges over the points of l, form a two-dimensional subspace of V, and hence determine a line of G'. But every line of G' must arise in this manner, since given two points of G', the unique line joining them will arise as the image of the line joining the two corresponding points of G. Thus, G and G' are isomorphic. We have shown that, given a division ring D of cardinality c, every geometry of order c arises as the lattice of subspaces of some vector loop over D, and we have given a concrete construction for such a loop.

Next, let V be a vector loop over D, G its associated geometry, and V' a vector loop over D constructed from G. We would like to discover how V' is related to V. Because of the wide latitude available in the setting up of addition in V' (we made use of any one-to-one correspondence between the

set of representatives of H and certain subsets of V'), we can certainly not expect V and V' to be isomorphic. However, there is a concept a little more general than isomorphism which does relate V and V'. Define two vector loops W and W' over the same division ring D to be *similar* if there is a one-to-one mapping f of W onto W' satisfying the axioms:

(1) $f(\alpha x) = \alpha f(x)$ *for any* $x \in W$, $\alpha \in D$.

(2) *For every* x *and* y *of* W, *there exist scalars* α *and* β *of* D *such that* $f(x + y) = \alpha f(x) + \beta f(y)$.

It is clear that the relation of being similar is an equivalence relation, and that similar vector loops have the same geometry associated with them. To show that V and V' are similar, let $\{x_i\}$ be a set of representatives of V, and let P_i be the point of G corresponding to x_i for each i. Then we may define a one-to-one map of V onto V' satisfying (1) by letting $f(\alpha x_i) = (P_i, \alpha)$ for each i and every $\alpha \in F$. To show that f satisfies axiom (2), we remark that the point of G corresponding to $x + y$ is on the line determined by the points of G corresponding to x and y, and hence $f(x + y)$ is in the two-dimensional subspace of V' determined by $f(x)$ and $f(y)$.

We have now finally proved

THEOREM 1. *For every division ring* D *of cardinality* c, *there is a one-to-one correspondence between similarity classes of vector loops over* D *and geometries of order* c. *Under this correspondence, the geometry corresponding to a vector loop is isomorphic to the lattice of subspaces of that loop (points corresponding to one-dimensional subspaces, lines to two-dimensional subspaces, etc., and inclusion relations being preserved).*

Because of the connection between vector loops and geometries given in Theorem 1, we shall sometimes find it convenient to use the same notation to denote subspaces of a loop as to denote the subgeometries corresponding to them. For example, if $x_1, \cdots, x_n$ are elements of a vector loop, $\langle x_1, \cdots, x_n \rangle$ may denote either the subspace that they generate or the subgeometry corresponding to it.

To make the concept of the similarity of vector loops clearer, we will now give an example. Let V be the abelian group of order p^3 and type (1, 1, 1) on the generators a, b, c (with operators from the field of p elements). Then every element of V can be expressed uniquely in the form $(ia + jb) + kc$, where $0 \leqq i, j, k \leqq p - 1$. Consider the subgroup K generated by a and $b + c$, consisting of the elements $(ia + jb) + jc$, where $0 \leqq i, j \leqq p - 1$. We may define a new operation of addition "$\oplus$" between the elements of K by defining

$$ia \oplus [(ka + mb) + mc] = [(ka + mb) + mc] \oplus ia = [(k - i)a + mb] + mc$$

for $m \neq 0$, and for i and k arbitrary, and

$$[(ia + jb) + jc] \oplus [(ka + mb) + mc] = [(i + k)a + (j + m)b] + (j + m)c$$

for j and m either both nonzero or both zero, and for i and k arbitrary. It is easy to verify that K is commutative and associative under "$\oplus$". We now extend our definition of "$\oplus$" to all of V by defining the new sum of any two elements that are not both in K to be the same as the old sum. Under this new operation V will still be a vector loop, but it will not be associative for $p \neq 2$. Since setting $a = 0$ in V under the new operation will still induce a homomorphism into an abelian group of order p^2, we have proved the case $n = 3$ of

THEOREM 2. *For $p \neq 2$, $n \geqq 3$, there exists a solvable vector loop over the field of p elements which has p^n elements and which is similar to the abelian group of order p^n and type $(1, \cdots, 1)$, but which is not associative.*

As suggested by group theory, we shall call a loop *solvable* if it has a factor series all of whose elements are abelian groups.

For $n > 3$, the theorem may be proved by taking the direct sum of the vector loop of order p^3 constructed above and an abelian group of order p^{n-3} and type $(1, \cdots, 1)$.

3. Existence theorems

In this section we shall develop some of the consequences of Theorem 1, with particular emphasis on exhibiting several different types of examples of vector loops. We begin with the comment that any projective geometry is a geometry under our definition, so that Theorem 1 implies that any projective plane of prime power or infinite order (which includes all known examples) will arise from a vector loop of dimension three. Any vector loop derived from a Desarguesian plane using the division ring which coordinatizes that plane, will be similar to an abelian group. However, if we use another division ring of the same cardinality, or if we use a non-Desarguesian plane with any division ring of the right cardinality, a new class of vector loops will result. This "coordinatization" of a projective plane by means of a vector loop looks as if it might be useful in the study of finite non-Desarguesian projective planes.

For vector loops derived from projective spaces, it is clear that the upper and lower dimensions are equal. That these are, in fact, the only finitely generated vector loops with this property, shows how strong this dimension property is, and gives a convenient characterization of these loops:

THEOREM 3. *A vector loop of dimension $n \geqq 3$ has a projective space of dimension $n - 1$ as its associated geometry.*

Using the remarks at the beginning of this section, we see that Theorem 3 has the following

COROLLARY. *There exist vector loops of any finite dimension over any infinite division ring which are not similar to vector spaces.*

We shall begin the proof of Theorem 3 by showing that a vector loop V of dimension three has a projective plane as its associated geometry G. Since D

has at least two elements, every line of G has at least three points on it, and it only remains to prove that any two lines of G intersect. Assume that there exist two lines of G which do not intersect, and let the two-dimensional subspaces of V corresponding to them be $\langle x, y\rangle$ and $\langle z, w\rangle$. Since V has dimension three, and since x, y, z are independent, we can write w in the form $(\alpha x + \beta y) + \gamma z$ for some α, β, γ, in D. But then the point corresponding to the subspace generated by $(\alpha x + \beta y) = (-\gamma)z + w$ is on both lines, contrary to hypothesis.

If V has dimension $n > 3$, we shall reduce the proof of the theorem to the case already proved. One of the usual sets of axioms for a projective space is the following:

(1) *There exists a unique line joining any two points.*
(2) *If any quadrilateral A, B, C, D has the property that the lines AB and CD intersect, then AC and BD intersect.*
(3) *There exists a quadrilateral.*
(4) *There are at least three points on every line.*

Now, axioms (1) and (3) are already satisfied, and axiom (4) follows as before, so that we need only prove (2). Let $\langle x\rangle$, $\langle y\rangle$, $\langle z\rangle$, $\langle w\rangle$ be any four points of G satisfying the property that $\langle x, y\rangle$ and $\langle z, w\rangle$ intersect in a point $\langle t\rangle$; then $t = \alpha x + \beta y = \gamma z + \delta w$ for some $\alpha, \beta, \gamma, \delta$, in D. If neither α nor γ are zero (otherwise switch the roles of x and y, or z and w), then the whole configuration is in $\langle x, z, t\rangle$. But $\langle x, z, t\rangle$ is a projective geometry by the first part of the proof, so that $\langle x, z\rangle$ and $\langle y, w\rangle$ must intersect. It is now trivial to verify that the dimension is correct, to finish the proof.

Another well-known class of geometrical objects fitting our definition of a geometry is that of the affine geometries. From Theorem 3 we know that a vector loop derived from an affine geometry has no dimension, and in §4 we shall see that a vector loop derived from a finite affine geometry never has prime power order. But perhaps the most interesting property of this class of examples is stated in

THEOREM 4. *A vector loop with an affine space as its associated geometry, is simple (i.e., has no normal subspaces).*

Let $\rho(y)$ be the mapping of V onto itself given by $x\rho(y) = x + y$. Then if x and x' are two elements of a vector loop V, we shall call x' a conjugate of x if x' is the image of x under a product of a finite number of mappings of V of the form $\rho(y)\rho(z)\rho^{-1}(y + z)$ or their inverses. We may now state a lemma which contains the gist of the proof of Theorem 4.

LEMMA 1. *If V' is a vector loop with an affine plane G as its associated geometry, and if x and w are independent elements of V', then x has a conjugate not in $\langle x, w\rangle$.*

Let $\langle y\rangle$ be any point of G not on the line $\langle x, w\rangle$; then the point $\langle x + y\rangle$ is also not on $\langle x, w\rangle$. Next, choose a point $\langle z\rangle$ which is distinct from $\langle y\rangle$ and

which has the property that the lines $\langle y, z\rangle$ and $\langle x, w\rangle$ are parallel. Then the line $\langle x + y, z\rangle$ must intersect $\langle x, w\rangle$, so that there exists a multiple αz of z with the property that $(x + y) + \alpha z$ is in $\langle x, w\rangle$. But $-(y + \alpha z)$ cannot be in $\langle x, w\rangle$ since $\langle y, z\rangle$ is parallel to $\langle x, w\rangle$, so that the conjugate

$$[(x + y) + \alpha z] - (y + \alpha z)$$

of x is not in $\langle x, w\rangle$.

Using this lemma it is now easy to prove Theorem 4. If V is a vector loop with an affine space as its associated geometry, it is sufficient to prove that given any two independent elements x and y of V, any normal subspace containing x contains y. We now let V' be any subspace of V on three generators which contains x and y. Since the subgeometry corresponding to V' is an affine plane, we may apply Lemma 1 (with any w in V' independent of x) to get a conjugate x' of x which is independent of x and in V'. Using the lemma again, this time with $w = x'$, yields a second conjugate x'' which is in V' but not in $\langle x, x'\rangle$. But then x, x', x'' must generate all of V'. Thus, a normal subspace containing x must contain all of V', and hence also the element y.

Since there exist affine spaces of any infinite order, Theorem 4 has the following

COROLLARY. *There exist simple vector loops on any number of generators over any infinite division ring.*

A third class of examples of vector loops arises from the two classes already discussed by applying various combinations of the two operations of taking direct sums and performing similarity transformations. One of the interesting features of this class of examples is illustrated by

THEOREM 5. *Let V and W be nontrivial vector loops over a division ring D, and let their direct sum $V \oplus W$ have finite dimension n; then V and W are vector spaces.*

Let $x_1, x_2, \cdots, x_i$ and $y_1, y_2, \cdots, y_j$ be maximal length weakly independent sequences in V and W respectively; then the union of these sequences is a weakly independent sequence in $V \oplus W$, implying that $i + j \leqq n$. On the other hand, if $x_1', x_2', \cdots, x_k'$ and $y_1', \cdots, y_m'$ are minimal generating sets for V and W respectively, then the union of these sets generates $V \oplus W$, giving $k + m \geqq n$. But since $k \leqq i$ and $m \leqq j$, we must have $i + j \leqq n \leqq k + m \leqq i + j$, or $i = k$ and $j = m$. Therefore, V and W will both have dimensions, and these dimensions are i and j respectively. Then any weakly independent sequence of V can be completed to a generating set of i elements, and similarly for W.

Now, assume that the theorem is not true; then we can find three elements in one of the two summands, say x_1, x_2, x_3, in V, which do not associate. Using the fact that the property of having a dimension is hereditary, we see that the conjugate $x_1' = x_1\rho(x_2)\rho(x_3)\rho^{-1}(x_2 + x_3)$ of x_1, which is in the

subspace generated by x_1, x_2, x_3, must satisfy the equation

$$x' = \alpha x_1 + (\beta x_2 + \gamma x_3)$$

for some α, β, γ, in D. Completing the set x_1, x_2, x_3 to a generating set $x_1, \cdots, x_i$ of V, and selecting any generating set $y_1, \cdots, y_j$ of W, we consider the set

$$(x_1, y_1), (x_2, 1), \cdots, (x_i, 1), (1, y_2), \cdots, (1, y_j)$$

of $n - 1$ elements of $V \oplus W$. Since $V \oplus W$ has dimension n, the subspace M generated by this set cannot be all of $V \oplus W$. If we add the element $(x_1, 1)$ to the $n - 1$ generators for M given above, we can clearly generate all of $V \oplus W$, so that $(x_1, 1)$ is not in M. But M contains the element

$$(x_1, y_1)\rho[(x_2, 1)]\rho[(x_3, 1)]\rho^{-1}[(x_2, 1) + (x_3, 1)] \cdot \rho^{-1}[(\beta x_2, 1) + (\gamma x_3, 1)]\rho^{-1}[(x_1, y_1)] = ((\alpha - 1)x_1, 1).$$

Therefore $\alpha = 1$, and $(\beta x_2 + \gamma x_3)$ is not unity. Say $\beta \neq 0$. Then consider the slightly modified set

$$(x_1, y_1), (x_2, y_1), (x_3, 1), \cdots, (x_i, 1), (1, y_2), \cdots, (1, y_j)$$

of $n - 1$ elements of $V \oplus W$. Arguing as before, we see that the subspace M' generated by these $n - 1$ elements cannot contain the element $(x_2, 1)$. But since

$$(x_1, y_1)\rho[(x_2, y_1)]\rho[(x_3, 1)]\rho^{-1}[(x_2, y_1) + (x_3, 1)] \cdot \rho^{-1}[(x_1, y_1)]\rho^{-1}[(\gamma x_3, 1)] = (\beta x_2, 1),$$

M contains $(x_2, 1)$. This contradiction proves the theorem.

As this theorem illustrates, the lower dimension of a direct sum is usually less than the sum of the lower dimensions of the summands. This fact enables us to create vector loops with many different combinations of upper and lower dimensions by performing different direct sums. For example, by taking the direct sum of a nonassociative vector loop of dimension n and a one-dimensional vector space, we obtain the class of vector loops described in the following

COROLLARY. *For any integer $n \geqq 3$ and for any division ring D, there exists a vector loop over D with lower dimension n and upper dimension $n + 1$.*

4. Finite vector loops

A vector loop will be called *finite* if it has finitely many elements. Similarly, a geometry will be called *finite* if it has only a finite number of points. In this section we shall consider the existence and possible orders of finite vector loops.

First, let G be a geometry satisfying the axiom

(iii) *There exist three lines, each with more than two points on it.*

Then we shall call G *nontrivial*. The only trivial geometries of order c are the geometry consisting of a single point and the geometry consisting of a single line with $c + 1$ points on it. Given a division ring D of cardinality c, these correspond respectively to a one-dimensional and a two-dimensional vector space over D, which we shall call the trivial vector loops over D.

THEOREM 6. *An alternative set of axioms for a nontrivial finite geometry of order n may be obtained by replacing axiom* (ii) *by*

(ii′) *There exists a nonnegative integer k satisfying the property that, given any line and point not on it, there are precisely k lines through the given point not intersecting the given line.*

If m is the number of points of G, then $m = n^2 + (k + 1)n + 1$, *and* $n + 1$ *divides* $k(k - 1)$.

Let G be a nontrivial finite geometry of order n with m points; then it is easy to see that every point has $(m - 1)/n$ lines through it, and that $(m - 1)/n - (n + 1)$ of these will not intersect a given line not through the given point. But since this quantity does not depend on which line and point we choose, we have satisfied axiom (ii′) with $k = (m - 1)/n - (n + 1)$. Solving this equation for m gives $m = n^2 + (k + 1)n + 1$, and substituting this into $m(m - 1)/(n + 1)n$ (which represents the total number of lines in the geometry) readily yields the condition that $n + 1$ divides $k(k - 1)$, by using the fact that the total number of lines must be an integer.

Conversely, if G satisfies (i), (ii′), and (iii), then take two distinct lines t_1, t_2 which intersect, and by (iii) we can find a point P not on t_1 or t_2. If P has s lines through it, then $s - k$ of them must intersect t_1. Hence, t_1 has $s - k$ points on it, and similarly t_2 also has $s - k$ points. This shows that any two intersecting lines have the same number of points. But by (i) any two lines intersect a common line, and the theorem is proved.

Now, if a vector loop V over $GF(q)$ has t elements, then the associated finite geometry G must have $(t - 1)/(q - 1)$ points, since each point of G corresponds to $q - 1$ elements of V (not counting the identity element). By Theorem 6, $(t - 1)/(q - 1) = q^2 + (k + 1)q + 1$, giving $t = q^3 + k(q^2 - q)$. This gives us a restatement of the second half of Theorem 6 in terms of loops.

THEOREM 7. *The order of a finite nontrivial vector loop over* $GF(q)$ *is of the form* $q^3 + k(q^2 - q)$ *for some nonnegative integer k satisfying the property that* $k(k - 1)$ *is divisible by* $q + 1$; *this number k is the same as the k in axiom* (ii′) *for the geometry associated with this loop.*

COROLLARY 1. *The order of any finite vector loop over* $GF(q)$ *is divisible by q.*

Since the order of a vector loop V which is not simple is equal to the order of the image of V under any (operator) homomorphism times the order of the kernel of that homomorph, we also have

COROLLARY 2. *If the order of a vector loop V over $GF(q)$ is not divisible by q^2, then V is simple.*

If $k = 0$ in a nontrivial finite geometry G, then any two lines must intersect, and G is a projective plane. If $k = 1$, the lines not intersecting a given line l do not intersect each other, since otherwise a point of intersection would have two lines through it not intersecting l. On the other hand, every point of G must have a line through it not intersecting l. Therefore the lines of G fall into equivalence classes of parallel lines, and G is an affine plane (although G is a geometry of order n by our definition, it will be an affine plane of order $n + 1$ by the usual definition). If $k \geqq 2$, then the condition $n + 1$ divides $k(k - 1)$ is no longer automatically satisfied, and in fact, it is clear that there can be only a finite number of different finite geometries with any given value of k.

This discussion tells us that a projective plane of order q is always associated with a vector loop of order q^3, and an affine plane of order $q + 1$ with a vector loop of order $q^3 + q^2 - q$. A vector loop over $GF(q)$ of order $q^3 + q^2 - q$ will be simple, as can be seen by Theorem 4 or Corollary 2 of Theorem 7. Stated formally,

THEOREM 8. *There exists a simple vector loop over $GF(q)$ of order $q^3 + q^2 - q$ if, and only if, there exists a projective plane of order $q + 1$.*

Now, a projective plane of order $q + 1$ will certainly exist whenever $q + 1$ is a power of a prime, and this will occur if and only if q is one of the following: a prime of the form $2^r - 1$, a power of two which is one less than a prime, or the number 8. Using this, and the theorem of Bruck and Ryser on the nonexistence of projective planes of certain order [Canadian J. Math., vol. 1 (1949), pp. 88–93], we immediately obtain the following

COROLLARY. *Vector loops over $GF(q)$ of order $q^3 + q^2 - q$ exist for $q = 2$, 3, 4, 7, 8, 31, 127, $\cdots$, and such loops do not exist for $q = 5$, 11, 13, 17, 23, 29, 37, $\cdots$.*

From this corollary, it is clear that the question of the existence of a finite vector loop of a given order is not easy to settle in general, and that it depends very much upon which finite field is involved. When $q + 1$ is a power of a prime, we can conclude the existence of an infinite class of simple finite vector loops over $GF(q)$ from Theorem 4, using the n-dimensional affine geometries ($n = 2, 3, \cdots$) over $GF(q + 1)$.

THEOREM 9. *Whenever $q + 1$ is a power of a prime, there exists a denumerable class of simple vector loops over $GF(q)$, the order of the $(n - 2)^{\text{nd}}$ one being $\sum_{i=1}^{n} \binom{n}{i}((2i - n)/i)q^i$.*

The only part of this theorem that has not already been proved is that a vector loop associated with an affine space of $n - 1$ dimensions will have the order given here. The calculation is straightforward and hence will be omitted.

Since the coefficient of q in this summation is $\binom{n}{1}(2-n)/n = 2-n$, the summation will be divisible by q^2 if and only if $n \equiv 2 \pmod{q}$. On the one hand, this means that most of these loops could have been proved simple by using Corollary 2 of Theorem 7; on the other hand, we get the following result.

COROLLARY. *There exist simple vector loops over $GF(q)$ divisible by q^2, and with the property that all similar loops are also simple.*

There are two other consequences of the last section that should be mentioned here. First of all, since finite projective spaces of dimension greater than or equal to three are Desarguesian, and hence unique, we can strengthen Theorem 3 in the special case of finite vector loops.

THEOREM 10. *A vector loop over $GF(p^m)$ of order p^{mn} $(n > 3)$, is similar to the abelian group of type $(1, \cdots, 1)$ and order p^{mn} if and only if it cannot be generated over $GF(p^m)$ by less than n elements. This assertion is valid for $n = 3$ if and only if it is true that there exists no non-Desarguesian plane of order p^m.*

Using Theorem 5, we immediately get the following

COROLLARY. *For $n \geqq 4$ and for all $q \neq 2$ there exist vector loops over $GF(q)$ of order q^n which are not similar to abelian groups.*

5. Simple vector loops of order q^n

The examples of finite simple vector loops that have been given so far have existed only over certain finite fields, and have had orders only divisible by a low power of q. Furthermore, these examples have had the property that the whole similarity class was simple. In this section we shall construct a class of simple vector loops which exist over all finite fields of odd order, and which are similar to vector spaces.

THEOREM 11. *Given any finite field $GF(q)$ of odd order, and any integer $n \geqq 3$, there exists a simple vector loop over $GF(q)$ of order q^n which is similar to an n-dimensional vector space over $GF(q)$.*

To construct this vector loop, we shall start with an $(n-1)$-dimensional projective space G over $F = GF(q)$, and construct a vector loop from it by the method used in the proof of Theorem 1. We may represent the points of G as that subset of n-tuples of elements from F with the property that the first nonzero element occurring is 1. If p is the prime which divides q, let O' be any ordering of the elements of F which puts the elements of the prime subfield of F first, and which puts them in the order $0, 1, \cdots, p-1$. Then O' induces an order O on the points of G by using the lexicographical ordering on the n-tuples which represent them.

Next, let H be a two-dimensional vector space over F, and let b and c be two independent elements of H. Then the element c and the set of elements of the form $b + \alpha c$ $(\alpha \in F)$, together form a set of representatives of H over F.

We order this set of representatives in any way which places the elements b, c, $b + c$, $b + 2c$, $\cdots$, $b + (p - 1)c$ first, and in this order. Having ordered the points of G and having selected an ordered set of representatives of H over F, we may construct the desired vector loop V over F by the method used in the proof of Theorem 1 by requiring that the one-to-one correspondence between the points on a line of G and the set of representatives of H must always be the unique order-preserving correspondence between these two sets.

To prove that V is simple over F, let V' be the subspace of V corresponding to the hyperplane of G whose points are represented by n-tuples starting with zero. Let us consider first the case $n = 3$, $p > 3$. We shall show first that every element in V' except one is conjugate to another element in V' not a multiple of it.

Let x_α, y, z be the representatives in V corresponding to the points $(0, 1, \alpha)$, $(1, 0, 1)$, $(1, 0, 2)$ of G respectively, and let us compute the value of the conjugate $x_\alpha \rho(y)\rho(z)\rho^{-1}(y + z)$ of x_α. Since $(0, 1, \alpha)$ and $(1, 0, 1)$ are the first two points on the line of G which they determine, x_α and y must correspond to b and c in H under the definition of addition in the subspace $\langle x_\alpha, y\rangle$. And since $b + c$ is the third representative of H, $x_\alpha + y$ must be the representative of the third point of this line, or $(1, 1, \alpha + 1)$. Similarly, we see that $(x_\alpha + y) + z$ is the representative of the point $(1, 2, 2\alpha)$, using the calculation $(b + c) + c = b + 2c$ in H. To find $y + z$, we observe that

$$(b + c) + (b + 2c) = 2b + 3c = 2(b + \tfrac{3}{2}c),$$

so that $y + z$ is twice the representative of the point $(1, 0, \frac{3}{2})$. In the same way, we compute that $x_\beta + (y + z)$ is the representative of the point $(1, 2, 2\beta + \frac{3}{2})$, and $(x_\alpha + y) + z$ and $x_\beta + (y + z)$ will be equal if they represent the same point, or if $2\beta + \frac{3}{2} = 2\alpha$. Therefore, choosing $\beta = \alpha - \frac{3}{4}$, we have $x_\alpha \rho(y)\rho(z)\rho^{-1}(y + z) = x_\beta$.

Now, if V is not simple, it contains a two-dimensional normal subspace W which has a nonzero element x in common with V', since any two subspaces of dimension two intersect nontrivially. And if x does not correspond to the point $(0, 0, 1)$, the calculation in the last paragraph shows that W contains a second element of V' not a multiple of x, implying that $W = V'$. Hence, the proof of simplicity for the case $n = 3$, $p > 3$ will be complete if we show that there is no proper normal subspace containing the representative of the point $(0, 0, 1)$.

Let x, u, w be the representatives in V of the points $(0, 0, 1)$, $(1, 0, 0)$, and $(1, 1, 0)$ respectively. Using the same method as above, we compute easily that $(x + u) + w = y + w$ is the representative of the point $(1, 2, p - 1)$, and that $u + w$ is the representative of $(1, 2, 0)$. Then

$$x\rho(u)\rho(w)\rho^{-1}(u + w) = [(x + u) + w]\rho^{-1}(u + w)$$

is seen to be the representative of the point $(1, 2, p - 2)$. Similarly, letting v be the representative of $(1, 2, 0)$, we have that $(x + u) + v = y + v$ is the

representative of $(1, 3, (p-1)/2)$, and that $u+v$ is the representative of $(1, 3, 0)$. Hence, $x\rho(u)\rho(v)\rho^{-1}(u+v)$ is the representative of $(1, 3, (p-3)/2)$. But x and the two conjugates of it exhibited here generate all of V, finishing the proof for the case $n = 3$, $p > 3$.

For the case $n = 3$, $p = 3$, let x_α, y, z be the representatives in V of the points $(0, 1, \alpha)$, $(1, 0, 0)$, $(1, 0, 1)$ respectively. Then we may compute in the same manner as above that $x_\alpha \rho(y)\rho(z)\rho^{-1}(y+z)$ is the representative of the point $(1, 1, \alpha - 1)$. Also, letting x_β, u, v be the representatives of $(0, 1, \beta)$, $(1, 2, 0)$, $(1, 2, 1)$ respectively, we get that $x_\beta \rho(u)\rho(v)\rho^{-1}(u+v)$ is twice the representative of $(1, 1, -\beta - 1)$. Taking $\beta = -\alpha$, it is clear that any normal subloop containing x_α also contains x_β. Finally, if s, t, w, y are the representatives of the points $(0, 1, 0)$, $(0, 0, 1)$, $(0, 1, 1)$, $(1, 0, 0)$ respectively, we compute that $t\rho(w)\rho(y)\rho^{-1}(w+y) = s$. We have shown that if any point of V' is in a normal subspace W of V, then some other point of V' not a multiple of it is also in W. Hence, V' is the only two-dimensional subspace which could be normal. However, we have also shown above that x_α has a conjugate not in V', so it is not normal either, finishing this case.

If $n > 3$, we may assume by induction that V' is simple. Letting W be any proper normal subspace of V, we have that $W \cap V'$ is normal in V', and hence that W is either equal to V' or is a one-dimensional subspace not included in V'. In the latter case, let U be the three-dimensional subspace generated by W and by the one-dimensional subspaces corresponding to the first two points of G. Then U is isomorphic to the vector loop proved simple by the first part of the proof (since the two geometries are order isomorphic), contrary to the fact that W is a normal subspace of U. On the other hand, if V' is normal in V, then let U be the three-dimensional subspace generated by the one-dimensional subspaces corresponding to the first two points of G and the last point of G. Again U is isomorphic to the vector loop proved simple by the first part of the proof, and again we have a contradiction, since $V' \cap U$ is a proper normal subspace of U.

6. Totally symmetric loops and alternating quasigroups

A *totally symmetric* loop has been defined by Bruck [2] as a loop whose elements satisfy the axioms (1) $ab = ba$, and (2) $ab \cdot a = b$. It is clear from (2) that all elements except the identity are of order two, and from both axioms that any two elements generate a subloop isomorphic to the (Klein) four group. This loop is then a vector loop over the field of two elements. Conversely, a vector loop over $GF(2)$ satisfies (1) and (2), so the two notions are equivalent. These systems also turn out to be equivalent to a special case of the "tactical configurations" considered by Carmichael [4], and fifty years before him these systems were considered by several more people under the name of "the schoolgirl problem". These investigators supply many examples and constructions, but unfortunately, none of their constructions seem to generalize to vector loops over fields other than $GF(2)$. However, the type

of approach used by these investigators has suggested to us a construction for vector loops over $GF(3)$ which makes use of objects which we have chosen to call alternating quasigroups.

Let us define an *alternating quasigroup* to be a quasigroup Q satisfying the two axioms: (i) $ab \cdot a = b$, for all a, b in Q, and (ii) $a \cdot ab = ba$, for all a, b in Q. An alternating quasigroup is idempotent, since $a^2 = a \cdot a^2 = a(a \cdot a^2) = a^2 \cdot a$ using only (ii), and $a^2 \cdot a = a$ by (i). Also, (i) tells us that if $ab = c$, then $ca = b$ and $bc = a$. Given two elements a, b in an alternating quasigroup, let $c = ab$ and $d = ba$, and then we can easily verify the following multiplication table for a, b, c, d from axioms (i) and (ii):

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Conversely, if a quasigroup satisfies the property that every two elements generate a subquasigroup of four elements isomorphic to the above one, then it is easy to verify that axioms (i) and (ii) are satisfied. Alternating quasigroups are related to the geometries of order three by

THEOREM 12. *The subquasigroup structure of an alternating quasigroup determines a geometry of order three with a number of points equal to the order of the quasigroup. Conversely, given a geometry of order three, an alternating quasigroup can be constructed with this given geometry as the geometry determined by its subquasigroup structure.*

Given an alternating quasigroup with elements a_1, a_2, $\cdots$, a_i, $\cdots$, define a geometry on an equal number of points P_1, P_2, $\cdots$ by the condition that P_i, P_j, P_k, P_m form a line if and only if a_i, a_j, a_k, a_m form a subquasigroup. It is clear from this definition and the properties of alternating quasigroups that we have mentioned, that any two points will determine a unique line, so that we have indeed a geometry of order three.

Conversely, in passing from the geometry to an alternating quasigroup, we let four elements form a subquasigroup whenever the corresponding four points of the geometry form a line, and the products in this subquasigroup are defined in either of the two ways which make it isomorphic to the multiplication table given above. (It will be noticed that this argument bears a certain resemblance to the proof of Theorem 1.) The justification for introducing alternating quasigroups here lies in the following theorem, the proof of which is immediate.

THEOREM 13. *The direct product of two alternating quasigroups is also an alternating quasigroup.*

COROLLARY. *If there exist two geometries of order three with n and m points respectively, then there exists a geometry of order three with nm points.*

This process essentially gives us a way of multiplying two geometries of order three to get another one. Let us take a quick look at the orders less than 1000 for which we have vector loops over $GF(3)$: we have first the projective space series with orders 27, 81, 243, and 729; then the affine space series (by Theorem 9) with orders 33, 129, and 513; and finally, using Theorems 12 and 13, five more with orders 105, 321, 339, 417, and 969. The last five loops will all be simple, since none of these numbers is divisible by 9.

The construction that we have given for $q = 3$ apparently cannot be extended to any other odd prime powers. The intuitive reason that it works here is that there exists an idempotent quasigroup of four elements with the property that its automorphism group is doubly transitive, and this does not seem to happen for quasigroups of order $q + 1$ for odd $q > 3$.

7. Free vector loops and geometries

In this section we shall develop the concept of a free geometry, and show how it may be used to get at the properties of free vector loops.

Let us define a *half-geometry* of order c to be a set of points and lines with the properties that every pair of points is joined by at most one line, and that no line contains more than $c + 1$ points. It is certainly not clear under what circumstances a finitely generated half-geometry may be completed to a geometry of finite upper dimension and the same order. On the other hand, any half-geometry that is not already a geometry has a completion to a geometry of the same order with infinite upper dimension, using what we shall call the free completion. To define the concept of free completion, consider the following two operations on a half-geometry:

(1) *To each line with less than $c + 1$ points add a sufficient number of new points so that it will have exactly $c + 1$ points.*

(2) *For each pair of points not connected by a line add a new line with just these two points on it.*

Now, if the processes (1) and (2) are applied alternately a denumerable number of times to a half-geometry G, then we shall call the resulting set of points and lines the *free completion* G^* of G. It is easy to show that G^* is a geometry generated by any set generating G. If we begin with the half-geometry consisting of m points, we shall call the free completion of this the *free geometry* of order c on m generators.

Using free completions we may construct examples of geometries (and hence vector loops) of a rather different nature than those already exhibited. To illustrate this, we prove

THEOREM 14. *For any order c and for any cardinal n, there exist countably many nonisomorphic geometries on n generators with infinite upper dimensions.*

Let us define a *triangle* in a half-geometry G to be system consisting of three noncollinear points of G (called the vertices), the three lines connecting these points (called the sides), and the $c - 1$ points on each of these three lines. A triangle will be called *restricted* in G if there is a line in G containing a point from each side of the triangle, but not containing any of the vertices. Since the application of either (1) or (2) to G will not change an unrestricted triangle into a restricted triangle or vice versa, the total number of restricted triangles in G is the same as the number in its free completion G^*. On the other hand, if G is not itself a geometry and if it has only a finite number of restricted triangles, we may apply (1), (2), and (1) to G, and then find a triangle which has the property that no two points on different sides are connected by a line. Selecting a point on each side of this triangle and adding a line through these three points, we have restricted this triangle, and shown that G may be imbedded in a half-geometry with a larger (but still finite) number of restricted triangles. Hence, we may construct an infinite sequence of half-geometries, each on n generators, and each with more restricted triangles than the previous one. Since the number of restricted triangles in a geometry is clearly invariant under isomorphism, the free completions of the half-geometries of this sequence will be nonisomorphic. The fact that these geometries will all have infinite upper dimensions follows immediately from

THEOREM 15. *If G^* is a geometry which is the free completion of a half-geometry $G \neq G^*$, then G^* contains subgeometries isomorphic to the free geometry on n generators for any integer $n \geqq 3$.*

In the construction of G^* from G, each application of the processes (1) and (2) adds at least one more point or line respectively to the figure (with the possible exception of the first application of (1)). Hence, at some stage of this construction, a half-geometry G_1 occurs which has at least $n + 2$ points $Q_1, \cdots, Q_{n+2}$ and which contains a line l with only two points on it, say Q_{n+1} and Q_{n+2}. Then let P be a point added to l by the application of (1), and let $l_1, \cdots, l_n$ be the n lines $PQ_1, \cdots, PQ_n$ added by the next application of (2). Selecting for each $i = 1, \cdots, n$ a point P_i which is added to the line l_i by the next application of (1), we claim that the subgeometry H of G^* generated by $P_1, \cdots, P_n$ is isomorphic to the free geometry F on n generators. But the half-geometry consisting of $P_1, \cdots, P_n$ is isomorphic to the set of generators of F, and this may be extended a step at a time to an isomorphism between H and F provided that, whenever we wish to extend the isomorphism to a line of H, only two points of that line will already be assigned images under the isomorphism. This condition will always be satisfied, however, by extending the isomorphism to the points and lines of H in the order that they are introduced in the construction of G^*, since no point

or line of H is present at an earlier stage in the construction of G^* than the P_i's.

We prove next

THEOREM 16. *The free geometry on n generators cannot be generated by fewer than n generators.*[1]

If this geometry has order c, then each line has $c + 1$ points on it, $c - 1$ of which are added to the geometry after the line is added, and the other two points of which were in the geometry before the line was added. Every point except the generators is then a later point on precisely one line and an earlier point on all other lines that it is on (added later or earlier than the line, that is). Given any set of N points which generate the geometry, if one of the points of this set is not an earlier point on the line joining it to some point generated by the other points of the set, then we can replace this point by an earlier point on this line, and the modified set of points still generates the geometry. Continuing this process, we must reach eventually a set of $N' \leqq N$ generators with the property that each generator is an earlier point on any line connecting it to a point generated by the other generators of this set. We call a set of generators with this last property a *normal set of generators.*

To show that $N \geqq n$, it is sufficient to show that a normal set of generators must include the original n generators. And to show this, it is sufficient to show that starting with a normal set of generators, the new points added at each stage are the later points on the new lines ("later" and "earlier" shall always refer to the original generation, and "new" and "old" shall refer to the generation by the normal set under investigation). Suppose that the new points added on a new line at some stage of generation by a normal set of generators are not all later points; then let us consider the first such case. Let Q and R be the old points on such a line, let P be an earlier point on the line ($\neq Q, R$), and let Q be the old point which is not an earlier point. If Q were not an element of the normal set of generators, then it would be a later point on two lines (since P is the first violation of the rule of newer points being later ones), which is impossible, so Q is one of the normal set of generators. If R were generated by the normal set without Q, then the whole normal set would not be normal by definition, so R depends on Q. Therefore R is also a later point on the line QR, and taking it instead of Q in the argument above shows that R is an element of the normal set of generators. But then we can modify our set of generators by replacing Q by the earlier element P, and our set of generators is not normal. This contradiction proves the theorem.

Consider now a homomorphism f of a vector loop V onto a second vector loop V' (it is assumed that V and V' are over the same field, and that f is an

[1] The author would like to thank J. W. Pratt for his suggestions on the proof of this theorem.

operator homomorphism). If G and G' are the respective geometries of V and V', and if H is the subgeometry of G corresponding to the kernel K of f, then f induces a map f^* of the points of G not in H onto the points of G'. Clearly the lines of G with one point in H go into points of G', and those with no points in H go into lines of G'. This motivates us to define a *homomorphism* f^* of a geometry G into a geometry G' to be a map of some of the points and lines of G onto the points and lines of G' satisfying the following conditions for any pair of points p, q of G:

(1) *If p and q have distinct images in G', then the line joining them goes into the line joining their images.*
(2) *If p and q have the same image in G', or if p has an image and q does not, then the line joining them has the same image as p.*
(3) *If neither p nor q has an image in G', then neither does the line joining them.*

It follows easily from this definition that the subset of elements of G having no image under f^* is a subgeometry of G called the *kernel* of f^*, and that f^* is an isomorphism if and only if its kernel is void. We have seen that every homomorphism between two vector loops induces a corresponding homomorphism between the corresponding geometries, but the converse of this is easily seen to be false.

THEOREM 17. *Every geometry is a homomorph of the free geometry with the same number of generators, and any homomorphism of a geometry of n ($< \infty$) generators onto the free geometry on n generators must be an isomorphism.*

Let G be any geometry, and let F be the free geometry on the same number of generators. We shall set up the homomorphism in a denumerable number of stages corresponding to the stages used in constructing F. At the first stage in the construction of F, we had just the generators, so we start here by mapping the generators of F onto the generators of G in some manner. Now at the $(2j)^{\text{th}}$ stage in the construction of F we added the lines between points of the $(2j-1)^{\text{st}}$ stage of F which were not already connected by lines, and so the $(2j)^{\text{th}}$ stage of construction of the homomorphism shall be devoted to finding images of this set of lines. But conditions (1), (2), and (3) prescribe exactly what the images of these lines must be. Similarly, if $\{p\}$ is the set of points of F introduced on a line l at the $(2j+1)^{\text{st}}$ stage in the construction of F, then its image is determined at the $(2j+1)^{\text{st}}$ stage as follows: If l has a line of G' as its image, then the points $\{p\}$ are mapped in a one-to-one manner onto the points of this line excluding the images of the two points of l whose images are already known; if l has a point as an image, the points $\{p\}$ are each assigned the same image as l, except that one point is given no image if both the old points of l have images; and, if l has no image, then the points $\{p\}$ are assigned no image. It is evident that this construction will yield a homomorphism.

To show the second half of the theorem, we need only comment that if we look at a homomorphism onto a free geometry broken down into stages as above, the number of points in the image and in the inverse image will be the same at each stage, and will be finite. Hence, there can be no kernel.

We are now ready to show that there is a well-defined concept of a free vector loop satisfying the usual properties that the word "free" implies. We begin by defining the *free vector loop X on n generators* (where n can be any cardinal) over the division ring D of cardinality c to be any vector loop over D corresponding to the free geometry on n generators. The fact that this vector loop is unique up to isomorphism, as well as the implications of the word "free", are established by the next theorem.

THEOREM 18. *Every vector loop over a division ring D is the homomorphic image of the free vector loop over D on the same number of generators, and any vector loop similar to a free vector loop is isomorphic to it.*

If V is an arbitrary vector loop, X the free vector loop on the same number of generators, and if G and F are their respective geometries, then we have already established the existence of a homomorphism of F onto G, which we shall try to cover with a homomorphism from X onto V. We begin by sending the generators of X onto the generators of V, and then, after constructing each stage of the homomorphism f^* of F onto G, we extend the partially constructed homomorphism of X onto V to cover it. The details of this process are straightforward except for one important point—of the many ways of mapping the new points of a line in the $(2j + 1)^{st}$ stage of the construction of f^* in Theorem 17, we may choose now only that unique way which can be covered (since we can restrict our attention to each line of G independently, this is really just a statement about constructing homomorphisms of two-dimensional vector spaces). This point reflects the fact that the homomorphism f of X onto V is completely determined once the images of the generators of X have been determined, while the homomorphism f^* of F onto G is certainly not determined by the images of the generators of F.

Now let X be a free vector loop with generators $\{x_i\}$, and let X' be similar to X. Then the set of elements $\{y_i\}$ in X' corresponding to the elements $\{x_i\}$ of X under the similarity transformation generate X'. Using the first half of Theorem 18, we conclude the existence of a homomorphism f of X onto X' such that $f(x_i) = y_i$. If f^* is the induced homomorphism of the associated geometry G onto itself, then f^* is the identity on the generators of G (which correspond to the x_i's), and hence the subgeometry generated by any finite set of these generators is mapped into itself by f^*. But if P is a point in the kernel of f^*, then it is in a subgeometry on a finite number of the generators of G and is in the kernel of f^* restricted to this subgeometry, contradicting the second half of Theorem 17. Thus, f^* is an isomorphism, implying that X and X' are isomorphic, and finishing the proof.

Using Theorems 15 and 16, we also have the following

COROLLARY. *If X_m and X_n are the free vector loops over a division ring D on m and n generators respectively, where m and n are distinct positive integers, then X_m and X_n are not isomorphic, but either one is isomorphic to a subspace of the other.*

BIBLIOGRAPHY

1. A. A. ALBERT, *Quasigroups. I*, Trans. Amer. Math. Soc., vol. 54 (1943), pp. 507–519.
2. R. H. BRUCK, *Some results in the theory of guasigroups*, Trans. Amer. Math. Soc., vol. 55 (1944), pp. 19–52.
3. ———, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), pp. 245–354.
4. R. D. CARMICHAEL, *Introduction to the theory of groups of finite order*, Boston, Ginn, 1937.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN