NONASSOCIATIVE VALUATIONS

DANIEL ZELINSKY

In a paper entitled *Noncommutative valuations*, Schilling [8][1] proved that if an algebra of finite order over its center is relatively complete in a valuation (where the value group of the nonarchimedean, exponential valuation is not assumed to be commutative) then the value group is commutative. A similar type of theorem, proved by Albert [1], states that if an algebra of finite order over a field is an ordered algebra, then the algebra is itself commutative.

In the present paper, the notions of valuation and ordered ring are carried over in the obvious fashion to the case of nonassociative algebras (the set of values of a valuation are no longer required to lie in an ordered group, but only in an ordered loop). In this situation, an analogue of Schilling's result remains true with an added hypothesis: If an algebra of finite order has a unity quantity and has a valuation inducing a rank one valuation of the base field, then the value loop of the algebra is commutative, associative, and archimedean-ordered. No completeness is needed. In particular, every valuation of an algebra (with a unity quantity) of finite order over an algebraic number field has a group of real numbers for its value loop.

However, in general the obvious extensions of both Schilling's and Albert's results are false, since there are noncommutative, nonassociative algebras of arbitrary finite order over a field which have valuations with nonassociative value loops and which are ordered algebras. Examples of such algebras are obtained by proving that a necessary and sufficient condition for an ordered loop L to be the value loop of some algebra of finite order is that some subgroup of the center of L have finite index in L. We construct some such loops in §3. All such loops will be determined in another paper.

1. **Ordered loops.** An ordered loop L is a set of elements $x, y, z, \cdots$ on which are defined a binary function, $+$, and a binary relation, $>$, with the following properties:

(1) $+$ is a single-valued function on LL to L.

(2) If x and y are in L, then there exist unique elements u and v in L such that $u+x=y$ and $x+v=y$.

Presented to the Society, December 28, 1946; received by the editors November 26, 1946, and, in revised form, May 10, 1947.

[1] Numbers in brackets refer to the bibliography at the end of this paper.

(3) There is an element 0 in L such that $0+x=x+0=x$ for every x in L.

(4) If $x>y$ and $y>z$ then $x>z$.

(5) For each x and y in L, one and only one of the three possibilities $x>y$, $y>x$, $x=y$ holds.

(6) If $x>y$ then for any z in L, $x+z>y+z$, $z+x>z+y$.

We shall use the notations $y-x$ and $-x+y$ for the quantities u and v, respectively, defined in (2).

Ordered loops have most of the elementary properties of ordered groups (in fact, lattice-ordered quasigroups, if suitably defined, have a theory closely paralleling that of l-groups). In particular, we list without proof the following lemmas, true in any ordered loop.

(7) If $x>y$ then $x-z>y-z$ and $-z+x>-z+y$.

(8) If $x>y$ and $x'\geqq y'$ or if $x\geqq y$ and $x'>y'$ then $x+x'>y+y'$, $x-y'>y-x'$ and $-y'+x>-x'+y$.

If n is a positive integer and x is an element of a loop we define the symbol nx inductively by writing $1x=x$, $nx=(n-1)x+x$; we call nx the nth right multiple of x.

(9) If $nx>ny$ then $x>y$.

(10) If $x\neq 0$ then every element of L obtained by adding a finite number of summands, each equal to x (with any association), is different from zero.

Let us also list a few definitions usually made in the study of loops. The center of a loop L is the set of all c in L that commute and associate with all elements of L. More precisely (cf. Albert [**2**, p. 516]) the elements c are characterized by the property that for all x and y of L,

$$c + (x + y) = (c + x) + y = x + (y + c).$$

An equivalent statement is that the center of L consists of all elements of L invariant under the group of inner mappings of L (cf. Bruck [**4**, p. 257]). The definition of the center of a loop leads readily to the theorem that if c is in the center of L, then the loop generated by c is an abelian group and is contained in the center of L.

A normal subloop N of a loop L is a subloop invariant under the inner mapping group of L. Equivalently,

$$N + (x + y) = (N + x) + y = x + (y + N)$$

for every x and y in L. The characteristic property of a normal subloop N is the existence of a quotient loop L/N, formed in the usual way, to which L is homomorphic. Clearly any loop contained in the center of L is a normal subloop of L.

An element x is positive if $x>0$. An ordered loop is discrete if it has a smallest positive element (note that this terminology differs from that of Krull [**7**, p. 171]).

Two ordered loops are order-isomorphic if there is a one-to-one correspondence between them which preserves the operation $+$ and the relation $>$.

A subset H of an ordered loop L is an isolated subloop or l-ideal in case H is a normal subloop and if H contains, with x and y, every z such that $x>z>y$ (an equivalent definition is obtained by taking $y=0$). Just as in the case of abelian groups, the characteristic property of an isolated subloop is the existence of a natural ordering of the quotient loop L/H, so that if $x>y$ in L, then $x+H\geqq y+H$ in L/H (cf. Birkhoff [**3**, p. 310]).

An ordered group is archimedean-ordered in case it has no isolated subgroups besides zero and the whole group. The principal property of archimedean-ordered groups is that every such group is order-isomorphic with an additive group of real numbers (Cartan [**5**]).

Our study of nonassociative valuations will be based on the following two theorems on ordered loops.

THEOREM 1. *Let L be a discrete ordered loop having a least positive element, e. Then e is in the center of L and so generates an associative, commutative, normal subloop G of L. Furthermore, G is an isolated subloop of L.*

PROOF. We must show that for all x, y in L,

$$e+(x+y)=(e+x)+y=x+(y+e). \tag{11}$$

First, there is no element of L between $x+y$ and $e+(x+y)$. For if $x+y<z<e+(x+y)$ then $0<z-(x+y)<e$, contradicting the hypothesis that e is the least positive element of L. Similarly there is no element between $x+y$ and $(e+x)+y$, nor between $x+y$ and $x+(y+e)$ so that of the three elements in (11), all are greater than $x+y$ but none is greater than any other. Hence they are equal. This proves that e is in the center of L so that the loop G generated by e is an abelian group and is also in the center of L. If this group is not isolated, there is an x in L but not in G and there is a positive integer n with $0<x<ne$. Let n be chosen as the smallest such positive integer. Then $(n-1)e<x<ne$, $0<x-(n-1)e<e$, contrary to our hypothesis on e.

THEOREM 2. *Let L be an ordered loop containing an archimedean-ordered group G in its center. Suppose there is a positive integer n such* *that G contains the nth right multiple of every element of L. Then L is commutative, associative and archimedean-ordered.*

PROOF. First, suppose G is discrete. Then G is order-isomorphic with the additive group of rational integers and we may prove that L also has a least positive element. For consider the set of all nx with $x>0$ in L. This is a set of positive elements in G and so there is a smallest one, say ne. By (9) this determines a unique $e>0$ in L which, again by (9), is a least positive element of L. By Theorem 1, e generates an isolated abelian group H in the center of L. The intersection $G\cap H$ is then an isolated subgroup of G and is not zero since it contains ne. Since G is archimedean-ordered, $G\cap H=G$ and $H\supset G$. But consider the mapping of L onto the ordered quotient loop L/H. The group G maps onto zero so that for every y in L/H, we have $ny=0$. Then by (10), it follows that $y=0$, $L/H=0$, $L=H$, which proves Theorem 2 in this case.

Second, suppose G has no least positive element. In this case, using the fact that G is order-isomorphic with an additive group G' of real numbers, we shall set up an order-isomorphism between L and a group L' of real numbers. We already have an isomorphism between G and G'. Let the correspondent in G' of an element u of G be denoted by u'. Then if x belongs to L, define

$$A(x) = [\text{all } u' \text{ in } G' \text{ such that } u \geqq x],$$
$$B(x) = [\text{all } u' \text{ in } G' \text{ such that } u \leqq x].$$

Since we are assuming that G' is not discrete it follows in the usual fashion that for each x, g.l.b. $A(x)=$ l.u.b. $B(x)$. We define a correspondence on L to the real numbers as follows:

$$x \to x' = \text{g.l.b. } A(x) = \text{l.u.b. } B(x). \tag{12}$$

If x is in G we then have two definitions for x' which obviously coincide. By the standard methods it can now be proved that (12) is a homomorphism so that the set L' of all x' is a group of real numbers. Then if $x'=y'$ we have $(nx)'=nx'=ny'=(ny)'$; but nx and ny are in G so that by hypothesis $nx=ny$ and by (9), $x=y$. Thus (12) is an isomorphism. Finally, if $x>y$ then $A(x)\subset A(y)$, $x'\geqq y'$ and $x'\neq y'$ by the one-to-one character of (12). It follows that (12) is an order-isomorphism, which completes our proof.

2. **Valuations.** Let R be a ring (not necessarily associative). A valuation of R is a function V which associates to each nonzero element of R an element of an ordered loop L with the properties

$$V(a+b) \geqq \min [V(a), V(b)], \tag{13}$$

$$V(ab) = V(a) + V(b), \tag{14}$$

whenever a, b and $a+b$ are nonzero elements of R. We define $V(0)=\infty$ where the symbol ∞ is to have the properties $\infty+x=x+\infty=\infty$, $\infty>x$ for all x in L. Then (13) and (14) hold for all a, b in R. We denote by $V(R)$ the set of all $V(a)$ for $a\neq 0$ in R.

Such a valuation, even though L is nonassociative, has most of the elementary properties of an ordinary valuation. In particular, $V(a_1, \cdots, a_t) = \min [V(a_1), \cdots, V(a_t)]$ unless for some pair of distinct subscripts i and j, $V(a_i)=V(a_j)$.

Note that a ring R with a valuation V has no divisors of zero, for if $ab=0$ then $\infty = V(ab) = V(a)+V(b)$ and at least one of $V(a)$, $V(b)$ must be ∞. If R is a division ring (that is, for every $a\neq 0$ and b of R there exist unique elements c and d in R such that $ac=da=b$), and if in addition R has a unity quantity e such that $ea=ae=a$ for all a in R, then $V(R)$ is an ordered loop called the value loop. This is the case in the following theorem.

THEOREM 3. *Let A be an algebra (not necessarily associative) of order n over a field F and let A contain a unity quantity. If A has a valuation V then V induces a valuation on F such that $V(F)$ is an ordered abelian group G. If G is archimedean-ordered, then the value loop $L=V(A)$ is in fact associative, commutative and archimedean-ordered.*

PROOF. Since A is an algebra of finite order over F without divisors of zero, it follows that A is a division ring and that L is an ordered loop. Since the elements of F commute and associate with the elements of A, G will be in the center of L. Our proof will then merely consist in showing that for every x of L, $(n!)x$ belongs to G, so that Theorem 2 will immediately give the desired result.

LEMMA 1. *L/G is a finite loop whose order is not greater than n.*

PROOF. Suppose there are $n+1$ distinct elements of L/G and hence $n+1$ elements $x_1, \cdots, x_{n+1}$ of L that are incongruent modulo G. Then $x_i = V(a_i)$ for some a_i of A. But there exist α_i in F, not all zero, with $\sum \alpha_i a_i = 0$. Then $\infty = V(\sum \alpha_i a_i)$ and since $\infty \neq \min [V(\alpha_i a_i)]$, we must have $V(\alpha_i a_i) = V(\alpha_j a_j)$ for some i and j with $i\neq j$. That is, $V(\alpha_i)+x_i = V(\alpha_j)+x_j$, $x_i = -V(\alpha_i)+V(\alpha_j)+x_j$, $x_i \equiv x_j \pmod{G}$. This is a contradiction.

LEMMA 2. *If K is a finite loop whose order is not greater than n, then for every x of K, $n!x=0$.*

PROOF. First, for every x there is a positive integer $n_x \leqq n$ such that $n_x x = 0$. For there certainly is a pair of distinct positive integers p_x and q_x, both not greater than n, such that $p_x x = q_x x$. And by subtracting x's from the right, one at a time, we arrive at $n_x x = 0$, where $n_x = |p_x - q_x|$.

Second, if n_x divides a positive integer p, then $px = 0$. This is proved by writing $p = n_x q$ and making an induction on q. Hence $p = n!$, being divisible by n_x for every x, has the property that $px = 0$ for all x.

Lemmas 1 and 2 together imply that for every x of L, $n!x$ maps into zero in L/G and so is in G. Then Theorem 2 immediately asserts the truth of Theorem 3, as predicted.

3. **Examples of ordered loops.** According to Lemma 1, L is an ordered loop containing the ordered group G in its center in such a way that the index of G in L is finite. In this section we shall demonstrate that for some nonarchimedean groups G there actually exist nonassociative ordered loops L in the relation to G described above.

In particular, let G be an ordered loop with an isolated subloop H and let G/H be discrete. Denote by e an element of G whose image in G/H is the least positive element of G/H. Next, let K be a cyclic group of order n generated by an element b. We shall construct an ordered, nonassociative loop L as a loop extension of G by K. L consists of all ordered pairs (k, g) with k in K and g in G. Addition in L is defined by the rule

$$(k_1, g_1) + (k_2, g_2) = (k_1 + k_2, g_1 + g_2 + f[k_1, k_2])$$

where $f(k_1, k_2)$ is a function on KK to G with $f(0, k) = f(k, 0) = 0$ for all k of K. This makes L a loop with the identity element $(0, 0)$. The loop G is embedded in L in the sense that the set of all $(0, g)$ is isomorphic with G. We make the following restrictions on the "factor set" $f(k_1, k_2)$ that will allow us to order L. If m_1 and m_2 are nonnegative integers, both less than n, then we demand that $f(m_1 b, m_2 b)$ be in H or in $e+H$ according as $m_1 + m_2 < n$ or $m_1 + m_2 \geqq n$. Clearly if $H \neq 0$ we may still choose the function f so that L is nonassociative and noncommutative. Regardless of this fact, we can order L by defining $(m_1 b, g_1) > (m_2 b, g_2)$ in case

$$g_1 + H > g_2 + H,$$

or

$$g_1 + H = g_2 + H \quad \text{and} \quad n > m_1 > m_2 \geqq 0,$$

or

$$g_1 + H = g_2 + H, \quad m_1 = m_2 \quad \text{and} \quad g_1 > g_2.$$

This is clearly a linear, transitive ordering of L which preserves the ordering of G. A straightforward application of the definition shows that L is actually an ordered loop under this ordering.

It is a trivial exercise to prove that the commutative and associative laws hold in L whenever one of the summands is in the center of G. Thus if G is an abelian group, it is in the center of L and L is an example of an ordered loop such as we were searching for.

4. **Examples of nonassociative valuations.** Let L be any ordered loop and D any ring (not necessarily associative) without divisors of zero. Then we shall exhibit a ring R with a valuation V with $V(R)=L$ and with a residue class ring[2] isomorphic with D. The ring R is constructed in the usual fashion as the ring of "power-series" with exponents in L and coefficients in D. More precisely, R consists of all functions f on L to D with the property that the set $L(f)$, consisting of all x in L for which $f(x)\neq 0$, is well-ordered by the ordering of L. If f and g are in R we define $f+g$ to be the function whose value at each x of L is $f(x)+g(x)$ and the product fg to be the function whose value at x is[3] $\sum f(y)g(z)$, the summation extending over all pairs (y, z) with $y+z=x$. The summation is meaningful because for a given x there is only a finite number of pairs (y, z) for which y is in $L(f)$, z is in $L(g)$ and $y+z=x$. The proof of this fact as well as the proofs that $L(f+g)$ and $L(fg)$ are well-ordered and that R is actually a ring are essentially identical with the proofs given by Hahn [6, pp. 647ff.]. A similar comment applies to the theorem that if D is a division ring, then so also is R. In particular if D has a unity quantity 1, then R has a unity quantity e with the characteristic property that $e(0)=1$, $e(x)=0$ if $x\neq 0$. If we define $V(f)$ for any f of R to be the smallest element of $L(f)$, we have a function on R to L with $V(R)=L$. In fact this is a valuation, the proof of (13) and (14) proceeding exactly as in the associative case. To prove that the residue class ring is isomorphic to D, remark that the ring Q consists of all f in R for which $f(x)=0$ when $x<0$ and that the prime ideal P consists of all f in R for which $f(x)=0$ when $x\leqq 0$. The correspondence $f\rightarrow f(0)$ is then an isomorphism of Q/P and D.

---

[2] If Q is the set of all x in R with $V(x)\geqq 0$ and P is the set of all x with $V(x)>0$, then Q is a ring in which P is a prime ideal. The residue class ring Q/P is called the residue class ring of R.

[3] This is a very special type of power series ring, but more generality here would be unwarranted.

THEOREM 4. *If we choose D to be a field and L to be an ordered loop such as was constructed in* §3 *(L contains a group G in its center with L/G finite), the resultant power-series ring R is an algebra of finite order over a field F and has a unity quantity. It also has a valuation V with a value loop L. The order of R over F is the index of G in L so that by suitable choice of L we can find algebras of arbitrary order over F with non-associative valuations.*

PROOF. Let F be the set of all f in R such that $L(f)\subset G$. By the classical result, F is a field (Hahn [6]). Let $x_1, \cdots, x_n$ be a maximal set of elements of L incongruent modulo G and let $f_1, \cdots, f_n$ be the elements of R defined by the equations $f_i(x_i)=1$, $f_i(x)=0$ if $x\neq x_i$. If $g(x)$ is any element of R, $gf_i(x)=\sum g(y)f(z)$, the sum ranging over all y of $L(g)$ and z of $L(f_i)$ with $y+z=x$. Since $L(f_i)$ consists of the single point x_i, we have the identity

$$gf_i(x) = g(x - x_i).$$

If f is any element of R, let $L_i(f)$ be the set of all x in $L(f)$ with $x\equiv x_i \pmod{G}$. Then each $L_i(f)$ is well-ordered and $L(f)$ is the union of the disjoint sets $L_i(f)$ $(i=1, \cdots, n)$. Define $f^i(x)$ to be the function which is equal to $f(x)$ on $L_i(f)$ but zero elsewhere and $g_i(x)$ to be $f^i(x+x_i)$. Then f^i and g_i are elements of R, $f^i=g_if_i$ and

$$f = \sum_{i=1}^{n} f^i = \sum_{i=1}^{n} g_if_i. \tag{15}$$

Since $g_i(x)\neq 0$ implies that $x+x_i$ is in $L_i(f)$ and hence congruent with x_i modulo G, we know that $g_i(x)$ is zero unless $x\equiv 0 \pmod{G}$, so that $L(g_i)\subset G$ and g_i is in F. Hence (15) expresses the fact that R is a linear space of order not greater than n over F. In fact the f_i are linearly independent over F, else $\sum g_if_i=0$ with the g_i in F, $V(g_if_i) = V(g_jf_j)$ for some pair of distinct indices i, j, which implies that $x_i\equiv x_j \pmod{G}$, a contradiction. This completes the proof of Theorem 4.

If, in particular, D is the field of real numbers, the ring R is an ordered division ring[4] if we define $f>0$ to mean $f(V[f])>0$ in D. The proof is trivial.

THEOREM 5. *There exist noncommutative and (necessarily) nonassociative ordered algebras of arbitrary finite order over a field.*

---

[4] An ordered division ring is a ring, linearly ordered by a relation $>$, such that $a>0$ and $b>0$ imply $a+b>0$ and $ab>0$.

Bibliography

1. A. A. Albert, *On ordered algebras*, Bull. Amer. Math. Soc. vol. 46 (1940) pp. 521–522.

2. ———, *Quasigroups*, I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.

3. G. Birkhoff, *Lattice-ordered groups*, Ann. of Math. vol. 43 (1942) pp. 298–331.

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

5. H. Cartan, *Un théorème sur les groupes ordonnés*, Bull. Sci. Math. vol. 63 (1939) pp. 201–205.

6. H. Hahn, *Über die nichtarchimedischen Grossensysteme*, Sitzungsberichte der Mathematisch-Naturwissenschaftlichen Klasse der Kaiserlichen Akademie der Wissenschaften, Wien vol. 116 IIa (1907) pp. 601–655.

7. W. Krull, *Allgemeine Bewertungstheorie*, J. Reine Angew. Math. vol. 167 (1932) pp. 160–196.

8. O. F. G. Schilling, *Noncommutative valuations*, Bull. Amer. Math. Soc. vol. 51 (1945) pp. 297–304.

University of Chicago