ANALOGUES OF THE RING OF RATIONAL INTEGERS

R. H. BRUCK

1. **Introduction.** Let $(R, +, \cdot)$ be any ring (not necessarily associative) with identity 1, and let $(S, +)$ be the subgroup of $(R, +)$ generated by 1. The present paper results from meditations upon the following well-known facts:

(a) S is a subring of R and a homomorphic image of a certain "universal" ring (the ring of rational integers).

(b) If $(A, +)$ is the (necessarily cyclic) free group on the free generator 1, A may be turned into the ring of rational integers by a group-theoretic introduction of multiplication: yx is the image of y under the endomorphism of $(A, +)$ which maps 1 on x.

(c) The homomorphism of $(A, +)$ upon $(S, +)$ which maps 1 on 1 also preserves multiplication.

(d) $(A, +, \cdot)$ is a commutative associative ring without nontrivial zero divisors (an integral domain). Every additive subgroup of A is a subring.

(e) If R is a ring without nontrivial zero divisors and if T is a subring of the centre of R which contains a nonzero element f, there exists an isomorphism mapping T into its quotient field $T//T$ and R into ring $R//T$ of formal fractions x/t, $x \in R$, $t \in T$, $t \neq 0$ (with the familiar definitions[1] of equality, multiplication and addition), namely, $x \to (fx)/f$.

We shall show that if, in (b), $(A, +)$ is replaced by the free loop of rank one, the endomorphisms determine a system $(A, +, \cdot)$ lacking one distributive law but with desirable properties and a rich substructure. In particular, a suitable widening of the notion of ring (to allow nonassociative addition) preserves both (a) and (c). Then (d) remains true with obvious changes in wording, provided the adjective "commutative" is deleted. And, finally, (e) has a perfect analogue.

The paper touches on a number of unsolved problems which seem worthy of study.

2. **Neorings.** A system $(R, +, \cdot)$ with two single-valued binary operations will be called a *right neoring* provided:

(i) $(R, +)$ is a loop with zero 0.

Received by the editors April 27, 1954.

[1] For the precise definitions see Theorem 2.2 below. The construction was used by Bruck and Kleinfeld [1]. (Numbers in square brackers refer to the bibliography at the end of the paper.)

(ii) R is closed under $(\cdot)$ and $x0=0$ for all x in R.

(iii) $(x+y)z=xz+yz$ for all x, y, z in R.

And a right neoring R will be called a *neoring* if also

(iv) $x(y+z)=xy+xz$ for all x, y, z in R.

Just as with rings, adjectives such as "commutative," "associative," "division," when modifying "(right) neoring," refer to multiplication. The prefix "neo" warns that the additive system is a loop but not necessarily an abelian group. Associative division neorings have been studied by Paige [2] under the name of neofields; we, however, reserve the name *neofield* for a commutative, associative division neoring. And finally, by an *integral neodomain* we mean a commutative associative neoring with at least two elements and with no nontrivial zero divisisors.

The *left nucleus* of a right neoring R is the set of all a in R such that $ax\cdot y=a\cdot xy$ for all x, y in R; the left nucleus is[2] a right subneoring of R. The *centre* of a neoring R is the subset (and subneoring) of R consisting of all a in R such that $ax=xa$, $a\cdot xy=ax\cdot y=x\cdot ay$ for all x, y in R. The following theorem is actually two theorems superimposed:

THEOREM 2.1. *Let R be a (right) neoring with (left) identity* 1. *Then the subloop $(S, +)$ of $(R, +)$ generated by* 1 *is a (right) subneoring $(S, +, \cdot)$ contained in the (left nucleus) centre of R.*

PROOF. The final clause of the theorem should be clear. Let T be the set of all t in S such that $tS\subset S$. Then 1 is in T. If t, t' are in T and if $t+t'=x$, $t+y=t'$, $z+t=t'$, then, by (iii), for all s in S, $ts+t's=xs$, $ts+ys=t's$, $zs+ts=t's$. Hence x, y, z are in T, showing that $(T, +)$ is a subloop of $(S, +)$. Since T contains the generator 1 of S, $T=S$. Therefore $SS\subset S$, and the proof is complete.

THEOREM 2.2. *Let the neoring R contain in its centre a subneoring D such that* (a) *D contains at least one nonzero element f*; (b) *no nonzero element of D is a zero divisor in R. Then D is an integral neodomain and the mapping $x\to(fx)/f$ is an isomorphism of R into a neoring $R//D$ (and of D into its quotient neofield $D//D$) consisting of formal fractions x/a, $x\in R$, $a\in D$, $a\neq 0$, subject to the following rules*: (I) $x/a=y/b\rightleftarrows bx=ay$; (II) $(x/a)(y/b)=(xy)/(ab)$; (III) $(x/a)+(y/b)=(bx+ay)/(ab)$.

PROOF. The proof follows familiar lines. We merely remark that the (unique) solutions U, V in $R//D$ of $(x/a)+U=y/b$, $V+(x/a)=y/b$ are given by $U=u/(ab)$, $V=v/(ab)$ where, in R, $bx+u=ay$, $v+bx$

[2] This remark I owe to Daniel R. Hughes, whose incisive comments led me to (4.5) and Lemma 3.1.

$=ay$. It is perhaps surprising that the usual properties of addition are quite unnecessary here, whereas the multiplicative properties of D are much needed.

3. **The free loop of rank one.** Let F be an (additively written) free[3] loop on a single free generator X. The salient fact about F is that if L is any additive loop and a any element of L, the mapping $X \to a$ can be extended uniquely to a homomorphism, say θ, of F into L. If we regard each element of F as a (nonassociative) word $W = W(X)$, we define $W(a)$ as the image, $W(X)\theta$, of $W(X)$ under θ. This turns each word W into a function defined on every loop. Moreover, if ϕ is a homomorphism of L into a loop, $W(a)\phi = W(a\phi)$, since $\theta\phi$ maps X upon $a\phi$.

Now specialize. Let $(L, +)$ be generated by a single element 1 and let θ be the homomorphism of F into L such that $X\theta = 1$. Since 1 generates L, θ is upon L. Therefore every element of L has the form $W(1)$ for at least one word W of F. If α is an endomorphism of L and if $1\alpha = a$, then $W(1)\alpha = W(a)$ for every word W. Hence, as is intuitively obvious: *every endomorphism of L is uniquely determined by its effect on* 1. Moreover, a must satisfy the following condition: (*) if W, W' are words such that $W(1) = W'(1)$, then $W(a) = W'(a)$. Conversely, if a is any element of L which satisfies (*), the mapping $W(1) \to W(a)$ of L is well-defined. Moreover, this mapping is an endomorphism of L, since $W_1 + W_2 = W_3$ implies $W_1(1) + W_2(1) = W_3(1)$, $W_1(a) + W_2(a) = W_3(a)$. Call the endomorphism α. Let $W_0(X)$ be any word such that $W_0(1) = a$. Then there is a unique endomorphism β of F such that $X\beta = W_0(X)$, namely, $W(X)\beta = W(W_0(X))$ for every word W. And $W(X)\beta\theta = W(W_0(X))\theta = W(W_0(X)\theta) = W(W_0(1)) = W(a) = W(1)\alpha = W(X)\theta\alpha$. Since this is true for every word $W(X)$, $\beta\theta = \theta\alpha$. We sum up our results in a lemma:

LEMMA 3.1. *Let F be the additive free loop on one free generator X. Let L be any additive loop generated by a single element* 1 *and let θ be the homomorphism of F upon L such that $X\theta = 1$. Then every endomorphism of L is induced by suitable endomorphisms of F. More specifically, if α is an endomorphism of L, then $\beta\theta = \theta\alpha$ for every endomorphism β of F such that $X\beta\theta = 1\alpha$.*

COROLLARY 1. *For each a in L there is at most one endomorphism α of L such that $1\alpha = a$.*

COROLLARY 2. *If, for every a in L, there is at least one endomorphism*

[3] The present discussion is somewhat informal. For a careful study of free loops see Bates [3]. Some of the present remarks are repeated from Bruck [4].

α of L such that $1\alpha = a$, then every endomorphism of F induces an endomorphism of L.

4. A universal right neoring. For reasons soon to be evident we now replace F by the (isomorphic) additive free loop $(A, +)$ on one free generator 1. For any x in A there is a unique endomorphism of $(A, +)$, call it $\phi(x)$, such that $1\phi(x) = x$. We define multiplication in A by

$$yx = y\phi(x), \qquad \text{all } x, y \text{ in } A. \tag{4.1}$$

This turns A into a right neoring $(A, +, \cdot)$. Indeed, $\phi(0)$ is the zero endomorphism, so $x0 = 0$ for all x in A; and postulates (i), (ii), (iii) are otherwise clear. Also $1x = x$ by definition; and $x1 = x$ since $\phi(1)$ is the identity endomorphism of A:

$$1x = x1 = x, \qquad \text{all } x \text{ in } A. \tag{4.2}$$

Moreover, $(A, +, \cdot)$ is associative. Indeed, every endomorphism of $(A, +)$ has the form $\phi(a)$. Thus, since $1\phi(x)\phi(y) = x\phi(y) = xy$,

$$\phi(x)\phi(y) = \phi(xy), \qquad (zx)y = z(xy), \qquad \text{all } x, y, z \text{ in } A. \tag{4.3}$$

The right neoring $(A, +, \cdot)$ is universal in the following sense:

THEOREM 4.1. *Let $(R, +, \cdot)$ be a right neoring with left identity 1 such that 1 generates the additive loop $(R, +)$. Let θ be the homomorphism of $(A, +)$ upon $(R, +)$ such that $1\theta = 1$. Then θ is a homomorphism of $(A, +, \cdot)$ upon $(R, +,)$:*

$$(x + y)\theta = x\theta + y\theta, \qquad (xy)\theta = (x\theta)(y\theta)$$

for all x, y in A. In particular, $(R, \cdot)$ is a semigroup with two-sided identity 1.

PROOF. We merely quote Lemma 3.1 and its Corollary 2, with L, F replaced by $(R, +)$, $(A, +)$ respectively. Indeed, $(xy)\theta = x\phi(y)\theta = x\theta\phi(y\theta) = (x\theta)(y\theta)$, where $\phi(a)$ denotes the unique endomorphism of $(R, +)$ which maps 1 on a. The concluding sentence of the Theorem is clear from (4.2), (4.3).

We now examine further the properties of $(A, +, \cdot)$.

LEMMA 4.1. *$(A, +, \cdot)$ satisfies both cancellation laws:*

$$xz = yz,\ z \neq 0 \rightarrow x = y; \tag{4.4}$$

$$zx = zy,\ z \neq 0 \rightarrow x = y. \tag{4.5}$$

PROOF. (4.4). If $z \neq 0$, $\phi(z)$ maps $(A, +)$ upon the nontrivial subloop $(B, +)$ generated by z. By a property of free loops (Bates [3]),

$(B, +)$ is free with free generator z. Hence $(B, +)$ possesses a homomorphism α upon $(A, +)$ such that $z\alpha = 1$. Then $\phi(z)\alpha$ is the identity endomorphism of $(A, +)$, since $1\phi(z)\alpha = 1$. Consequently $\phi(z)$ is one-to-one, proving (4.4).

(4.5). We need some knowledge of the manner[4] in which $(A, +)$ is generated. We begin with a system consisting of two elements 0, 1 and addition defined only as follows: $0+0=0$, $0+1=1+0=0$. Then we fill out A in stages, always preserving the property $0+a=a+0=0$, by "freely" adjoining in regular alternation (i) all elements p such that a, b are present, p is not, and $a+b=p$; (ii) all elements q such that a, b are present, q is not, and $a+q=b$; (iii) all elements r such that a, b are present, r is not, and $r+a=b$. Now consider two elements x, y of A, with $x \neq y$, and let B be the subset of A consisting of all elements z of A such that $z\phi(x) \neq z\phi(y)$. Of course 0 is not in B, but 1 is in B. Furthermore, if, in (i), a, b are in B, then the "freeness" of p implies[5] that p is in B. Similarly for (ii), (iii). Consequently, B contains every nonzero element of A. Therefore $z \neq 0$, $x \neq y$ implies $zx \neq zy$, whence we deduce (4.5).

LEMMA 4.2. *If $(B, +)$ is any subloop of $(A, +)$, then $(B, +, \cdot)$ is a right subneoring of $(A, +, \cdot)$. Indeed,*

$$AB = B. \tag{4.6}$$

PROOF. If b is in B, $\phi(b)$ maps A upon the additive subloop $\{b\}$ generated by b; that is, $Ab = \{b\}$. Therefore we have (4.6).

[4] See footnote 3.

[5] The implication reflects the fact that the only forced identifications in the construction are those of form $0+k=k$, $k+0=k$. A detailed examination of the points involved, even in quite informal terms, would be prohibitively long. We give a brief indication. Since $x \neq y$, at most one of x, y is 0 or 1; and cases such as $x=0$, $y=1$ will be omitted as trivial. Then at least one of $p\phi(x)$, $p\phi(y)$ must first turn up in the construction at at least as late a stage as does p, essentially because at least one of x, y first turns up later than does 1. Since we are to disprove that $p\phi(x) = p\phi(y)$, we need only consider the critical case that both of $p\phi(x)$, $p\phi(y)$ first appear at the same stage of the construction. At this stage, which is necessarily an extension of type (i), the only sums involving $p\phi(x)$ are $0+p\phi(x) = p\phi(x)$, $p\phi(x)+0 = p\phi(x)$, $a\phi(x)+b\phi(x) = p\phi(x)$; and similarly with x replaced by y. Since a, b are in B, $a\phi(x) \neq a\phi(y)$ and $b\phi(x) \neq b\phi(y)$. The proof now hinges on (*): $a\phi(x)$, $a\phi(y)$, $b\phi(x)$, $b\phi(y)$ are all nonzero. For, if (*) holds, necessarily $p\phi(x) \neq p\phi(y)$. To prove (*), suppose, for example, that $a\phi(x) = 0$; then, also, $b\phi(x) = p\phi(x)$. If $x=0$, then $p\phi(x) = 0$, contradicting the hypothesis that $p\phi(x)$, $p\phi(y)$ first appeared together and not before the (constructed) element p. If $x \neq 0$, then, by (4.4), $b = p$, contradicting the fact that p first appeared later than b. Hence (*) holds and p is in B. The changes to be made in connection with (ii) or (iii) are quite minor; there, however, we must add the case that $b=0$ and a is in B.

As Bates [3] shows, every subloop of $(A, +)$ is free and, moreover, $(A, +)$ contains subloops of countable rank and (hence) subloops of every finite rank. Thus Lemmas 4.2, 4.1 yield the following:

THEOREM 4.2. *Let $(F, +)$ be a free loop of finite or countable rank. Then $(F, +)$ can be imbedded in at least one associative right neoring $(F, +, \cdot)$ which satisfies the cancellation laws* (4.4), (4.5) *and the relation $FG \subset G$ for every subloop $(G, +)$ of $(F, +)$.*

It is to be noted, however, that, in Lemma 4.2, $(B, +, \cdot)$ has no identity element unless $B = A$. And the question remains open as to whether there are "universal" right neorings of arbitrary rank as additive free loops.

In view of Theorems 4.1, 4.2, it is of interest to characterize the kernels of homomorphisms of a right neoring $(R, +, \cdot)$ upon right neorings. Such a kernel must, of course, be a normal subloop of $(R, +)$.

LEMMA 4.3. *Let $(K, +)$ be a normal subloop of the additive loop $(R, +)$ of a right neoring $(R, +, \cdot)$. Then the following properties are n.a.s.c. that K be the kernel of a homomorphism of $(R, +, \cdot)$ upon a right neoring*:

(a) $$KR \subset K;$$

(b) $$x(y + K) \subset xy + K, \qquad \text{all } x, y \text{ in } R.$$

PROOF. *Necessity.* Let ϕ be a homomorphism, with kernel K, of R upon a right neoring. If $k \in K$, $x \in R$, $(kx)\phi = k\phi \cdot x\phi = 0 \cdot x\phi = 0$, so $kx \in K$. This proves (a). Again, $(x(y+k))\phi = x\phi \cdot (y+k)\phi = x\phi \cdot (y\phi + k\phi) = x\phi \cdot y\phi = (xy)\phi$, so $x(y+k) \in xy+K$, proving (b).

Sufficiency. Since $(K, +)$ is normal in $(R, +)$, the mapping ϕ defined by $x\phi = x+K$ is a homomorphism of $(R, +)$ upon a loop $(R/K, \oplus)$ where $\oplus$ is defined by $(x+K) \oplus (y+K) = xy+K$. If $x, y \in R$, $k, k' \in K$, then (a), (b) and the normality of K yield, mod K, $(x+k)(y+k') \equiv x(y+k') + k(y+k') \equiv xy + 0 \equiv xy$. Hence multiplication $\odot$ can be defined unambiguously in R/K by $(x+K) \odot (y+K) = xy+K$. Then ϕ is a homomorphism of R upon a right neoring $(R/K, \oplus, \odot)$.

In any right neoring $(R, +, \cdot)$ define the commutators (x, y) by

$$xy = yx + (x, y). \tag{4.7}$$

LEMMA 4.4. *Let $(K, +)$ be a normal subloop of the additive loop of a right neoring R. Then n.a.s.c. that K be the kernel of a homomorphism of R upon a commutative neoring are*: (a) *(of Lemma* 4.3) *and*

(c) $(x, y) \in K$, *all* x, y *in* R.

COROLLARY. *In the case of* $(A, +, \cdot)$, (c) *alone is n.a.s.c.*

PROOF. (a), (c) are clearly necessary. Conversely, by (a), (c) and the normality of K we have, mod K, $x(y+k) \equiv (y+k)x \equiv yx+kx \equiv yx \equiv xy$. This proves (b) of Lemma 4.3; and (a), (b), (c) are clearly sufficient. In the case of the corollary, by (4.6), (c) implies (a).

Returning to A, we note, from Lemma 4.4 and corollary, that, if $(N, +)$ is the smallest normal subloop of $(A, +)$ containing all multiplicative commutators (x, y), then $(A/N, +, \cdot)$ is a commutative associative neoring with identity, additively generated by its identity. Clearly, $(A/N, +, \cdot)$ is universal for all such neorings and, in particular, for all integral neodomains with identity which are additively generated by the identity. But there remains the question: *Is* $(A/N, +, \cdot)$ *an integral neodomain?* This I have been unable to answer. If the answer is no, one may easily describe "prime" kernels K containing N such that $(A/K, +, \cdot)$ is an integral neodomain; but the problem of universality now arises: Is the set of such kernels closed under intersection?

5. **Finite integral neodomains.** Every finite integral neodomain is, of course, a (commutative) neofield. Paige [2] shows that, for every $n \geqq 2$ and every multiplicative abelian group G of order $n-1$, there exists a neofield $(R, +, \cdot)$ of order n with G as the multiplicative group of nonzero elements. By Bruck [5], either $(R, +, \cdot)$ is a field or $(R, +)$ is a (not associative) simple loop. If $n-1$ is odd or if the 2-Sylow subgroup of G is noncyclic, Paige's work implies that the subneofield of $(R, +, \cdot)$ generated by the identity is the field of order two. For a nontrivial example of a finite neofield generated by its identity it is therefore simplest to take $n \equiv 3 \bmod 4$; and since the loop of order three is a cyclic group, the smallest nontrivial example has order 7. The addition is given by:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	6	3	5	0	2	4
2	2	5	1	4	6	0	3
3	3	4	6	2	5	1	0
4	4	0	5	1	3	6	2
5	5	3	0	6	2	4	1
6	6	2	4	0	1	3	5

Since $(1+1)+1=2$, $1+(1+1)=4$, addition is not associative. It may be verified that the permutation (123456) is an automorphism; the multiplication table is then obvious.

It seems likely that similar examples exist for every $n=4k+3$ where k is a positive integer. In the infinite case, the methods of Paige [2] and Bateman [6] again give neofields of characteristic two, so no example is known of a nontrivial infinite integral neodomain generated by the identity element.

By modifying Paige's work one can readily show how to construct an associative division right neoring in terms of its multiplicative group—the case $1+1=0$ is tied to the theory of complete mappings of groups—but this I will omit.

One final remark. If one attempts to characterize a universal integral neodomain, it is an easy step to the consideration of the notion of a radical of a neoring. It is interesting to note that if a, b are nilpotent elements of a commutative associative neoring, $a+b$ is nilpotent but (I suspect, at least) the solutions x, y of $x+a=b$, $a+y=b$ may not be.

Added September 30, 1954. Recent work of Artzy [7] can be adapted immediately to the construction of infinitely many nonisomorphic "minimal" neofields of countable order, thus solving one of our problems. Moreover the additive loop is simple in each case. We use the proof of Artzy's Theorem 2. If N is the set of all nonzero rational integers, let $k \to f(k)$ be a single-valued transformation of N into N such that

$$f(-f(k)) = k + 1 - f(k) \tag{5.1}$$

for all k in N. If T is a generator of the (multiplicatively written) infinite cyclic group, let $(R, +)$ be the system consisting of a zero, 0, and the powers of T, with $0+0=0$, $0+T^k=T^k+0=T^k$, $T^k+T^{k+1}=0$ for all integers k and with

$$T^j + T^{k+1} = T^{j+f(k-j)} \qquad \text{for } k \neq j. \tag{5.2}$$

As Artzy shows, $(R, +)$ is a loop; moreover there are infinitely many functions f and distinct ones define nonisomorphic loops. Since $T^k+T^{k+1}=0$ for every k, T^k generates $(R, +)$ for every k; in particular, $(R, +)$ is simple. And, finally, if $0\cdot 0=0\cdot T^k=T^k\cdot 0=0$ and $T^j\cdot T^k=T^{j+k}$, $(R, +, \cdot)$ is a neofield.

Bibliography

1. R. H. Bruck and Erwin Kleinfeld, *The structure of alternative division rings*, Proc. Amer. Math. Soc. vol. 2 (1951) pp. 878–890.

2. Lowell J. Paige, *Neofields*, Duke Math. J. vol. 16 (1949) pp. 39–60.

3. Grace E. Bates, *Free loops and nets and their generalizations*, Amer. J. Math. vol. 69 (1947) pp. 499–550.

4. R. H. Bruck, *An extension theory for a certain class of loops*, Bull. Amer. Math. Soc. vol. 57 (1951) pp. 11–26.

5. ———, *Loops with transitive automorphism groups*, Pacific Journal of Mathematics vol. 1 (1951) pp. 481–483.

6. P. T. Bateman, *A remark on infinite groups*, Amer. Math. Monthly vol. 57 (1950) pp. 623–624.

7. Raphael Artzy, *On loops with a special property*, to appear in Proc. Amer. Math. Soc.

UNIVERSITY OF WISCONSIN

THE SCHWARZIAN DERIVATIVE AND CONVEX FUNCTIONS

RICHARD F. GABRIEL

1. **Introduction.** In a comparatively recent paper [2], Nehari has shown that if

$$f(z) = 1/z + a_1 z + a_2 z^2 + \cdots \qquad \text{for } 0 < |z| < 1 \tag{1.1}$$

and

$$|\{f(z), z\}| \leqq \frac{\pi^2}{2} \qquad \text{for } |z| < 1, \tag{1.2}$$

where $\{f(z), z\}$ is the Schwarzian derivative of $f(z)$ with respect to z, then $f(z)$ is univalent in the unit circle. The methods of Nehari can be modified to apply to functions of the form (1.1) to be shown univalent and convex in the unit circle. The principal result obtained in this paper is the following:

THEOREM 1. *If $f(z)$ is of the form* (1.1), *regular for $0<|z|<1$, and if*

$$|\{f(z), z\}| \leqq 2c_0 \qquad \text{for } |z| < 1, \tag{1.3}$$

where c_0 is the smallest positive root of the equation

$$2x^{1/2} - \tan x^{1/2} = 0, \tag{1.4}$$

then $f(z)$ is univalent in $0<|z|<1$ and maps the interior of each circle $|z| = r < 1$ onto the exterior of a convex region. The constant c_0 is the largest possible one.

Presented to the Society, April 24, 1954; received by the editors May 20, 1954.