Kyungpook Math. J.
Volume 28. Number 1
June, 1988

EXAMPLES OF NEAR-RING NEUMANN SYSTEMS

By B. C. McQuarrie and J. J. Malone, Worcester

Abstract: In 1940, B. H. Neumann, working with a system more general than a near-field, proved that the additive group of such a system (and of a near-field) is commutative. The algebraic structure he used is known as a Neumann system (N-system). Here, the prime N-systems are classified and for each possible characteristic, examples of N-systems which are neither near-fields nor rings are given. It is also shown that a necessary condition for the set of all odd polynomials over $GF(p)$ to be an N-system is that p is a Fermat prime.

1. Introduction

A Neumann system is a (left) near-ring $(N, +, \cdot)$ such that

(1) $rt=st$ and $t\neq 0$ imply $r=s; r, s, t$ in N.

(2) there exists $e\neq 0$ in N such that $e^2=e$, and

(3) there exists an h in N such that $h+h=e$.

Such a system, more briefly referred to as an N-system, was introduced in [5] and there shown to have commutative addition. Since any near field is an N-system, this demonstrated commutativity of the additive group of a near-field. N-systems have also been discussed in [2], [4], and [6].

It is easy to show that e is a right identity and the characteristic of an N-system must be zero or an odd prime. Furthermore, with a prime N-system defined to be an N-system whose only sub-N-system is itself, we can quickly discern the prime N-systems. If N is an N-system of characteristic 0, then N contains a copy of Z and so must also contain 1/2. Let S N be the sub-N-system generated by 1/2, i.e. $S=\{m/2^k \mid k$ a non-negative integer, m an odd integer or $0\}$. It is readily seen that S is an N-system and an integral domain. If N is an N-system of characteristic p, then the proof used to establish the prime fields of characteristic p may be adapted and used to show that the prime N-system of N is $GF(p)$. This last result is to be expected since Theorem 1.4 of [1] or Theorem 1.2 of [3] guarantees a finite N-system is a near-field.

The only proper N-system (one that is neither a near-field nor a ring)

appearing in the literature is the one of characteristic zero originally given in [4]. The main goal of this paper is to show that there are proper N-systems for each possible characteristic. Obviously, any proper N-system has to be infinite.

2. Examples

In this section the example of [4] is generalized and examples of proper N-systems are given for each possible characteristic. The basic approach used is to consider sets of polynomials over prime N-systems. Addition will be as usual; however multiplication will be taken as substitution or composition: $(x)f \circ (x)h=((x)f)h$. If R is a commutative ring with identity, then $R[x]$ will be used to designate the set of all polynomials over R with operations as just described. It is well known that $R[x]$ is a near-ring whose additive group is abelian.

Note that although $R[x]$ is a near-ring, it is not an N-system since $x \circ x^2 = (-x) \circ x^2$. Because of such difficulties we restrict attention, except for the zero polynomial, to polynomials in which each term has odd degree and refer to these as odd polynomials. Also, when R is some $GF(p)$ we take the polynomials to be polynomial forms rather than polynomial functions since, for the polynomial functions, $x \circ (x+x^{p-2}) = x^{p-2} \circ (x+x^{p-2})$ for each odd prime p although, for $p>3$, x and x^{p-2} define different functions.

The set of all odd polynomials forms (and the 0) with operations as given above will be designated by $R((x))$. Clearly, $R((x))$ is a near-ring. Also, in order for $R((x))$ to be an N-system, R itself must be an N-system. If e is the halvable identity of R, then ex is the halvable identity of $R((x))$. Thus, to show $R((x))$ is an N-system, we need only show that $R((x))$ satisfies the right cancellation law. In investigating the right cancellation law in $R((x))$ the following notation will be used.

Let $(x)f$, $(x)h$, $(x)g$ be in $R((x))$ where $(x)f=a_1x+a_3x^3+\cdots$, $(x)h=b_1x+b_3x^3+\cdots$, and $(x)g=c_1x+c_3x^3+\cdots$. Assume

$$(x)f \circ (x)g=(x)h \circ (x)g, \quad (x)g \neq 0.$$

By equating the coefficients of like powers of x, we attempt to show recursively that $a_1=b_1$, $a_3=b_3$, etc., so that $(x)f=(x)h$.

Note that if the coefficient of an arbitrary power of x, say x^s, is considered, then t he contribution to the coefficient from $c_v((x)f)^v$ is c_v times a sum of terms.

Each of these terms has v of the a's as factors and in fact the subscripts of the a's in any one of the terms constitute a partition of the integer s into v positive, odd, integer summands. With each term there is a numerical coefficient which corresponds to the number of permutations of the a's used in that term.

Also, k will be such that c_k is the first non-zero coefficient of $(x)g$ and, if $(x)f \neq 0$, q will be the subscript of the first non-zero coefficient of $(x)f$.

The following proposition introduces a condition which will be of continuing interest.

PROPOSITION 1. *Let R be a halvable integral domain. A necessary condition for $R((x))$ to be an N-system is that* ($*$) $a^w=b^w$ *implies* $a=b$ *for* a, b *in* R; w *an odd positive integer.*

PROOF. If $a^w=b^w$ but $a\neq b$, then $ax \circ x^w=a^w x^w=b^w x^w=bx \circ x^w$ so that the right cancellation law does not hold.

We now show that, for each possible characteristic, there are proper N-systems. Theorem 2 lays the groundwork for characteristic 0 while Theorem 3 takes care of characteristic p.

THEOREM 2. *Let R be a halvable integral domain of characteristic* 0. *Then condition* ($*$) *is necessary and sufficient for $R((x))$ to be an N-system.*

PROOF. If $(x)f=0$, then $(x)f \circ (x)g=0$. Assume $(x)h\neq 0$ and that b_i is the first non-zero coefficient of $(x)h$. But then, equating coefficients of x^{ik}, we have that $0=c_k b_i^k$. Hence $b_i=0$ and $(x)h=0$.

Now consider the case in which $(x)f\neq 0$. Equating coefficients of x^k we obtain $c^k a_1^k=c_k b_1^k$ which implies $a_1^k=b_1^k$ so that by ($*$) $a_1=b_1$. Assume that $a_s=b_s$ for s such that $0<s<t$. If $q\geq t$, that is if $a_s=b_s=0$ for each such s then from the coefficients of x^{tk} we have $c_k a_t^k=c_k b_t^k$ and $a_t=b_t$.

If $q<t$ then consider the coefficients of $x^{(k-1)q+t}$. On the left a contribution to this coefficient of $kc_k a_q^{k-1} a_t$ is obtained from $c_k((x)f)^k$. If any other contributions come from $c_m((x)f)^m$, $m\geq k$, then all a_j involved in these must have $j<t$. Similarly on the right, $c_k((x)h)^k$ yields $kc_k b_q^{k-1} b_t$ and other contributions involve b_j with $j<t$. Since the pattern of coefficients is the same on the right

as on the left except that b_i appears rather than a_i, since $a_i=b_i$ for $i<t$. and since, after composition, corresponding coefficients on each side of the equality are equal, it follows that $kc_k a_q^{k-1} a_t = kc_k a_q^{k-1} b_t$. Since none of the first three factors is 0, we conclude that $a_t=b_t$ so that $(x)f=(x)h$ and the right cancellation law holds.

It is of interest to note that the complex numbers do not satisfy (*) but that any subring of the reals does. In particular, $S((x))$ is an N-system as is $F((X))$ where F is the field of real numbers. This result on $F((x))$ was previously given in [4] where it was also shown that $F((x))$ is a proper N-system. In [4] the right cancellation law for $F((x))$ was proved by using Rolle's Theorem.

THEOREM 3. *For each odd prime p, there exist proper N-systems of characteristic p.*

PROOF. For each odd prime p, let R be $GF(p)$ and let m be a fixed positive even integer. Consider the set $R[[x]]$ of polynomials over R of the form $\sum_w a_w x^{1+wm}$, w a non-negative integer. To establish that $R[[x]]$ is a near-ring, it must be shown that $R[[x]]$ is closed under multiplication. Because of the left distributive law it is sufficient to show that a product such as $(\sum_{w=0}^{k} r_w x^{1+wm}) \circ (sx^{1+um})$ has the required pattern for its exponents. An arbitrary term in the expansion of the product will have the form of a constant times

$$(sr_{k_1}^{a_1} r_{k_2}^{a_2} \cdots r_{k_n}^{a_n}) x^{a_1(1+mk_1)+\cdots+a_n(1+mk_n)},$$

where it is important to note that $\sum_{i=1}^{n} a_i = 1+um$. But then

$$a_1(1+mk_1)+\cdots+a_n(1+mk_n)=\Sigma a_i + m\Sigma a_i k_i = 1+m(u+\Sigma a_i k_i)$$

which is as required. Also, x is in $R[[x]]$ and $((p+1)/2)x$ is its half. The right cancellation law remains to be proved.

Condition (*) applied here takes the form:

(**) $a^{1+wm}=b^{1+wm}$ implies $a=b$ for a, b in R; w a non-negative integer.

In essence this requires that the correspondence $a \to a^{1+wm}$ is an automorphism of the multiplicative group of non-zero elements of $R=GF(p)$. That is, for all possible w, $(p-1,\ 1+wm)=1$. For reasons explained below, we also impose the condition that p not divide $1+wm$. Now it is seen that a possible choice for m is $p(p-1)$. Obviously, many other choices could be made.

The proof of the right cancellation law can now proceed as in the proof of Theorem 2. Since $p-1$ divides m, we have condition (**). Since p divides m, p can never divide and exponent and so, in the third paragraph of the proof of

Theorem 2, the difficulties which would arise if k, as a coefficient, were zero are avoided.

It is easy to show that for each odd prime p, $GF(p)[[x]]$ is a proper N-system. The polynomial x^{1+m} is not invertible; hence the system is not a near field. Also, $(x+x^{1+m})\circ x^{1+m}$ is not equal to $x\circ x^{1+m}+x^{1+m}\circ x^{1+m}$; hence the system is not a ring.

3. A question

THEOREM 3. *Skirts the issue of whether $R((x))$ is an N-system if R is a finite field. The next theorem shows that in most cases the answer is no.*

THEOREM 4. *$GF(p^n)$ satisfies condition ($*$) if and only if p is a Fermat prime and $n=1$ or $p=3$ and $n=2$.*

PROOF. In the first case, condition ($*$) is satisfied if and only if the correspondence $a\to a^w$ is an automorphism of the multiplicative group of non-zero elements of $GF(p)$. That is if and only if, $(w, p-1)=1$ for each odd integer w. Hence $p-1$ is a power of 2 and p has the form 2^S+1. This implies that s itself is a power of 2 and that p is a Fermat prime.

In the second case, p^n-1 must be a power of 2. Then $2^t=p^n-1=(p-1)(p^{n-1}+p^{n-2}+\cdots+p+1)$. Since the second factor on the right of the equation has n terms, each of which is odd, adding up to a power of 2, it follows that n is even. Since this is so, $2^t=p^n-1$ can be written as $(p^{n/2}-1)(p^{n/2}+1)$. These two factors are consecutive even integers each of which is a power of two. Hence $p=3$ and $n=2$.

It is not known whether $GF(p^n)((x))$ is an N-system if p^n is as described in Theorem 4. The proof employed for Theorem 2 and adapted for Theorem 3, will not work if k is divisible by p since, in that case, the statement $kc_k a_q^{k-1} a_t = kc_k a_q^{k-1} b_t$ does not imply $a_t=b_t$ because k, as a coefficient, is zero.

REFERENCES

[1] Graves, J. A., and Malone, J. J., *Embedding near domains*, Bull. Austral. Math. Soc. 9, 33—42. (1973).

[2] Ligh, S., *On the commutativity of near rings* Ⅲ, Bull. Austral. Math. Soc. 6, 459—464. (1972).

[3] Ligh, S., and Malone J.J., *Zero divisors and finite near-rings*, J. Austral. Math. Soc. 11, 374—378. (1970).

[4] Ligh, S., McQuarrie, B and Slotterbeck, O., *On near fields*, J. London Math. Soc. (2), 5, 87—90 (1972).

[5] Neumann, B.H., *On the commutativity of addition*, J. London Math. Soc. 15. 203--208 (1940).

[6] Pilz, G., *Near-Rings* revised ed. Amsterdam-New York-Oxford: North-Holland. 1983.

Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, Massachusetts 01609
U.S.A.