ON PROVING THE ABSENCE OF ZERO-DIVISORS FOR SEMI-GROUP RINGS

Bernhard Banaschewski

(received May 12, 1961)

For any semi-group S and any ring Λ with unit 1 (always taken to be distinct from 0, the neutral element of Λ under addition) there is known to exist a ring $\Lambda[S] \supseteq S$ which is a Λ-bimodule such that (i) S is a subsemi-group of the multiplicative semi-group of $\Lambda[S]$, (ii) $\lambda s = s\lambda$, (iii) $\lambda(st) = (\lambda s)t = s(\lambda t)$ ($s, t \in S$ and $\lambda \in \Lambda$) and (iv) S is a Λ-basis of $\Lambda[S]$. This ring is uniquely determined by these conditions and is usually called <u>the semi-group ring of S over Λ</u>. It may be described explicitly as consisting of the functions $f : S \rightarrow \Lambda$ which vanish at all but finitely many places, with functional addition $(f+g)(s) = f(s) + g(s)$ and convolution $(fg)(s) = \Sigma f(u) g(v)$ $(uv = s)$ as the ring operations, the functional Λ-bimodule operations $(\lambda f)(s) = \lambda f(s)$ and $(f\lambda)(s) = f(s)\lambda$, and each $s \in S$ identified with the characteristic function of $\{s\}$ with values in Λ.

Via the correspondence $S \rightarrow \Lambda[S]$, every property of rings induces a property of semi-groups, and the natural problem arising here is that of characterizing the latter directly in semi-group terms. In the present note, this problem will be studied for the following condition on semi-groups S:

(NZ) If Λ has no zero divisors then $\Lambda[S]$ also has no zero divisors.

Concerning this and the further condition

(O) S is totally orderable,

(i.e., there exists a total ordering $\leq$ of S such that $s < t$ implies $us < ut$ and $su < tu$) one has the well-known implication

$$(O) \Rightarrow (NZ).$$

Proof. Any non-zero $x \in \Lambda[S]$ is a sum $\xi_1 s_1 + \dots + \xi_n x_n$ of $n \geq 1$ terms with uniquely determined non-zero $\xi_i \in \Lambda$ if the

Canad. Math. Bull., vol. 4, no. 3, September 1961

s_i are taken to be distinct. Moreover, it may be assumed that $s_1 < s_2 < \ldots < s_n$. Now, given any two non-zero elements of $\Lambda[S]$ in this form, $a = \alpha_1 s_1 + \ldots + \alpha_n s_n$ and $b = \beta_1 t_1 + \ldots + \beta_m t_m$, one sees that the product ab, if also written in this manner, will have the "leading" term $\alpha_n \beta_m s_n t_m$ which is non-zero since $\alpha_n \beta_m \neq 0$ by hypothesis on Λ. Thus one has $ab \neq 0$.

The essential feature of (O) used in this proof is that it implies a certain other condition for S, namely

(U) For any two finite subsets $F, G \subseteq S$, there exists a unique product in FG, i.e., there exists a pair (a, b), $a \in F$ and $b \in G$, such that $ab = xy$, $x \in F$ and $y \in G$, implies $a = x$ and $b = y$. It is clear that this is all one uses of (O) and that, therefore,

$$(U) \Rightarrow (NZ)$$

Whether the converse of this implication also holds seems an interesting open question. In the case of abelian S this is indeed so, as will be seen later; however, the proof of this draws heavily on the commutativity of S, leaving no indication as to how it might carry over to non-abelian S.

Turning from sufficient to necessary conditions for (NZ), one may consider the Cancellation Law

(C) If $sx = sy$ or $xs = ys$ then $x = y$

for which one has

$$(NZ) \Rightarrow (C)$$

Proof. If $x \neq y$ in S then $x - y \neq 0$ in $\Lambda[S]$, and since $s \neq 0$ in $\Lambda[S]$ for any $s \in S$ one obtains from (NZ) that $s(x-y)$ and $(x-y)s$ are both non-zero. Back in S this means that $sx \neq sy$ and $xs \neq ys$.

A similar result, though less general, is[1]

$$(NZ) \underset{A}{\Rightarrow} (PC)$$

with the Power Cancellation Law

(PC) If $x^n = y^n$ then $x = y$ for any $n = 1, 2, \ldots$.

---

[1] In the following, $\underset{A}{\Rightarrow}$ denotes implication for all abelian S.

Proof. Let $x \neq y$ and suppose there exist natural numbers $n > 1$ such that $x^n = y^n$. Then, let k be the first one of these and consider the equations

$$0 = x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \ldots + xy^{k-2} + y^{k-1})$$

from which

$$x^{k-1} + x^{k-2}y + \ldots + xy^{k-2} + y^{k-1} = 0$$

follows in view of $x \neq y$. This latter equation, however, cannot hold if all summands on its left-hand side are distinct, since S is a basis for $\Lambda[S]$. Hence one must have $x^{k-i}y^{i-1} = x^{k-j}y^{j-1}$ for some $i, j > i$. By cancellation this leads to $x^{j-i} = y^{j-i}$ with $0 < j-i < k$, which contradicts the choice of k.

Combining the last two implications one obtains

$$(NZ) \underset{A}{\Rightarrow} (C) \ \& \ (PC).$$

Now, here one has arrived at a proposition whose converse (restricted to the abelian case) also holds, i.e.,

$$(C) \ \& \ (PC) \underset{A}{\Rightarrow} (NZ).$$

It seems that, so far, transfinite methods have always been employed in obtaining this result. Thus a typical proof proceeds through the following steps: (i) By (C), S can be imbedded in a group G and (ii) (PC) implies that this G is torsion free. Hence (iii) G, written additively now, can be imbedded in a module $\tilde{G}$ over the rational field. (iv) $\tilde{G}$ has a basis which (v) can be totally ordered and (vi) then be used to order $\tilde{G}$ lexicographically. This establishes that S is orderable and thus (O) $\Rightarrow$ (NZ) completes the proof. Clearly, the steps (iv) and (v) require transfinite arguments. Of course, this line of reasoning may be shortened somewhat: the orderability of S can actually be deduced directly, without the intervention of $\tilde{G}$, by a suitable application of Zorn's Lemma. However, that does not change the essential nature of the proof.

The question which naturally arises here is : Can the implication (C) & (PC) $\underset{A}{\Rightarrow}$ (NZ) be obtained without the use of transfinite methods? The answer to this turns out to be: yes, and it will now be shown how this can be done.

We introduce the following concept:

DEFINITION. An element a of a subset $F \subseteq S$ is called an extremity of F if, for any natural number $k > 0$, $a^k = c_1 c_2 \ldots c_k$, $c_i \in F$, implies $c_i = a$ for all i.

Using this notion, one can formulate a further condition on S:
(E) Any non-void finite subset of S has extremities.

In passing, we note that (O) $\Rightarrow$ (E), for if (O) then the greatest and the least element of a finite $F \subseteq S$ with respect to any total ordering of S are clearly extremities of F.

The first step is:

$$(C) \ \& \ (PC) \underset{A}{\Rightarrow} (E)$$

Proof. Let the finite set $F \subseteq S$ have an extremity a and consider $F' = F \cup \{b\}$ where $b \in S$ but $b \notin F$. If b is not an extremity of F' there esist $c_1, \ldots, c_k \in F'$, not all equal to b, such that $b^k = c_1 c_2 \ldots c_k$ with $c_i \in F'$. Cancelling out all $c_i = b$ one obtains, after suitable renumbering, $b^l = c_1 c_2 \ldots c_l$. Now, if a also fails to be an extremity of F' one has $a^m = d_1 d_2 \ldots d_m$ with certain $d_i \in F'$, not all equal to a. Moreover, since a is an extremity of F, not all d_i can belong to F, i.e., some must be equal to b. Let these be exactly the d_i with $i \leq r$ where $r \leq m$; here, one actually has $r < m$ since $r = m$ leads to $a = b$ which contradicts $b \notin F$. Then, $a^m = b^r p$ where p is a product of $m-r$ terms from F. Now, $a^{ml} = b^{lr} p^l = c_1^r c_2^r \ldots c_l^r p^l$ shows a^{ml} to be a product of $rl + (m-r)l = ml$ factors, all in F, and by the choice of a this implies $c_1 = \ldots = c_l = a$. It follows that $b^l = a^l$ and hence $b = a$ which contradicts $b \notin F$.

Thus $F' = F \cup \{b\}$ has a or b as extremity. Since the collection of all non-void finite $F \subseteq S$ satisfies the minimum condition and each $F = \{c\}$ clearly has an extremity, the statement is proved by induction.

Next, we prove

$$(C) \ \& \ (E) \underset{A}{\Rightarrow} (U).$$

Proof. Let $F, G \subseteq S$ be finite and non-void, a an extremity of F and $G = \{b_1, \ldots, b_n\}$. If FG does not contain any unique product then there exists, for each pair (a, b_i) some pair (a_i, b_j) with $a_i \in F$, $b_j \in G$, $(a_i, b_j) \neq (a, b_i)$ and $ab_i = a_i b_j$. Hence, there exists a mapping ϕ of $\{1, \ldots, n\}$ into itself such that

$$ab_1 = a_1 b_{\phi(1)}, \quad ab_2 = a_2 b_{\phi(2)}, \quad \ldots, \quad ab_n = a_n b_{\phi(n)}$$

where $a \neq a_i$ or $b_i \neq b_{\phi(i)}$. By (C) it follows that both conditions, $a \neq a_i$ and $b_i \neq b_{\phi(i)}$ hold for each i, and the latter means that $\phi(i) \neq i$ for each i. Now, there exists a set $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots n\}$ on which ϕ acts as a cyclic permutation: for instance, the numbers $\phi(1), \phi^2(1), \ldots, \phi^{n+1}(1)$ cannot all be distinct, hence there exists a first r such that $\phi^r(1) = \phi^s(1)$ with some $s < r$ and $\{\phi^s(1), \ldots, \phi^{r-1}(1)\}$ is such a set. Now one obtains

$$a^k b_{i_1} b_{i_2} \ldots b_{i_k} = a_{i_1} a_{i_2} \ldots a_{i_k} b_{\phi(i_1)} b_{\phi(i_2)} \ldots b_{\phi(i_k)}$$

and hence, by the choice of $\{i_1, \ldots, i_k\}$ and by (C),

$a^k = a_{i_1} a_{i_2} \ldots a_{i_k}$. However, a was taken as an extremity of F and, therefore, this leads to $a_{i_1} = \ldots = a_{i_k} = a$ which is a contradiction.

The final step in our argument is $(U) \Rightarrow (NZ)$ which has already been dealt with, and thus $(C) \ \& \ (PC) \underset{A}{\Rightarrow} (NZ)$ is established.

Some further relations between the conditions considered here are:

$$(NZ) \underset{A}{\Rightarrow} (U) \quad , \quad (E) \Rightarrow (PC) \quad , \quad (U) \Rightarrow (C).$$

The first one immediately follows from $(NZ) \underset{A}{\Rightarrow} (C)$ & (PC) and (C) & $(PC) \underset{A}{\Rightarrow} (U)$, the second one is obtained by applying (E) to two-element sets and the last one by applying (U) to sets $\{a, b\}$ and $\{c\}$. For abelian S, one now has that the four conditions (U), (C) & (PC), (C) & (E), (U) & (E) are all equivalent to (NZ), and one wonders whether it might be possible to modify any one of these in order to obtain a condition which is generally equivalent to (NZ). In a similar vein, the implications $(O) \Rightarrow (E)$ & (U) and (E) & $(U) \underset{A}{\Rightarrow} (O)$ raise the question whether (E) & (U), or some modification thereof, might be equivalent with (O), either in general or, perhaps, for a restricted class of S such as groups.

In conclusion, we give, as another application of the notion of extremal elements, a characterization of the additive semi-groups of rational numbers. The condition to be considered here is

(2E) Any finite subset of S of at least two elements has exactly two extremities.

Now one has the proposition

$$(C) \ \& \ (2E) \underset{A}{\Leftrightarrow} S \text{ is isomorphic to a subsemigroup of } Q^{+}.$$

Here, Q^{+} denotes the additive group of the rational field Q.

Proof. Let S be abelian and satisfy (C) and $(2E)$. Since $(2E) \Rightarrow (E) \Rightarrow (PC)$, S is a subsemigroup of a torsion free group G. If rank $G > 1$ there exist independent elements $a, b \in S$. Now, for any $c \in S$, consider $F = \{ac, bc, c\}$. If $(ac)^{k+l} = (bc)^{k} c^{l}$ with $k, l \geq 0$ and $k+l \neq 0$ one has $a^{k+l} = b^{k}$ which either contradicts the independence of a and b or the fact that G is torsion free. Hence, ac and, similarly, bc are extremities of F. Next, if $c^{k+l} = (ac)^{k}(bc)^{l}$ with $k, l \geq 0$ and $k+l \neq 0$ one has $1 = a^{k} b^{l}$ which again is not possible; thus c is also an extremity of F. However, this contradicts $(2E)$ and therefore rank $G = 1$. It follows now from a known theorem that G is isomorphic to a subgroup of Q^{+}, and this

https://doi.org/10.4153/CMB-1961-024-4 Published online by Cambridge University Press

proves the assertion concerning S.

Conversely, let S be a subsemigroup of Q^+ and suppose $F \subseteq S$ has at least three elements a, b and c. Let $a = f/n$, $b = g/n$ and $c = h/n$ with integers f, g, h and n where $n > 0$ and $f < g < h$. Then $(h-f)g = (h-g)f + (g-f)h$ and therefore $(h-f)b = (h-g)a + (g-f)c$ where all coefficients are positive and $h-f = (h-g) + (g-f)$. This shows that b is not an extremity of F. On the other hand, any finite $F \subseteq S$ of at least two elements does have two extremities, namely its least and its greatest element with respect to the natural ordering of Q. Hence, S satisfies (2E).

Hamilton College,
McMaster University

https://doi.org/10.4153/CMB-1961-024-4 Published online by Cambridge University Press