Quasigroups and Related Systems **29** (2021), 171 – 176

On the torsion in multiplicatively closed subsets of power associative algebras

Evgenii L. Bashkirov

Abstract. Let A be a commutative ring with 1, M an ideal of A, E a power associative algebra over A having a basis and a unit element e. In the paper, the torsion in the multiplicatively closed subset $e + ME$ of E has been studied when A is an integral domain of characteristic 0 with a theory of divisors. The main theorem of the paper generalizes a result concerning the torsion in the congruence subgroup of the general linear group over A.

One of the most useful way to study an algebraic system with a single binary operation is to ask whether or not a property satisfied by some class of groups is valid for the system in question. The present short note has its origin in the observation that the results of [4] concerning the torsion in the congruence subgroups of the general linear groups over rings can not only be proved for matrix groups over commutative integral domains that have a theory of divisors (this kind of commutative rings is more general than that considered in [4]) but also can be carried over to some multiplicatively closed sets in power associative algebras over rings belonging to the family indicated. In particular, this features to investigate the torsion in Moufang loops because these are power associative by Moufang's theorem ([3], p. 117). To pose the problem properly as well as to formulate the main result one must, first, introduce and recall some terminology and notation.

Let A be a commutative ring with 1. Let E be an algebra over A with unit element e. If M is an ideal of A, then ME denotes the set of all finite sums $\sum_i a_i x_i$ with $a_i \in M, x_i \in E$. Define $S(M)$ to be the set of all elements $e+x$ where $x \in ME$. Since ME is a two-sided ideal of E, the subset $S(M)$ is multiplicatively closed, that is, the product uv is in $S(M)$ whenever u and v are in $S(M)$.

Hereafter A is assumed to be an integral domain. Recall that the requirement A to have a theory of divisors means that there is a commutative semigroup D with identity and with unique factorization such that there exists a homomorphism $a \mapsto (a)$ of the semigroup $A^* = A \setminus \{0\}$ into D satisfying conditions (1)–(3) listed on p. 171 [2]. In particular, an element $a \in A^*$ is divisible by $b \in A^*$ in the ring A if and only if (a) is divisible by (b) in the semigroup D. Also an element $a \in A^*$ is said to be divisible by an element $\mathfrak{a} \in D$, in symbols $\mathfrak{a}|a$, if (a) is divisible by $\mathfrak{a}$ in

2010 Mathematics Subject Classification: 20N02, 20N05, 17A05, 17D05
Keywords: Power associative algebras; Moufang loops; alternative algebras; commutative rings; congruence subgroups

the semigroup D. Accordingly, the notation $\mathfrak{a} \nmid a$ means that (a) is not divisible by $\mathfrak{a}$ in D. The set of all elements of A that are divisible by $\mathfrak{a}$ form an ideal of A, written $I(\mathfrak{a})$. Under the settings established, the following result is valid.

Theorem. *Let A be a commutative integral domain of characteristic 0 with an identity 1. Suppose that A has a theory of divisors $A^* \to D$ such that D contains a prime element $\mathfrak{P}$ satisfying the following conditions: $\mathfrak{P} \nmid 2$ and $\mathfrak{P}^2 \nmid p$ for every prime rational integer p. Let E be a power associative algebra over A with unit element e. Suppose that the underlying A-module of E is free. Then the set $S(I(\mathfrak{P}))$ contains no element of finite order.*

Proof. Suppose that $S(I(\mathfrak{P}))$ contains an element of finite order other than e. Then it contains an element a of prime order p. Let $a = e + b$ with $b \in I(\mathfrak{P})E$. By the condition of the theorem, the module E admits a basis, say $(e_\lambda)_{\lambda\in\Lambda}$ where Λ is an index set which need not be finite. Write $b = \sum_{\lambda\in\Lambda} b_\lambda e_\lambda$ with all b_λ in A, only a finite number of b_λ being nonzero. Moreover, since $b \in I(\mathfrak{P})E$, all b_λ must be in the ideal $I(\mathfrak{P})$. Now due to the power associativity of the algebra E, one gets

$$a^p = (e+b)^p = e + bp + \frac{p(p-1)}{2!}b^2 + \ldots + b^p = e,$$

whence it follows that

$$pb + \frac{p(p-1)}{2!}b^2 + \ldots + b^p = 0. \tag{1}$$

For any integer $t \geqslant 1$, write

$$b^t = \sum_{\lambda\in\Lambda} b_\lambda^{(t)} e_\lambda, \quad b_\lambda^{(t)} \in A, \tag{2}$$

where certainly $b_\lambda^{(1)} = b_\lambda$ for each $\lambda \in \Lambda$. If t ranges from 1 through p, then equations (2) contains only a finite number of nonzero coefficients $b_\lambda^{(t)}$ and, in fact, a finite number of basis elements e_λ. Therefore the set of all indices λ occurring in (2) with t ranging from 1 through p is finite and so it can be identified with the set of positive integers $\{1, 2, \ldots, n\}$ for an appropriate n. Thus equations (2) with $t \in \{1, 2, \ldots, p\}$ can be rewritten as

$$b^t = \sum_{i=1}^{n} b_i^{(t)} e_i. \tag{3}$$

Since each $b_i = b_i^{(1)}$ is divisible by $\mathfrak{P}$ (it should be kept in mind that the zero element of A is supposed to be divisible by all elements of D), one can find an integer $l \geqslant 1$ such that $\mathfrak{P}^l$ divides all $b_1, \ldots, b_n$ while $\mathfrak{P}^{l+1}$ does not divide some $b_j (j \in \{1, 2, \ldots, n\})$. This means that

$$(b_j) = \mathfrak{P}^l \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}, \tag{4}$$

where $r \geqslant 0$, m_i are positive integers and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime elements of D such that

$$\mathfrak{P} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}. \tag{5}$$

On substituting (3) into (1), one obtains

$$p\sum_{i=1}^{n} b_i e_i + \frac{p(p-1)}{2!}\sum_{i=1}^{n} b_i^{(2)} e_i + \ldots + \sum_{i=1}^{n} b_i^{(p)} e_i = 0.$$

Matching the coefficients of e_j gives the equation

$$pb_j = -\sum_{i=2}^{p-1} \frac{p(p-1)\ldots(p-i+1)}{i!} b_j^{(i)} - b_j^{(p)}. \tag{6}$$

There are two possibilities to consider: (a) $\mathfrak{P} \nmid p$; (b) $\mathfrak{P}|p$.

Consider (a). Assume first that $\mathfrak{P}^{l+1}|pb_j$. This assumption means that

$$(pb_j) = \mathfrak{P}^{l+u}\mathfrak{q}_1^{k_1}\ldots\mathfrak{q}_s^{k_s}. \tag{7}$$

for some integers $u \geqslant 1, s \geqslant 0$, some positive integers k_i and some prime elements $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in D$ different from $\mathfrak{P}$. In view of (4),

$$(pb_j) = (p)\mathfrak{P}^l\mathfrak{p}_1^{m_1}\ldots\mathfrak{p}_r^{m_r}. \tag{8}$$

Equations (8) and (7) are combined to yield

$$(p)\mathfrak{p}_1^{m_1}\ldots\mathfrak{p}_r^{m_r} = \mathfrak{P}^u\mathfrak{q}_1^{k_1}\ldots\mathfrak{q}_s^{k_s}. \tag{9}$$

Here $u \geqslant 1$, so $\mathfrak{P}$ arises on the right-hand side of (9) and consequently it must coincide with some of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ which is false by (5). This shows that $\mathfrak{P}^{l+1} \nmid pb_j$. On the other hand for each $i = 2, \ldots, p$, $\mathfrak{P}^{li}$ divides $b_j^{(i)}$, and hence $\mathfrak{P}^{l+1}$ divides all $b_j^{(2)}, \ldots, b_j^{(p)}$. Thus $\mathfrak{P}^{l+1}$ divides each summand on the right-hand side of (6), and therefore $\mathfrak{P}^{l+1}|pb_j$. This contradiction shows that possibility (a) is in fact impossible.

Consider (b). Assume first that $\mathfrak{P}^{l+2}|pb_j$. In other words,

$$(pb_j) = \mathfrak{P}^{l+v}\mathfrak{r}_1^{d_1}\ldots\mathfrak{r}_t^{d_t}, \tag{10}$$

where $v \geqslant 2$, all d_i are positive integers and $\mathfrak{r}_1, \ldots, \mathfrak{r}_t (t \geqslant 0)$ are prime elements of D different from $\mathfrak{P}$. By the condition of the theorem, $\mathfrak{P}^2 \nmid p$, and hence

$$(p) = \mathfrak{P}\mathfrak{q}_1^{k_1}\ldots\mathfrak{q}_s^{k_s}, \tag{11}$$

where k_i are positive integers and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s (s \geqslant 0)$ are prime elements of D such that

$$\mathfrak{P} \notin \{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}. \tag{12}$$

Further, by (4) and (11),

$$(p)(b_j) = \mathfrak{P}^{1+l}\mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r},$$

and comparing the last relation with (10), one concludes, after cancelling $\mathfrak{P}^l$, that

$$\mathfrak{P}^v\mathfrak{r}_1^{d_1}\dots\mathfrak{r}_t^{d_t} = \mathfrak{P}\mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r}.$$

Since $v \geqslant 2$, the last equation can be rewritten as

$$\mathfrak{P}^{v-1}\mathfrak{r}_1^{d_1}\dots\mathfrak{r}_t^{d_t} = \mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r},$$

where $v-1 \geqslant 1$, and so $\mathfrak{P}$ must occur on the right-hand side of the last equality which is impossible in view of (12) and (5). Thus the assumption $\mathfrak{P}^{l+2}|pb_j$ has led to a contradiction, and therefore, $\mathfrak{P}^{l+2} \nmid pb_j$, or, to put it another way, $\mathfrak{P}^{l+2}$ is not a divisor of the left-hand side of (6). On the other hand, if $2 \leqslant i \leqslant p-1$, the element

$$\frac{p(p-1)\dots(p-i+1)}{i!}b_j^{(i)}$$

of A has $\mathfrak{P}(\mathfrak{P}^l)^i = \mathfrak{P}^{1+li}$ as a divisor, and so $\mathfrak{P}^{l+2}$ is its divisor too. Also $\mathfrak{P}^{lp}|b_j^{(p)}$. Now notice that $p > 2$ due to the assumption $\mathfrak{P}|p$ defining possibility (b) and in view of the relation $\mathfrak{P} \nmid 2$ which is true by the condition of the theorem. Therefore, one has $lp \geqslant l+2$, and consequently $\mathfrak{P}^{l+2}|b_j^{(p)}$. Thus every term on the right-hand side of (6) has $\mathfrak{P}^{l+2}$ as a divisor, and hence $\mathfrak{P}^{l+2}$ divides the entire expression on the right-hand side of (6). This final contradiction completes the proof. □

As a special case of the preceding theorem, the following assertion dealing with general alternative algebras deserves to be formulated.

Corollary 1. *Let A, E and $\mathfrak{P}$ be as in Theorem. Suppose that the algebra E is alternative. Then the set of invertible elements of E that are contained in $S(I(\mathfrak{P}))$ is a Moufang loop without torsion.*

Proof. By [1], p. 81, the set of invertible elements in E is a Moufang loop. So having in view Theorem, it suffices to show that for any invertible $x \in S(I(\mathfrak{P}))$, its inverse x^{-1} is also in $S(I(\mathfrak{P}))$. Now one can write $x^{-1} = e+b$ with $b \in E$. Recalling that $x = e+a$ with $a \in I(\mathfrak{P})E$, one has $e = xx^{-1} = (e+a)(e+b) = e+a+b+ab$, whence $b = -a-ab$. But $I(\mathfrak{P})E$ is a two-sided ideal of E, and so b must lie in $I(\mathfrak{P})E$ as required. □

To obtain an application of Theorem in a more concrete situation of the split Cayley-Dickson algebra $O(A)$ as well as in the case of associative matrix algebras, the following portion of notation is needed.

The set $O(A)$ is formed by all symbols $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ such that $a, b \in A$ and $\alpha, \beta \in A^3$, where A^3 is the rank 3 free A-module of length 3 columns with components in A. In $O(A)$, equality, addition and multiplication by elements of A are fulfilled

componentwise so that $O(A)$ is a free A-module of rank 8. The operation of multiplication in $O(A)$ is defined by

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}$$
$$(a, b, c, d \in A, \alpha, \beta, \gamma, \delta \in A^3),$$

where $\cdot$ and $\times$ denote the usual dot product and crossed product, respectively, in A^3. This makes $O(A)$ a non-associative alternative algebra over A. The algebra $O(A)$ is called the (split) octonion (or Cayley–Dickson) algebra over A, and its elements $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ are called octonions. The identity of the algebra $O(A)$ is the octonion $\left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{smallmatrix}\right)$, where $\mathbf{0}$ denotes the element of A^3 all of whose components are zeros. The Moufang loop of invertible elements of $O(A)$ is denoted $G(A)$.

Now let M be an ideal of A. It is a straightforward verification that the canonical homomorphism $f_M \colon A \to A/M = B$ can be extended to an epimorphism of alternative rings $h_M \colon O(A) \to O(B)$,

$$\left(\begin{array}{c|c} a_1 & \begin{bmatrix} a_2 \\ a_3 \\ a_4 \end{bmatrix} \\ \hline \begin{bmatrix} a_5 \\ a_6 \\ a_7 \end{bmatrix} & a_8 \end{array}\right) \mapsto \left(\begin{array}{c|c} f_M(a_1) & \begin{bmatrix} f_M(a_2) \\ f_M(a_3) \\ f_M(a_4) \end{bmatrix} \\ \hline \begin{bmatrix} f_M(a_5) \\ f_M(a_6) \\ f_M(a_7) \end{bmatrix} & f_M(a_8) \end{array}\right).$$

This h_M determines, in turn, a loop homomorphism $g_M \colon G(A) \to G(B) \colon x \mapsto h_M(x)$. The kernel of g_M, denoted $CL(A, M)$, will be termed the *M-congruence subloop* by analogy with the corresponding concept in the theory of matrix groups (see [4], p. 65) and it is appropriate to recall this concept here.

First, if $n \geqslant 2$ and R is an associative ring with identity, then the group of all invertible $n \times n$ matrices over R is denoted by $GL(n, R)$ and called the general linear group (of degree n over R). Now the canonical homomorphism f_M determines the group homomorphism $\beta_M \colon GL(n, A) \to GL(n, B)$ which sends a matrix $a \in GL(n, A)$ whose element in row i, column j is denoted $a_{ij} (1 \leqslant i, j \leqslant n)$ to the matrix of $GL(n, B)$ whose element in row i, column j is equal to $f_M(a_{ij})$. The kernel of β_M is just the M-congruence subgroup $GL(n, A, M)$.

Corollary 2. *Let A and $\mathfrak{P}$ be such as in Theorem. Let n be an integer, $n \geqslant 3$. Then the $I(\mathfrak{P})$-congruence subloop $C(A, I(\mathfrak{P}))$ as well as the $I(\mathfrak{P})$-congruence subgroup $CL(n, A, I(\mathfrak{P}))$ are torsion free.*

Proof. Note that the subloop $C(A, I(\mathfrak{P}))$ (the subgroup $CL(n, A, I(\mathfrak{P}))$, respectively) coincides with the set of invertible elements in the multiplicatively closed subset $S(I(\mathfrak{P}))$ of the algebra $O(A)$ (the algebra of $n \times n$ matrices over A, respectively). Using Corollary 1 completes the proof. □

References

[1] *Alternative loop rings*, Edited by E.G. Goodaire, E. Jespers, C.P. Milies, North Holland Math. Studies, (1996).

[2] **Z.I. Borevich, I.R. Shafarevich**, *Number theory*, Academic Press, New York, (1966).

[3] **R.H. Bruck**, *A survey of binary systems*, Springer, New York, (1971).

[4] **D.A. Suprunenko**, *Matrix groups*, Transl. Math. Monographs, **45**, Amer. Math. Soc., Providence, Rhode Island, (1976).

Received July 29, 2021

Kalinina str 25, ap. 24
220012 Minsk
Belarus
e-mail: zh.bash@mail.ru