International Journal of Pure and Applied Mathematics
Volume 112 No. 4 2017, 763-775
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: 10.12732/ijpam.v112i4.8
ijpam.eu

ON $\mathbb{Z}_p$-INVOLUTION

Ameer Jaber[1 §], Hamed M. Obiedat[2], Ibrahim Abu Falahah[3]
[1,2,3]Department of Mathematics
The Hashemite University
Zarqa, 13115, JORDAN

Abstract: Our main purpose is to study the existence of $\mathbb{Z}_p$-involution on central simple $\mathbb{Z}_p$-algebras. Then we define a $\mathbb{Z}_3$-involution on a central simple $\mathbb{Z}_3$-algebra.

AMS Subject Classification: 16W10
Key Words: central simple $\mathbb{Z}_p$-algebras, $\mathbb{Z}_p$-involutions, division $\mathbb{Z}_p$-algebras

1. Introduction

The existence of superinvolution on associative superalgebras was studied by many authors, for example Michel Racine in [5] and A.Elduque and O. Villa in [1] studied superalgebras, which are $\mathbb{Z}_2$-graded algebras, and existence of superinvolutions on finite dimensional central simple superalgebras, and they found that non-trivial central division superalgebras are never endowed with superinvolution of the first kind, but they prove the graded version of the classical Albert and Albert-Riehm Theorem of existence of superinvolution of the second kind.

Continuing on the studying of superalgebras, in [2] we developed the theory of existence of pseudo-superinvolutions of the first kind on finite dimensional central simple associative superalgebras over a field K of characteristic not 2. We proved that a central division superalgebra $\mathcal{D}$, over a field K of characteristic

Received: October 28, 2016
Revised: December 19, 2016
Published: February 16, 2017

§Correspondence author

not 2, of even type has a pseudo-superinvolution of the first kind if and only if $\mathcal{D}$ is of order 2 in the Brauer-Wall group BW(K).

Moreover we proved that if $\mathcal{D}$ is of type then $\mathcal{D}$ has a pseudo-superinvolution of the first kind if and only if $\sqrt{-1} \in K$ and $\mathcal{D}$ is of order 2 in the Brauer-Wall group BW(K).

Let p be any prime number. An *associative* $\mathbb{Z}_p$-ring $R = \bigoplus_{i=0}^{p-1} R_i$ is nothing but a $(\mathbb{Z}/p\mathbb{Z})$-graded *associative* ring. A $(\mathbb{Z}/p\mathbb{Z})$-graded ideal $I = \bigoplus_{i=0}^{p-1} I_i$ of an associative $\mathbb{Z}_p$-ring R is called a $\mathbb{Z}_p$*-ideal* of R. An associative $\mathbb{Z}_p$-ring R is *simple* if it has no non-trivial $\mathbb{Z}_p$-ideals. An *associative* $\mathbb{Z}_p$-ring R is a commutative $\mathbb{Z}_p$-ring if

$$a_\alpha b_\beta = (-1)^{\alpha\beta} b_\beta a_\alpha \quad \forall a_\alpha \in R_\alpha,\ b_\beta \in R_\beta,$$

where the product $\alpha\beta$ is taken modulo p. We will say that such elements $\mathbb{Z}_p$-commute.

Let R be an associative $\mathbb{Z}_p$-ring with $1 \in R_0$, then R is said to be a *division* $\mathbb{Z}_p$-ring if all nonzero homogeneous elements are invertible, i.e., every $0 \neq r_\alpha \in R_\alpha$ has an inverse r_α^{-1}, necessarily in $R_{p-\alpha}$, where the subscript $p-\alpha$ is taken modulo p.

Let K be a field of characteristic 0. An *associative* $(\mathbb{Z}/p\mathbb{Z})$-graded K-algebra $\mathcal{A} = \bigoplus_{i=0}^{p-1} \mathcal{A}_i$ is a *finite dimensional central simple* $\mathbb{Z}_p$-algebra over a field K, if $Z(\mathcal{A}) \cap \mathcal{A}_0 = K$, where $Z(\mathcal{A}) = \{a \in \mathcal{A} \mid ab = ba \ \forall\ b \in \mathcal{A}\}$ is the *center* of $\mathcal{A}$, and the only $\mathbb{Z}_p$-ideals of $\mathcal{A}$ are (0) and $\mathcal{A}$ itself.

In Section 2 we prove the structure theory of $\mathbb{Z}_p$-division algebra, where p is a prime number, which is a restate of Division Superalgebra Theorem, see [6, P. 438].

In Section 3 we define the $\mathbb{Z}_p$-involution on $\mathbb{Z}_p$-algebras, then we prove that a central simple $\mathbb{Z}_p$-algebra $\mathcal{A} = M_n(\mathcal{D})$ over a field K, where $\mathcal{D}$ is a division $\mathbb{Z}_p$-algebra with $\mathcal{D}_1 \neq \{0\}$, has a $\mathbb{Z}_p$-involution if and only if $\mathcal{D}$ has. Also we prove that if a central simple $\mathbb{Z}_p$-algebra $\mathcal{A} = M_n(\mathcal{D})$ over a field K, where $\mathcal{D}$ is a division algebra with $\mathcal{D}_j = \{0\}$ for all $1 \leq j \leq p-1$ has a $\mathbb{Z}_p$-involution then $\mathcal{D}$ has.

2. Division $\mathbb{Z}_p$-Algebra

We start this work by proving a structure theorem on $\mathbb{Z}_p$-division algebras which is a restate of Division Superalgebra Theorem, see [6, P. 438], but first we need the following lemma. The proof of this lemma is exactly the same as the proof of [4, Lemmata 3,5].

Lemma 2.1. *Let p be a prime number. If $\mathcal{A} = \bigoplus_{i=0}^{p-1} \mathcal{A}_i$ is a central simple unital $\mathbb{Z}_p$-algebra over K then either $\mathcal{A}$ is simple as an algebra or $\mathcal{A}_0$ is simple and $\mathcal{A}_i = \mathcal{A}_0 u^i$, with $u \in Z(\mathcal{A}) \cap \mathcal{A}_1$ and $u^p = 1$.* □

Theorem 2.2 (Division $\mathbb{Z}_p$-algebra Theorem)**.** *If $\mathcal{D} = \bigoplus_{i=0}^{p-1} \mathcal{D}_i$ is a finite dimensional central division $\mathbb{Z}_p$-algebra over the field K of characteristic 0, then exactly one of the following holds where throughout $\mathcal{C}$ denotes a central division algebra over K and $\omega \in K$ denotes a primitive pth root of unity.*

(i) $\mathcal{D} = \mathcal{D}_0 = \mathcal{C}$, i.e., $\mathcal{D}_i = \{0\}$ for all $1 \le i \le p-1$.

(ii) $\mathcal{D} = \mathcal{C} \otimes_K K[u]$, $u^p = \lambda \in K^\times$, $\mathcal{D}_0 = \mathcal{C} \otimes_K K$, $\mathcal{D}_i = \mathcal{C} \otimes_K K u^i$ for all $1 \le i \le p-1$.

(iii) $\mathcal{D} = \mathcal{C}$, $\mathcal{D}_0 = C_{\mathcal{D}}(u)$, the centralizer of u in $\mathcal{C}$,

$$\mathcal{D}_i = \{c \in \mathcal{D} \ : \ cu = \sigma^i(u)c\} \ \forall 1 \le i \le p-1,$$

for some Galois extension $K[u] \subset \mathcal{C}$ of order p with Galois automorphism σ.

(iv) $\mathcal{D} = M_p(\mathcal{C}) = \mathcal{C} \otimes_K M_p(K)$,
$\mathcal{D}_0 = \mathcal{C} \otimes_K K[u]$, $\mathcal{D}_i = \mathcal{C} \otimes_K K[u]W^i$, $\quad \forall 1 \le i \le p-1$, where

$$u = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & \vdots & \vdots & \ddots & 1 \\ \lambda & 0 & 0 & \cdots & 0 \end{bmatrix},$$

$$W = \begin{bmatrix} 1 & & & & & \\ & \omega & & & & \\ & & \omega^2 & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & \omega^{p-1} \end{bmatrix},$$

where $\lambda \notin K^p$.

Proof. Let $\mathcal{D} = \bigoplus_{i=0}^{p-1} \mathcal{D}_i$ be a central division $\mathbb{Z}_p$-algebra over K, and let $\mathcal{D}_1 \neq \{0\}$, then $\mathcal{D}_i \neq \{0\}$ $\forall 2 \le i \le p-1$. If $0 \neq v \in \mathcal{D}_1$, then $\mathcal{D}_0 v^i \subseteq \mathcal{D}_i =$

$\mathcal{D}_i v^{-i} v^i \subseteq \mathcal{D}_0 v^i$. Therefore, for any $1 \leq i \leq p-1$ and for any $0 \neq v \in \mathcal{D}_1$ we have that $\mathcal{D}_i = \mathcal{D}_0 v^i$.

For any $a \in \mathcal{D}_0$, $va = a^{\psi_v} v$, where $a^{\psi_v} = vav^{-1}$, and $\psi_v|_{\mathcal{D}_0}$ is an automorphism of $\mathcal{D}_0$ as an algebra over $K = Z(\mathcal{D}) \cap \mathcal{D}_0$. Since any element of $\mathcal{D}_1$ is of the form $c_0 v$, $c_0 \in \mathcal{D}_0$, the restriction of ψ_v to $Z(\mathcal{D}_0)$ does not depend on the particular choice of $v \in \mathcal{D}_1$. Assume first that $\psi_v|_{\mathcal{D}_0}$ is an inner automorphism of $\mathcal{D}_0$, say $\psi_v|_{\mathcal{D}_0} = \psi_c$, where $c \in \mathcal{D}_0$ (up to multiplication by an element of $Z(\mathcal{D}_0)$). Therefore $vav^{-1} = cac^{-1}$ implies that $c^{-1}vav^{-1}c = a$ for all $a \in \mathcal{D}_0$. Letting $u = c^{-1}v \in \mathcal{D}_1$ then $u^{-1} \in \mathcal{D}_{p-1}$ and $uau^{-1} = a$ for all $a \in \mathcal{D}_0$, so u centralizes $\mathcal{D}_0$. Since $\mathcal{D}_i = \mathcal{D}_0 u^i$ $\forall 1 \leq i \leq p-1$, u centralizes $\mathcal{D}_i$ $\forall 1 \leq i \leq p-1$. Thus $u \in Z(\mathcal{D})$ and $u^p \in Z(\mathcal{D}) \cap \mathcal{D}_0$, say $u^p = \lambda \in K^\times$. Letting $\mathcal{C} = \mathcal{D}_0$, $\mathcal{D} = \mathcal{C} \otimes_K K[u]$. Note that $\mathcal{D}$ is simple as an algebra if and only if $\lambda \notin K^p$. If $\lambda \in K^p$, we may assume that $\lambda = 1$. This is the only case where $\mathcal{D}$ is not simple as an algebra.

Assume next that $\sigma = \psi_v|_{\mathcal{D}_0}$ is not an inner automorphism of $\mathcal{D}_0$ over K. If σ is not the identity then K is the fixed subfield of $Z(\mathcal{D}_0)$, which implies that $Z(\mathcal{D}_0)$ is a Galois extension of K of order p with Galois automorphism σ. We may choose $u \in Z(\mathcal{D}_0)$ such that $Z(\mathcal{D}_0) = K[u]$, $u^p = \lambda \notin K^p$ with $\sigma(u) \neq u \in K[u]$. Now, $(av)u = a\sigma(u)v = \sigma(u)(av)$ implies that $\sigma(vu) = v\sigma(u) = \sigma(\sigma(u)v) = \sigma^2(u)v$ and hence $av^2u = av\sigma(u)v = a(v\sigma(u))v = a(\sigma^2(u)v)v = \sigma^2(u)(av^2)$ for all $a \in \mathcal{D}_0$. We prove that $av^iu = a\sigma^i(u)v^i$ for all $a \in \mathcal{D}_0$ and for all $2 \leq i \leq p-1$ by induction on i. Note that it is true for $i = 1, 2$. Suppose that $av^{i-1}u = \sigma^{i-1}(u)(av^{i-1})$ for all $a \in \mathcal{D}_0$. Then $av^iu = av(v^{i-1}u) = av(\sigma^{i-1}(u)v^{i-1}) = av\sigma^{i-1}(u)v^{-1}v^i = a\sigma^i(u)v^i$. Therefore $\mathcal{D}_0 = C_{\mathcal{D}}(u)$, the centralizer of u in $\mathcal{D}$ and for $1 \leq i \leq p-1$ we have $\mathcal{D}_i = \{c \in \mathcal{D} : cu = \sigma^i(u)c\} = \mathcal{D}_0 v^i$. If $\mathcal{D}$ is a division algebra then $\mathcal{D} = \bigoplus_{i=0}^{p-1} \mathcal{D}_i$ as above.

If $\mathcal{D}$ is not a division algebra then since $\mathcal{D}_0$ is not central simple over $K = Z(\mathcal{D}) \cap \mathcal{D}_0$ then, by Lemma 2.1, $\mathcal{D}$ is a central simple algebra over K. Let $J \neq \{0\}$ be a right ideal of $\mathcal{D}$. If $0 \neq \Sigma_{i=0}^{p-1} a_i \in J$ then at least one of $a_i \neq 0$ and multiplying by a_i^{-1} on the right, $1 + \Sigma_{i=1}^{p-1} b_i \in J$ for some $b_i \in \mathcal{D}_i$, $1 \leq i \leq p-1$. Hence $(1 + \Sigma_{i=1}^{p-1} b_i)\mathcal{D} \subseteq J$. If J contains an element $0 \neq \Sigma_{i=0}^{p-1} a_i' \notin (1 + \Sigma_{i=1}^{p-1} b_i)\mathcal{D}$ then arguing as above, we obtain an element $1 + \Sigma_{i=1}^{p-1} b_i' \in J$, $\Sigma_{i=1}^{p-1} b_i' \neq \Sigma_{i=1}^{p-1} b_i$. In that case $0 \neq \Sigma_{i=1}^{p-1}(b_i - b_i') \in J$, where $b_i - b_i' \in \mathcal{D}_i$ for all $1 \leq i \leq p-1$. If $b_j - b_j' \neq 0$ for some $1 \leq j \leq p-1$, then multiplying $\Sigma_{i=1}^{p-1}(b_i - b_i')$ by $(b_j - b_j')^{-1}$, we get that $1 + c \in J$ and we may assume that $c = \Sigma_{i=1}^{p-2} c_i$. If $c = 0$ then $J = \mathcal{D}$. If $c \neq 0$ and J contains an element $0 \neq \Sigma_{i=0}^{p-1} a_i'' \notin (1 + c)\mathcal{D}$, then arguing as above, we obtain an element $1 + c' \in J$, $c' \neq c$. Thus $0 \neq \Sigma_{i=1}^{p-2}(c_i - c_i') \in J$ and so there exists $1 \le j \le p-2$ such that $c_j - c'_j \neq 0$. Multiplying $\Sigma_{i=1}^{p-2}(c_i - c'_i)$ by $(c_j - c'_j)^{-1}$, we get that $1 + d \in J$, and we may assume that $d = \Sigma_{i=1}^{p-3} d_i$. Continuing as above to obtain $1 + f_1 \in J$, where $f_1 \in \mathcal{D}_1$. If $f_1 = 0$ then $J = \mathcal{D}$. If $f_1 \neq 0$ and J contains an element $0 \neq \Sigma_{i=0}^{p-1} a''_i \notin (1 + f_1)\mathcal{D}$, then arguing as above, we obtain an element $1 + f'_1 \in J$, where $f'_1 \in \mathcal{D}_1$ and $f'_1 \neq f_1$. In that case $0 \neq f_1 - f'_1 \in J$ and hence $1 \in J$ which must be the whole of $\mathcal{D}$. Therefore a descending chain of nonzero right ideals in $\mathcal{D}$ has length at most p and $\mathcal{D}$ is isomorphic to $M_p(\mathcal{C})$, where $\mathcal{C}$ is a central division algebra over K. If $K[u]$ were to embed in $\mathcal{C}$ then $\mathcal{D}_0 = C_{\mathcal{D}}(u) \supseteq M_p(\mathcal{C})$ which is not a division algebra. Therefore $K[u]$ does not embed in $\mathcal{C}$ but rather the algebraic extension $K[u]$ of order p embeds in $M_p(K)$ and u, W can be chosen as $u = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ 0 & \vdots & \vdots & \ddots & 1 \\ \lambda & 0 & 0 & \cdots & 0 \end{bmatrix}$, $W = \begin{bmatrix} 1 & & & & & \\ & \omega & & & & \\ & & \omega^2 & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & \omega^{p-1} \end{bmatrix}$, $\lambda \notin K^p$ where $\mathcal{D}_0 = \mathcal{C} \otimes_K K[u]$, $\mathcal{D}_i = \mathcal{C} \otimes_K K[u]W^i \forall 1 \le i \le p-1$. □

3. $\mathbb{Z}_p$-Involution on $\mathbb{Z}_p$-Algebra

Definition 1. A $\mathbb{Z}_p$-involution of an associative $\mathbb{Z}_p$-algebra $\mathcal{A}$ is a graded additive map $* : \mathcal{A} \to \mathcal{A}$ such that

$$a^{**} = a \quad \text{and} \quad (a_\alpha b_\beta)^* = (-1)^{\alpha\beta} b_\beta^* a_\alpha^*.$$

Let $V = \bigoplus_{i \in \mathbb{Z}_p} V_i$ be a (left) $\mathbb{Z}_p$-space over a division $\mathbb{Z}_p$-algebra $\mathcal{C}$ and $W = \bigoplus_{i \in \mathbb{Z}_p} W_i$ a right $\mathbb{Z}_p$-space over $\mathcal{C}$. A bilinear pairing $(\ ,\ )_\nu$ is a biadditive map $(\ ,\ )_\nu : V \times W \to \mathcal{C}$ satisfying

$$(v_\alpha, w_\beta)_\nu \in \mathcal{C}_{\alpha+\beta+(p-1)\nu}, \qquad (c_\gamma v_\alpha, w_\beta)_\nu = c_\gamma (v_\alpha, w_\beta)_\nu,$$

$$(v_\alpha, w_\beta c_\gamma)_\nu = (v_\alpha, w_\beta)_\nu c_\gamma,$$

for all $v_\alpha \in V_\alpha$, $w_\beta \in W_\beta$ and $c_\gamma \in \mathcal{C}_\gamma$. The bilinear pairing $(\ ,\ )_\nu$ is *nondegenerate* if

$$(v_\alpha, W)_\nu = \{0\} \Rightarrow v_\alpha = 0 \quad \text{and} \quad (V, w_\beta)_\nu = \{0\} \Rightarrow w_\beta = 0.$$

If $(\ ,\ )_\nu$ is nondegenerate we say that the $\mathbb{Z}_p$-paces V and W are *dual*.

The right $\mathbb{Z}_p$-space W over $\mathcal{C}$ may be viewed as a (left) $\mathbb{Z}_p$-space over $\mathcal{C}^{op}$ via

$$c_\gamma w_\beta := (-1)^{\beta\gamma} w_\beta c_\gamma.$$

An element $a_\alpha \in \mathrm{End}_{\mathcal{C}}(V)_\alpha$ (acting from the right) is said to have an *adjoint* $a^*_\alpha \in \mathrm{End}_{\mathcal{C}^\circ}(W)_\alpha$ (acting from the right) if

$$(v_\beta a_\alpha, w_\delta)_\nu = (-1)^{\alpha\delta}(v_\beta, w_\delta a^*_\alpha)_\nu, \qquad \forall v_\beta \in V_\beta,\ w_\delta \in W_\delta.$$

Therefore if $\mathcal{D}$ is a division $\mathbb{Z}_p$-algebra and σ is an antiautomorphism of $\mathcal{D}$, then it is an isomorphism of $\mathcal{D}$ onto $\mathcal{D}^{op}$ and a right $\mathbb{Z}_p$-space W over $\mathcal{D}^{op}$ is a left $\mathbb{Z}_p$-space over $\mathcal{D}$ under the action

$$d_\delta w_\beta := (-1)^{\delta\beta} w_\beta d^\sigma_\delta, \qquad d_\delta \in \mathcal{D}_\delta,\ w_\beta \in W_\beta.$$

Thus, $(\ ,\ )_\nu : V \times W \to \mathcal{D}$ is a *sesquilinear pairing* of (left) $\mathbb{Z}_p$-spaces over $\mathcal{D}$, i.e.,

$$\begin{aligned} (d_\delta v_\alpha, w_\beta)_\nu &= d_\delta (v_\alpha, w_\beta)_\nu, \\ (v_\alpha, d_\delta w_\beta)_\nu &= (-1)^{\beta\delta}(v_\alpha, w_\beta)_\nu d^\sigma_\delta \end{aligned}$$

for all $v_\alpha \in V_\alpha,\ w_\beta \in W_\beta,\ d_\delta \in \mathcal{D}_\delta$. If $^-$ is a $\mathbb{Z}_p$-involution of $\mathcal{D}$ then $\mathcal{D}$ is isomorphic to $\mathcal{D}^{op}$ and we may consider sesquilinear pairings of $V \times V$. If $\epsilon \in Z(\mathcal{D})$ with $\epsilon\bar{\epsilon} = 1$, an ϵ-*hermitian* $\mathbb{Z}_p$-form is a sesquilinear pairing satisfying

$$(v_\alpha, w_\beta)_\nu = (-1)^{\alpha\beta}\epsilon\overline{(w_\beta, v_\alpha)_\nu}, \qquad \forall v_\alpha \in V_\alpha,\ w_\beta \in V_\beta.$$

If $\epsilon = 1$ (respectively, -1), $(\ ,\ )_\nu$ is said to be *hermitian* (respectively, *skewhermitian*).

Theorem 3.1. *A nondegenerate symmetric $\mathbb{Z}_p$-form $(\ ,\ )$ $(\nu = 0)$ on a finite dimensional $\mathbb{Z}_p$-space V over a field K, induces a $\mathbb{Z}_p$-involution $*$ on $\mathrm{End}_K V$ via*

$$(v_i a_k, v_j) = (-1)^{kj}(v_i, v_j a^*_k)\ \forall v_i, v_j \in V.$$

proof. Let a_α, b_β be homogeneous elements in $\mathrm{End}_K V$, then

$$\begin{aligned} (v_i a_\alpha b_\beta, v_j) &= (-1)^{(\alpha+\beta)j}(v_i, v_j(a_\alpha b_\beta)^*) \\ &= (-1)^{\beta j}(v_i a_\alpha, v_j b^*_\beta) \\ &= (-1)^{\alpha(\beta+j)}(-1)^{\beta j}(v_i, v_j b^*_\beta a^*_\alpha), \end{aligned}$$

and hence $(-1)^{(\alpha+\beta)j}(v_i, v_j(a_\alpha b_\beta)^*) = (-1)^{\alpha(\beta+j)}(-1)^{\beta j}(v_i, v_j b_\beta^* a_\alpha^*)$. Since $\mathbb{Z}_p$ is a field, we have that

$$\begin{aligned}\alpha(\beta+j)(\bmod p) + \beta j(\bmod p) &= \alpha(\beta+j) + \beta j(\bmod p) \\ &= (\alpha+\beta)j + \alpha\beta(\bmod p).\end{aligned}$$

Thus $(a_\alpha b_\beta)^* = (-1)^{\alpha\beta} b_\beta^* a_\alpha^*$ which implies that $*$ is a $\mathbb{Z}_p$-involution on $\mathrm{End}_K V$. □

Now we are able to prove the main result in this work.

Theorem 3.2. *A primitive $\mathbb{Z}_p$-ring $\mathcal{A}$ with a minimal right $\mathbb{Z}_p$-ideal has a $\mathbb{Z}_p$-involution $*$ if and only if $\mathcal{A}$ has a selfdual right $\mathbb{Z}_p$-module I, the commuting $\mathbb{Z}_p$-ring $\mathcal{C}$ of $\mathcal{A}$ on I has a $\mathbb{Z}_p$-involution, and $*$ is the adjoint with respect to a non-degenerate hermitian or skewhermitian $\mathbb{Z}_p$-form on I.*

Proof. Assume that there is a minimal right $\mathbb{Z}_p$-ideal I and an homogeneous element $a_i \in I_i$ such that $a_i a_i^* I \neq \{0\}$. Then take $x = a_i a_i^* \in I$ and note that $x^* = (-1)^{i^2} x$. By [3, Theorem 3.9] there is a primitive idempotent $e \in I_0$ with $I = e\mathcal{A}$ and $xe = ex = x$. Therefore, $xee^* = xe^* = (-1)^{i^2} x^* e^* = (-1)^{i^2}(ex)^* = (-1)^{i^2} x^* = x$. Then, as in the proof of [3, Theorem 3.9], $f = ee^*$ is an idempotent, with $f^* = f$ and $I = f\mathcal{A}$. So $\mathcal{D} = f\mathcal{A}f$ is a division $\mathbb{Z}_p$-algebra with $\mathbb{Z}_p$-involution $^- = *|_{\mathcal{D}}$ and the right $\mathbb{Z}_p$-ideal $V = f\mathcal{A}$ is a left $\mathbb{Z}_p$-space over $\mathcal{D}$. For $v_i = fa_i \in V_i$, $w_j = fb_j \in V_j$, define

$$(v_i, w_j)_0 := fa_i(fb_j)^* = fa_i b_j^* f \in \mathcal{D}_{i+j},$$

one checks that for all $d_k \in \mathcal{D}_k$, $v_i \in V_i$, $w_j \in V_j$,

$$(d_k v_i, w_j)_0 = d_k(v_i, w_j)_0, \quad (v_i, d_k w_j)_0 = (-1)^{kj}(v_i, w_j)_0 \bar{d}_k,$$

$$\overline{(v_i, w_j)}_0 = (-1)^{ij}(w_j, v_i)_0,$$

that V is self dual with respect to $(\, , \,)_0$, and that $*$ is the adjoint with respect to the hermitian $\mathbb{Z}_p$-form $(\, , \,)_0$.

Otherwise, for any minimal right $\mathbb{Z}_p$-ideal I of $\mathcal{A}$, and any homogeneous element $a \in I$, $aa^*I = \{0\}$ holds. Take a minimal right $\mathbb{Z}_p$-ideal I of $\mathcal{A}$ and assume that there exists an homogeneous element $a \in I$ such that $aa^* \neq 0$. By minimality, $I = aa^*\mathcal{A} = a\mathcal{A}$, and $I^*I = \mathcal{A}aa^*aa^*\mathcal{A} \subseteq \mathcal{A}(aa^*I) = \{0\}$. By [3, Theorem 3.9(iv)], $\mathcal{A}a$ is a minimal left $\mathbb{Z}_p$-ideal, and hence $a^*\mathcal{A} = (\mathcal{A}a)^*$ is a minimal right $\mathbb{Z}_p$-ideal. Take $J = a^*\mathcal{A}$. If there was an homogeneous element x in J with $xx^* \neq 0$, as before we would have $\{0\} = J^*J = \mathcal{A}aa^*\mathcal{A}$, but this is impossible since $\mathcal{A}$ is prime. So for any homogeneous element x in J, $xx^* = 0$.

Hence, from now on let I be a minimal right $\mathbb{Z}_p$-ideal of $\mathcal{A}$ such that $xx^* = 0$ for any homogeneous element x in I. By [3, Theorem 3.9], $I = e\mathcal{A}$ for a primitive idempotent $e \in I_0$, we have $e\mathcal{A}e^* \neq \{0\}$ by primeness. Therefore $e\mathcal{A}_\nu e^* \neq \{0\}$ for some $\nu \in \mathbb{Z}_p$. We choose ν to be 0 if possible. We will show that this will always be the case, let $\mathcal{D} = e\mathcal{A}e$, if $\mathcal{D}_j = e\mathcal{A}_j e \neq \{0\}$ for some $1 \leq j \leq p-1$, then $\mathcal{D}_{p-j} = e\mathcal{A}_{p-j}e \neq \{0\}$ (since $\mathcal{D}$ is a division $\mathbb{Z}_p$-algebra). If $e\mathcal{A}_{p-j}e^* \neq \{0\}$, since $e^*\mathcal{A}_j e^* = (e\mathcal{A}_j e)^* \neq \{0\}$,

$$e\mathcal{A}_0 e^* \supseteq (e\mathcal{A}_{p-j}e^*)(e^*\mathcal{A}_j e^*) \neq \{0\}.$$

Similarly if $e\mathcal{A}_j e^* \neq \{0\}$, since $e^*\mathcal{A}_{p-j}e^* = (e\mathcal{A}_{p-j}e)^* \neq \{0\}$,

$$e\mathcal{A}_0 e^* \supseteq (e\mathcal{A}_j e^*)(e^*\mathcal{A}_{p-j}e^*) \neq \{0\}.$$

We may therefore assume that if $\nu \neq 0$ then $\mathcal{D}_j = \{0\}$ for all $1 \leq j \leq p-1$.

Assume $e\mathcal{A}_\nu e^* \neq \{0\}$. If $e(r_\nu + r_\nu^*)e^* \neq 0$, for some $r_\nu \in \mathcal{A}_\nu$, letting $t_\nu = r_\nu + r_\nu^*$ we may assume that $(et_\nu e^*)^* = et_\nu e^*$. Otherwise $(er_\nu e^*)^* = -er_\nu e^*$, for all $r_\nu \in \mathcal{A}_\nu$ and one chooses $t_\nu \in \mathcal{A}_\nu$ such that $(et_\nu e^*)^* = -et_\nu e^* \neq 0$. Thus

$$(et_\nu e^*)^* = \epsilon et_\nu e^*, \qquad \epsilon = \pm 1.$$

Since $e^*\mathcal{A}et_\nu e^* \neq \{0\}$, by primeness, and since $e^*\mathcal{A}_0 e^*$ is a division algebra, one can choose $s_{(p-1)\nu} \in \mathcal{A}_{(p-1)\nu}$ such that

$$e^* s_{(p-1)\nu} et_\nu e^* = e^*.$$

Applying $*$,

$$\begin{aligned} e &= (-1)^{(p-1)\nu^2} et_\nu^* e^* s_{(p-1)\nu}^* e \\ &= (-1)^{(p-1)\nu^2} et_\nu^* e^* s_{(p-1)\nu}^* e. \\ &= (-1)^{(p-1)\nu^2} \epsilon et_\nu e^* s_{(p-1)\nu}^* e. \end{aligned}$$

Therefore,

$$\begin{aligned} e^* s_{(p-1)\nu} e &= e^* s_{(p-1)\nu}((-1)^{(p-1)\nu^2} \epsilon et_\nu e^* s_{(p-1)\nu}^* e) \\ &= (-1)^{(p-1)\nu^2} \epsilon (e^* s_{(p-1)\nu} et_\nu e^*) s_{(p-1)\nu}^* e \\ &= (-1)^{(p-1)\nu^2} \epsilon e^* s_{(p-1)\nu}^* e. \end{aligned}$$

Thus

$$(e^* s_{(p-1)\nu} e)^* = (-1)^{(p-1)\nu^2} \epsilon e^* s_{(p-1)\nu} e.$$

We therefore have

$$e^* s_{(p-1)\nu} e t_\nu e^* = e^*, \qquad e t_\nu e^* s_{(p-1)\nu} e = e,$$

$$(e t_\nu e^*)^* = \epsilon e t_\nu e^*, \qquad (e^* s_{(p-1)\nu} e)^* = (-1)^{(p-1)\nu^2} \epsilon e^* s_{(p-1)\nu} e.$$

For $v_\alpha = e a_\alpha \in I_\alpha$, $w_\beta = e b_\beta \in I_\beta$,

$$\begin{aligned} v_\alpha w_\beta^* &= e a_\alpha b_\beta^* e^* \\ &= e a_\alpha b_\beta^* e^* s_{(p-1)\nu} e t_\nu e^*. \end{aligned}$$

Define

$$(v_\alpha, w_\beta)_\nu := e a_\alpha b_\beta^* e^* s_{(p-1)\nu} e \in e\mathcal{A}_{\alpha+\beta+(p-1)\nu} e = \mathcal{D}_{\alpha+\beta+(p-1)\nu}.$$

By the last claim $(v_\alpha, v_\alpha)_\nu := e a_\alpha a_\alpha^* e^* s_{(p-1)\nu} e = 0$, for all $v_\alpha \in I_\alpha$. If $(v_\alpha, I)_\nu = \{0\}$,

$$e a_\alpha \mathcal{A} e^* s_{(p-1)\nu} e = \{0\},$$

and, since $e^* s_{(p-1)\nu} e \neq 0$,

$$e a_\alpha = 0, \qquad \text{by primeness.}$$

Similarly, $(I, w_\beta)_\nu = \{0\}$ implies $w_\beta = 0$ and $(\ ,\ )_\nu$ is nondegenerate. If $d_\delta \in \mathcal{D}_\delta$, $(d_\delta v_\alpha, w_\beta)_\nu = d_\delta (v_\alpha, w_\beta)_\nu$. Moreover

$$\begin{aligned} (v_\alpha, d_\delta w_\beta)_\nu &= (e a_\alpha, d_\delta e b_\beta)_\nu \\ &= (-1)^{\delta\beta} e a_\alpha b_\beta^* e^* d_\delta^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\delta\beta} e a_\alpha b_\beta^* e^* s_{(p-1)\nu} e t_\nu e^* d_\delta^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\delta\beta} (v_\alpha, w_\beta)_\nu e t_\nu e^* d_\delta^* e^* s_{2\nu} e \\ &= (-1)^{\delta\beta} (v_\alpha, w_\beta)_\nu \overline{d_\delta}, \end{aligned}$$

where

$$\overline{d_\delta} := e t_\nu e^* d_\delta^* e^* s_{(p-1)\nu} e.$$

For $d_\delta \in \mathcal{D}_\delta$,

$$\begin{aligned} \overline{\overline{d_\delta}} &= e t_\nu e^* (e t_\nu e^* d_\delta^* e^* s_{(p-1)\nu} e)^* e^* s_{(p-1)\nu} e \\ &= (-1)^{(p-1)\nu(\nu+\delta)} (-1)^{\delta\nu} e t_\nu e^* s_{(p-1)\nu}^* e d_\delta e t_\nu^* e^* s_{(p-1)\nu} e \\ &= (-1)^{(p-1)\nu(\nu+\delta)} (-1)^{\delta\nu} (-1)^{(p-1)\nu^2} \epsilon e d_\delta \epsilon e \\ &= (-1)^{(p-1)\nu(\nu+\delta)} (-1)^{\delta\nu} (-1)^{(p-1)\nu^2} d_\delta, \end{aligned}$$

$$= d_\delta,$$

since if $\nu \neq 0$, then δ must be 0. For $c_\gamma \in \mathcal{D}_\gamma$ and $d_\delta \in \mathcal{D}_\delta$,

$$\begin{aligned}\overline{c_\gamma d_\delta} &= et_\nu e^*(c_\gamma d_\delta)^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\gamma\delta} et_\nu e^* d_\delta^* c_\gamma^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\gamma\delta} et_\nu e^* d_\delta^* e^* s_{(p-1)\nu} et_\nu e^* c_\gamma^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\gamma\delta} \overline{d_\delta}\,\overline{c_\gamma}.\end{aligned}$$

Thus $^-$ is a $\mathbb{Z}_p$-involution of $\mathcal{D}$ and $(\ ,\ )_\nu$ is a nondegenerate sesquilinear $\mathbb{Z}_p$-form on I whose adjoint is $*$. Finally

$$\begin{aligned}\overline{(v_\alpha, w_\beta)_\nu} &= et_\nu e^*(ea_\alpha b_\beta^* e^* s_{(p-1)\nu} e)^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\alpha\beta}(-1)^{(p-1)\nu(\alpha+\beta)} et_\nu e^* s_{(p-1)\nu}^* eb_\beta a_\alpha^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\alpha\beta}(-1)^{(p-1)\nu(\alpha+\beta)}(-1)^{(p-1)\nu^2} \epsilon eb_\beta a_\alpha^* e^* s_{(p-1)\nu} e \\ &= (-1)^{\alpha\beta}(-1)^{(p-1)\nu(\alpha+\beta)}(-1)^{(p-1)\nu^2} \epsilon (w_\beta, v_\alpha)_\nu.\end{aligned}$$

If $\nu = 0$, then $\overline{(v_\alpha, w_\beta)_0} = (-1)^{\alpha\beta}\epsilon(w_\beta, v_\alpha)_0$. Thus $(\ ,\ )_0$ is ϵ-hermitian $\mathbb{Z}_p$-form. If $\nu \neq 0$, then we have assumed that $\mathcal{D}_j = \{0\}$ for all $1 \leq j \leq p-1$ and so $(v_\alpha, w_\beta)_\nu = 0$, if $\alpha + \beta + (p-1)\nu = j \mod p$, where $j \neq 0$, which implies that $\alpha + \beta = \nu + j \mod p$. Thus the right hand side is 0 unless $\alpha + \beta = \nu \mod p$, and therefore

$$\overline{(v_\alpha, w_\beta)_\nu} = (-1)^{\alpha\beta}\epsilon(w_\beta, v_\alpha)_\nu.$$

Thus $(\ ,\ )_\nu$ is ϵ-hermitian $\mathbb{Z}_p$-form. □

Now we have the following results for a prime number p.

Corollary 3.3. *A central simple $\mathbb{Z}_p$-algebra $\mathcal{A} = M_n(\mathcal{D})$ over a field K, where $\mathcal{D}$ is a division $\mathbb{Z}_p$-algebra with $\mathcal{D}_1 \neq \{0\}$, has a $\mathbb{Z}_p$-involution if and only if $\mathcal{D}$ has.*

Corollary 3.4. *If a central simple $\mathbb{Z}_p$-algebra $\mathcal{A} = M_n(\mathcal{D})$ over a field K, where $\mathcal{D}$ is a division algebra with $\mathcal{D}_j = \{0\}$ for all $1 \leq j \leq p-1$ has a $\mathbb{Z}_p$-involution then $\mathcal{D}$ has.*

In the next example we define a $\mathbb{Z}_3$-involution on a central simple $\mathbb{Z}_3$-algebra $\mathcal{A} = M_{1+1+1}(K)$, where K is a given field.

Example 1. Let $\mathcal{A} = M_{1+1+1}(K)$ be a $\mathbb{Z}_3$-algebra then the $\mathbb{Z}_3$-additive map

$$\sigma : \mathcal{A} \to \mathcal{A}$$

defined by

$$\sigma(\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}) = \begin{pmatrix} c & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{pmatrix}, \quad \sigma(\begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix}) = \begin{pmatrix} 0 & 0 & -c \\ b & 0 & 0 \\ 0 & a & 0 \end{pmatrix}, \quad \sigma(\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}) = \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & a \\ -c & 0 & 0 \end{pmatrix}$$

is a $\mathbb{Z}_3$-involution on $\mathcal{A}$.

Let $\mathcal{A} = M_{p+q+p}(\mathcal{D})$ be a central simple $\mathbb{Z}_3$-algebra, where $\mathcal{D}$ is a division algebra. In the last result we define a $\mathbb{Z}_3$-involution on $\mathcal{A}$ induced by an involution $^-$ defined on $\mathcal{D}$.

Theorem 3.5. *Let $\mathcal{D}$ be a division algebra, and let $\mathcal{A} = M_{p+q+p}(\mathcal{D})$, $p, q > 0$ be a $\mathbb{Z}_3$-algebra with $\mathcal{A}_0 = M_p(\mathcal{D}) \oplus M_q(\mathcal{D}) \oplus M_p(\mathcal{D})$ and*

$$\mathcal{A}_1 = \begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix}, \quad \mathcal{A}_2 = \begin{pmatrix} 0 & x & 0 \\ 0 & 0 & y \\ z & 0 & 0 \end{pmatrix}$$

with $a, y \in M_{q\times p}(\mathcal{D})$, $b, x \in M_{p\times q}(\mathcal{D})$, $c, z \in M_{p\times p}(\mathcal{D})$. If $\mathcal{D}$ has an involution $^-$, then $*$ defined by

$$\begin{pmatrix} f & x & c \\ a & g & y \\ z & b & h \end{pmatrix}^* = \begin{pmatrix} \tilde{h} & \tilde{y} & -\tilde{c} \\ \tilde{b} & \tilde{g} & \tilde{x} \\ -\tilde{z} & \tilde{a} & \tilde{f} \end{pmatrix}$$

is a $\mathbb{Z}_3$-involution on $\mathcal{A}$, where for any matrix a over $\mathcal{D}$, $\tilde{a} = \bar{a}^t$, t the transpose.

proof. If $\mathcal{D}$ has an involution $^-$, then for any $a \in M_p(\mathcal{D})$ or $a \in M_q(\mathcal{D})$, $\tilde{a} = \bar{a}^t$, t the transpose, defines involutions on $M_p(\mathcal{D})$ and on $M_q(\mathcal{D})$. Moreover if $a \in M_{p\times q}(\mathcal{D})$ $(M_{q\times p}(\mathcal{D}))$, then $\tilde{a} \in M_{q\times p}(\mathcal{D})$ $(M_{p\times q}(\mathcal{D}))$.

Let $\begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & z \\ x & 0 & 0 \\ 0 & y & 0 \end{pmatrix}$ be two matrices in $\mathcal{A}_1$, then

$$[\begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & z \\ x & 0 & 0 \\ 0 & y & 0 \end{pmatrix}]^* = \begin{pmatrix} 0 & cy & 0 \\ 0 & 0 & az \\ bx & 0 & 0 \end{pmatrix}^* = \begin{pmatrix} 0 & \widetilde{az} & 0 \\ 0 & 0 & \widetilde{cy} \\ -\widetilde{bx} & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \tilde{z}\tilde{a} & 0 \\ 0 & 0 & \tilde{y}\tilde{c} \\ -\tilde{x}\tilde{b} & 0 & 0 \end{pmatrix}.$$

And

$$-\begin{pmatrix} 0 & 0 & z \\ x & 0 & 0 \\ 0 & y & 0 \end{pmatrix}^* \begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix}^* = -\begin{pmatrix} 0 & 0 & -\tilde{z} \\ \tilde{y} & 0 & 0 \\ 0 & \tilde{x} & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -\tilde{c} \\ \tilde{b} & 0 & 0 \\ 0 & \tilde{a} & 0 \end{pmatrix}$$

$$= -\begin{pmatrix} 0 & -\tilde{z}\tilde{a} & 0 \\ 0 & 0 & -\tilde{y}\tilde{c} \\ \tilde{x}\tilde{b} & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \tilde{z}\tilde{a} & 0 \\ 0 & 0 & \tilde{y}\tilde{c} \\ -\tilde{x}\tilde{b} & 0 & 0 \end{pmatrix}.$$

Which implies that $(XY)^* = -Y^*X^*$ for all $X, Y \in \mathcal{A}_1$. Moreover

$$[\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & y & 0 \\ 0 & 0 & z \\ x & 0 & 0 \end{pmatrix}]^* = \begin{pmatrix} 0 & 0 & az \\ bx & 0 & 0 \\ 0 & cy & 0 \end{pmatrix}^* = \begin{pmatrix} 0 & 0 & -\widetilde{az} \\ \widetilde{cy} & 0 & 0 \\ 0 & \widetilde{bx} & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & -\tilde{z}\tilde{a} \\ \tilde{y}\tilde{c} & 0 & 0 \\ 0 & \tilde{x}\tilde{b} & 0 \end{pmatrix}.$$

And

$$-\begin{pmatrix} 0 & y & 0 \\ 0 & 0 & z \\ x & 0 & 0 \end{pmatrix}^* \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}^* = -\begin{pmatrix} 0 & \tilde{z} & 0 \\ 0 & 0 & \tilde{y} \\ -\tilde{x} & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & \tilde{b} & 0 \\ 0 & 0 & \tilde{a} \\ -\tilde{c} & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & -\tilde{z}\tilde{a} \\ \tilde{y}\tilde{c} & 0 & 0 \\ 0 & \tilde{x}\tilde{b} & 0 \end{pmatrix}.$$

Which implies that $(XY)^* = -Y^*X^*$ for all $X, Y \in \mathcal{A}_2$.

Finally, let $X = \begin{pmatrix} 0 & 0 & c \\ a & 0 & 0 \\ 0 & b & 0 \end{pmatrix}$ be a general matrix in $\mathcal{A}_1$ and $Y = \begin{pmatrix} 0 & y & 0 \\ 0 & 0 & z \\ x & 0 & 0 \end{pmatrix}$ a general matrix in $\mathcal{A}_2$, then

$$(XY)^* = \begin{pmatrix} cx & 0 & 0 \\ 0 & ay & 0 \\ 0 & 0 & bz \end{pmatrix}^* = \begin{pmatrix} \widetilde{bz} & 0 & 0 \\ 0 & \widetilde{ay} & 0 \\ 0 & 0 & \widetilde{cx} \end{pmatrix}$$
$$= \begin{pmatrix} \tilde{z}\tilde{b} & 0 & 0 \\ 0 & \tilde{y}\tilde{a} & 0 \\ 0 & 0 & \tilde{x}\tilde{c} \end{pmatrix}$$

and $Y^*X^* = \begin{pmatrix} 0 & \tilde{z} & 0 \\ 0 & 0 & \tilde{y} \\ -\tilde{x} & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & -\tilde{c} \\ \tilde{b} & 0 & 0 \\ 0 & \tilde{a} & 0 \end{pmatrix} = \begin{pmatrix} \tilde{z}\tilde{b} & 0 & 0 \\ 0 & \tilde{y}\tilde{a} & 0 \\ 0 & 0 & \tilde{x}\tilde{c} \end{pmatrix} = (XY)^*.$

Similarly, $(YX)^* = X^*Y^*$. □

References

[1] A. Elduque, O. Villa, The existence of superinvolutions, *Journal of Algebra*, **319** (2008), 4338-4359.

[2] A. Jaber, Existence of Pseudo-Superinvolutions of The First Kind, *International Journal of Mathematics and Mathematical Sciences*, Volume 2008 (2008), Article ID 386468, 13 pages, **doi:** 10.1155/2008/386468.

[3] A. Jaber, On Primitive $\mathbb{Z}_\mathsf{p}$-Algebra, *Submitted*.

[4] C.T.C. Wall, Graded Brauer groups, *Reine Angew. Math.*, **213** (1963), 187-199.

[5] M.L. Racine, Primitive superalgebras with superinvolution, *Journal of Algebra*, **206** (1998), 588-614.

[6] M.L. Racine, E.I. Zelmanov, Simple Jordan superalgebras with semisimple even part, *Journal of Algebra*, **270** (2003), 374-444.