Annales Univ. Sci. Budapest., Sect. Comp. 58 (2025) 157–165

A NOTE ON DIVISION RINGS WITH INVOLUTION

Dau Thi Hue (Ho Chi Minh City, Vietnam)

Communicated by Bui Minh Phong

(Received 7 October 2024; accepted 10 November 2024)

Abstract. In this note, we investigate the structure of division rings with involution. It is shown that if we impose a suitable condition on some subset of symmetric elements then the algebraic structure of a division ring is effected.

1. Introduction

Let R be an associative ring with identity $1 \neq 0$. Recall that an *involution* on R is a map $^\star : R \to R$ which satisfies the following conditions for all elements x and y in R:

(i) $(x+y)^\star = x^\star + y^\star$,

(ii) $(xy)^\star = y^\star x^\star$,

(iii) $(x^\star)^\star = x$.

Let R be such a ring, and let $Z(R)$ denote the center of R. It is straightforward to check that $Z(R)$ is preserved under the involution $\star$. The restriction of $\star$ to $Z(R)$ is therefore an automorphism which is either the identity or of order 2. Accordingly, an involution which leaves the elements of $Z(R)$ fixed is called an *involution of the first kind.* An involution whose restriction to the center is an automorphism of order 2 is called *involution of the second kind.*

Key words and phrases: Symplectic involution, commuting involution, scalar involution, quaternion division algebra.

2010 Mathematics Subject Classification: 16K20, 16K40, 16W10.

https://doi.org/10.71352/ac.58.101124

First published online: 8 March 2025

Throughout this note, we only investigate rings with involutions of the first kind.

Recall that the set of *symmetric* elements, the set of *traces*, and the set of *norms* of R are defined as follows:

$$R_+ = \{x \in R \mid x^\star = x\},$$
$$T_R = \{x + x^\star \mid x \in R\},$$
$$N_R = \{xx^\star \mid x \in R\}.$$

Clearly that the sets T_R and N_R both are contained in R_+.

In a series of his papers (see e.g. [4]–[6]), Chacron has considered the following conditions for a ring R with involution $\star$:

(C1) $x^\star x = xx^\star$, for all $x \in R$.

(C2) For each x in R, there exists a positive integer N depending on x such that $\mathrm{d}_x^N(x^\star) = 0$, where $\mathrm{d}_x : R \to R$ is a map given by $y \mapsto yx - xy$, and d_x^N is the N-th power of d_x under composition.

(C3) For each x in R, there exists a positive integer N depending on x such that $x^\star x^N = x^N x^\star$.

(C4) $x + x^\star$ is central for all $x \in R$.

(C5) $xx^\star$ is central for all $x \in R$.

In accordance with [10, Propostion 2.6], if the involution $\star$ satisfies (C1), (C4) or (C5), then it is said to be *commuting*, *symplectic* or *scalar* respectively, while (C2) and (C3) are called *local power commuting condition* and *local Engel condition* respectively. The relationships between these conditions are imposed on the following implications which are obvious:

$$\text{(C5)} \implies \text{(C4)} \implies \text{(C1)} \implies \text{(C2) and (C3)}.$$

Over the past few years, there have been many works devoted to the study of certain rings with involutions satisfying some of these conditions. It was shown in [5, Theorem 4.7] that if R is a semiprime ring satisfying a polynomial identity, then the conditions (C1), (C2), and (C3) are equivalent. If R is a semiprime ring instead, then it was proved in [4, Theorem 2.3] that (C1), (C4) and (C5) are equivalent. At the other extreme, it was shown in [6, Theorem 2.13] that in case R is a non-commutative simple ring which is algebraic over its center, then (C2) is equivalent to (C4) and R must be a quaternion algebra over its center.

There are close relationships between the conditions introduced by Chacron and the conditions on the set T_R of traces and on the set N_R of norms of R. It is clear that $\star$ satisfies (C4) if and only if $T_R \subseteq Z(R)$, while $\star$ satisfies (C5) if and only if $N_R \subseteq Z(R)$. Thus, in view of [6, Theorem 2.13], if R is a non-commutative simple ring algebraic over $Z(R)$ such that $T_R \subseteq Z(R)$, then R is a quaternion algebra over its center. This fact particularly says, in some sense, that the condition $T_R \subseteq Z(R)$, or equivalently that $\star$ satisfies (C4), is really a strong condition which imposes a special structure on the whole R.

In this note, we consider the case when $R = D$ is a division ring, and the influence of some subsets of the sets T_D and N_D on the structure of D. Let G be a non-central subgroup of the multiplicative group $D^\times$ of D. This means that G is not contained in the center F of D. For such a subgroup G, let us consider the sets T_G and N_G, defined as follows:

$$T_G = \{x + x^\star \mid x \in G\} \text{ and } N_G = \{xx^\star \mid x \in G\}.$$

From [3], it can be seen that if we impose suitable conditions on the set $T_G \cup N_G$ then the algebraic structure of whole D is effected. For instance, [3, Corollary 5.6] says that if $T_G \cup N_G$ is contained in the center F of D, then D is a quaternion division algebra over F and $\star$ is of the symplectic type, provided G is a non-central normal subgroup of $D^\times$. Here, we consider the case when G is a non-central subnormal subgroup of $D^\times$, and we obtain the same result provided either $T_G \subseteq F$ or $N_G \subseteq F$. Moreover, we show the following equivalences:

$$T_G \subseteq F \iff N_G \subseteq F \iff T_D \subseteq F \iff N_D \subseteq F.$$

Throughout this note, if X is either a ring or a group then $Z(X)$ stands for the center of X. An element $x \in X$ is said to be *central* if $x \in Z(X)$; otherwise x is *non-central*. A subset S of X is *non-central* if and only if there is at least one non-central element in S.

2. Division rings with involution

Let D be a division ring with involution $\star$ and center F. In this section, we investigate the structure of D under the influence of a condition imposed on some subset of symmetric elements of D. The main result is Theorem 2.2, which generalizes [3, Corollary 5.6].

Since finite-dimensional central simple algebras play a crucial role in our investigation, let us firstly establish the necessary background by recalling some fundamental facts about these algebras. Let A be a finite-dimensional central simple algebra over a field F. Then, by the well-known Wedderburn-Artin Theorem, there is a unique integer r and a unique up to isomorphism division ring D with center F such that $A \cong \mathrm{M}_r(D)$. It is known that the dimension of D over F is a square; that is, $[D : F] = k^2$, for some integer $k \geq 1$. It follows that $[A : F] = r^2k^2$, and hence $[A : F]$ is also a square. Accordingly, the *degree* of A is defined to be $\deg(A) = \sqrt{[A : F]}$. Let A be such an F-algebra with involution $\star$. As F is invariant under $\star$, it can be checked that the set of traces $T_A = \{x + x^\star \mid x \in A\}$ of A is a F-subspace of A, while the set of norms $N_A = \{xx^* \mid x \in A\}$ is not. The dimension $[T_A : F]$ of T_A over F is given in the following lemma.

Lemma 2.1. *Let A be a finite-dimensional central simple F-algebra of degree m with involution $\star$, and $d = [T_A : F]$. Then, either $d = \frac{m(m+1)}{2}$ or $d = \frac{m(m-1)}{2}$.*

Proof. This lemma is an immediate corollary of [10, Proposition 2.6]. ■

The evaluation of the dimensions above shows that the F-subspace T_A is significantly large in A. As noted in the introduction, N_A is a subset of A_+, but it is not an F-subspace. However, there is the connection between N_A and the F-subspace T_A. A straightforward calculation shows that if $N_A \subseteq Z(A)$, then $T_A \subseteq Z(A)$ as well. Indeed, for any $x \in A$, we have

$$(1 + x)(1 + x)^\star = (1 + x)(1 + x^\star) = 1 + x + x^\star + xx^\star.$$

Because both $(1 + x)(1 + x)^\star$ and $xx^\star$ are contained in $Z(A)$, we get $x + x^\star \in$ $\in Z(A)$, yielding that $T_A \subseteq Z(A)$. This implies that N_A, despite not being a subspace, significantly influences to the structure of A.

Corollary 2.1. *Let D be a centrally finite division ring with center F, n a positive integer, and $\star$ an involution on $\mathrm{M}_n(D)$. If $T_{\mathrm{M}_n(D)} \subseteq F$, then either*

(i) *$n = 1$, and $D = F$ or D is a quaternion division algebra over F, or*

(ii) *$n = 2$, and $D = F$ and $\star$ is the ordinary symplectic involution on $\mathrm{M}_2(F)$; that is, the involution $\star$ is given by:*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\star = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Proof. Let $[D : F] = k^2$, for some integer $k \geq 1$. It follows that $A := \mathrm{M}_n(D)$ is a F-central simple algebra of degree $m := kn$. In view of Lemma 2.1, there are two possible cases:

Case 1. $[T_A : F] = \frac{m(m+1)}{2}$. In this case, the involution $\star$ must be of orthogonal type. Moreover, as $T_A \subseteq F$, we get that $\frac{m(m+1)}{2} = 1$, from which it follows that $m = 1$. This means that $n = k = 1$, and so $A = D = F$.

Case 2. $[T_A : F] = \frac{m(m-1)}{2}$. As in Case 1, the condition $T_A \subseteq F$ implies that $\frac{m(m-1)}{2} = 1$. It follows that $m = 2$, which means that $n = 2$ and $k = 1$, or else $n = 1$ and $k = 2$.

Case 2.1. $n = 2$ and $k = 1$. In this case, we have $D = F$ and so $A \cong \mathrm{M}_2(F)$. By [4, Theorem 2.3], the involution $\star$ is scalar.

Assume that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\star} = \begin{pmatrix} m & n \\ p & q \end{pmatrix}$. Since $\star$ is a symplectic and scalar, it follows that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\star} \in F$, and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\star} \in F$. Therefore,

$$\begin{pmatrix} a+m & b+n \\ c+p & d+q \end{pmatrix} \in F$$

and

$$\begin{pmatrix} am-bc & -ab+bq \\ cm-cd & -cb+dq \end{pmatrix} \in F,$$

which implies that $b+n = c+p = -ab+bq = cm-cd = 0$. Hence, $n=-b$, $p=-c$, $q=a$, $m=d$, and we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\star} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Case 2.2. $n=1$ and $k=2$. It follows that $A=D$ and $[D:F]=4$, which means that A is a quaternion algebra over F. The proof of the corollary is now complete. ■

The following lemma follows immediately from [4, Theorem 2.3].

Lemma 2.2. *Let A be an unital semi-prime ring with center Z, and $\star$ be an involution on A. Then, $T_A \subseteq Z$ if and only if $N_A \subseteq Z$.*

Lemma 2.3. *Let D be a division ring with center F, n a positive integer, and $\star$ an involution on $\mathrm{M}_n(D)$. If $T_{\mathrm{M}_n(D)} \subseteq F$, then D is centrally finite. Consequently, either assertion* (i) *or* (ii) *of Corollary 2.1 holds for D.*

Proof. In view of Lemma 2.2, the involution $\star$ is both symplectic and scalar. Hence, for each $a \in \mathrm{M}_n(D)$, the elements $s := a^\star + a$ and $p := a^\star a$ are both contained in F. It is straightforward to check that $a^2 - sa + p = 0$. This shows that the matrix ring $\mathrm{M}_n(D)$ is algebraic of bounded degree 2, and so is D. By the famous result of Jacobson [8, Theorem 7], D is finite dimensional over F as desired. ■

Lemma 2.4. *Let R be a ring with involution $\star$, G a subgroup of $R^\times$. Let $Z[G]$ be the subring of R generated by G over the center Z of R. If $T_G \subseteq Z$, then the restriction of $\star$ to $Z[G]$ is a symplectic involution on $Z[G]$.*

Proof. Take an arbitrary element $x \in Z[G]$, and write it in the form

$$x = a_1 g_1 + a_2 g_2 + \cdots + a_n g_n,$$

where $a_i \in Z$ and $g_i \in G$. Because $\star$ leaves fixed elements in Z, it follows that

$$x + x^\star = a_1(g_1 + g_1^\star) + a_2(g_2 + g_2^\star) + \cdots + a_n(g_n + g_n^\star).$$

As $T_G \subseteq Z$, we conclude that $g_i + g_i^\star \in Z$ for all $i \in \{1, \dots, n\}$, and so $x + x^\star \in Z$, which implies that $x^\star \in Z[G]$. Hence, the restriction of $\star$ to $Z[G]$ is also an involution on $Z[G]$ which is clearly symplectic. ■

Lemma 2.5. *Let D be a division ring with center F, and H a subset of $D^\times$. For an element $g \in D$, let $F(g)$ be the subfield of D generated by g over F. If $h^{-1}gh \in F(g)$ for any $h \in H$, then $F(g)$ is H-invariant.*

Proof. Every element in $F(g)$ can be written in the form $a(g)b(g)^{-1}$, where $a(t), b(t)$ are two polynomials in $F[t]$ such that $b(g) \neq 0$. For any $0 \neq h \in H$, we have

$$h^{-1}a(g)b(g)^{-1}h = (h^{-1}a(g)h)(h^{-1}b(g)^{-1}h) = (h^{-1}a(g)h)(hb(g)h^{-1})^{-1}.$$

Write

$$a(g) = a_0 + a_1 g + \cdots + a_n g^n,$$
$$b(g) = b_0 + b_1 g + \cdots + b_m g^m,$$

where $a_i, b_j \in F$ for all $0 \leq i \leq n$ and $0 \leq j \leq m$. Because $h^{-1}gh \in F(g)$, it is easily checked that the elements $h^{-1}a(g)h$ and $hb(g)h^{-1}$ belong to $F(g)$. It follows that $h^{-1}a(g)b(g)^{-1}h \in F(g)$, and the proof of the lemma is proved. ■

Lemma 2.6. *Let D be a division ring with center F, G non-central subnormal subgroup of $D^\times$, and $\star$ an involution on D. Then, $N_G \subseteq F$ if and only if $\star$ is scalar.*

Proof. The "if" part is clear. Now, assume that $N_G \subseteq F$. To prove $N_D \subseteq F$, it suffices to show that $N_{D^\times} \subseteq F$. Because G is subnormal in $D^\times$, there exist a smallest integer $r \geq 1$ and a series of subgroups

$$G = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = D^\times,$$

in which G_i is normal in G_{i-1} for all $1 \leq i \leq r$. For each i, we claim that if $N_{G_i} \subseteq F$ then $N_{G_{i-1}} \subseteq F$. Assume by contrary that $N_{G_{i-1}} \not\subseteq F$. Fix an element $g \in G_i \backslash F$. For any $x \in G_{i-1}$, since $x^{-1}gx \in G_i$, we have

$$a := x^{-1}gxx^\star g^\star (x^\star)^{-1} = (x^{-1}gx)(x^{-1}gx)^\star \in F,$$

which implies that

$$gxx^\star g^\star = axx^\star. \tag{2.1}$$

Since $N_{G_i} \subseteq F$ and $g \in G_i$, we have $b = gg^\star \in F$. Replace $g^\star = bg^{-1}$ in (2.1), we get $bgxx^\star g^{-1} = axx^\star$, which implies that

$$(xx^\star)^{-1}gxx^\star = b^{-1}ag \in F(g).$$

Because x was chosen arbitrarily in G_{i-1}, in view of Lemma 2.5, the last equation shows that the subfield $F(g)$ is $N_{G_{i-1}}$-invariant. Let N be the subgroup of $D^\times$ generated by $N_{G_{i-1}}$. Then, $F(g)$ is N-invariant, and so it is $N \cap G_{i-1}$-invariant. Observe that $N \cap G_{i-1}$ is subnormal in G_{i-1}, and so it is subnormal in $D^\times$. Because $N_{G_{i-1}}$ is non-central, N is also non-central, and in view of [11, 14.4.5], $N \cap G_{i-1}$ is a non-central subnormal subgroup of $D^\times$. In view of [12, Theorem 1], it follows that either $F(g) \subseteq F$ or $F(g) = D$. The first case cannot occur because $g \notin F$. If the second case occurs, then D is non-commutative, a contradiction. Thus, the claim is shown. Now, by induction on r, we conclude that $N_D \subseteq F$, and so $\star$ is scalar. ■

Proposition 2.1. *Let D be a division ring with center F, and G a subgroup of $D^\times$ such that $F(G) = D$. Let $\star$ be an involution on D. If $T_G \subseteq F$, then D is a centrally finite division ring.*

Proof. Assume that $T_G \subseteq F$. Let $F[G]$ be the subring of D generated by G over F. According to Lemma 2.4, we conclude that the restriction of $\star$ to $F[G]$ is an symplectic involution on $F[G]$. Hence, by [4, Theorem 2.3], the restriction of $\star$ to $F[G]$ is scalar. So, for each $a \in F[G]$, we have $aa^\star \in Z(F[G]) \subseteq C_D(G)$, where $C_D(G)$ is the centralizer of G in D. Since $F(G) = D$, $C_D(G) = C_D(D) = F$, and so, $aa^\star \in F$. If we set $s := a^\star + a$ and $p := a^\star a$, then s and p are both in F. It is straightforward to check that $a^2 - sa + p = 0$, from which it follows that a satisfies the polynomial $x^2 - sx + p \in F[x]$. This shows that the prime ring $F[G]$ is algebraic of bound degree 2 over the field F, and by [9, Theorem 3], $F[G]$ satisfies a polynomial identity. By [1, Lemma 1], $F[G]$ has a division ring of quotients, consisting of all elements of the form sr^{-1}, where $r, s \in F[G]$ and $r \neq 0$, which coincides with $F(G) = D$. According to [1, Theorem 1], we conclude that $D = F(G)$ satisfies a polynomial identity, and so $[D : F] < \infty$ by [9, Theorem 1]. ■

We are now ready to prove our main theorem.

Theorem 2.2. *Let D be a division ring with center F, and $\star$ an involution on D. If G is a non-central subnormal subgroup of $D^\times$, then the following assertions are equivalent:*

(i) $T_G \subseteq F$,

(ii) $T_D \subseteq F$,

(iii) $N_D \subseteq F$,

(iv) $N_G \subseteq F$.

Moreover, if one of these conditions holds then D is a quaternion division algebra over F, and $\star$ is symplectic.

Proof. Firstly, we show that (i) $\Leftrightarrow$ (ii). It is clear that (ii) implies (i). Now, assume $T_G \subseteq F$. Because G is a non-central subnormal subgroup of $D^\times$, according to a Stuth's result (see [12, Theorem 1]), we have $F(G) = D$, and so $[D : F] < \infty$ by Proposition 2.1. In view of [7, Lemma 2.3], it follows that $D = F(G) = F[G]$, and by Lemma 2.4, $\star$ is a symplectic involution on D. This implies that $T_D \subseteq F$, and so (ii) holds. The equivalence (ii) $\Leftrightarrow$ (iii) follows from Lemma 2.2, while the implication (iii) $\Rightarrow$ (iv) follows immediately from the fact that $N_G \subseteq N_D$. Finally, the implication (iv) $\Rightarrow$ (iii) follows from Lemma 2.6.

To finish the proof of the theorem, assume that (ii) holds. Then, in view of Proposition 2.1, we get $[D : F] < \infty$. Hence, by Corollary 2.1, D is a quaternion division algebra over F, and $\star$ is symplectic. ■

Corollary 2.2. *Let D be a division ring with center F, $\star$ an involution on D, and G a non-central subnormal subgroup of $D^\times$. Then, the conditions* (C1)–(C5) *are all equivalent for D, and these conditions are also equivalent to the followings conditions:*

(i) *$x + x^\star$ is central for all $x \in G$,*

(ii) *$xx^\star$ is central for all $x \in G$.*

Moreover, if one of these conditions holds then D is a quaternion division algebra over F.

Proof. The equivalences of (C1)–(C5) follow from [4] and [5]. By Theorem 2.2, the conditions (i) is equivalent to (C4), and the condition (ii) is equivalent to (C5). ■

We close the paper with an interesting question which we shall investigate in a near future.

Remark. Let D be a division ring with involution $\star$ of the first kind, and K an arbitrary subfield of D which is unnecessary invariant under $\star$. If $T_D \cup N_D \subseteq K$, then every element $a \in D$ satisfies the quadratic equation $x^2 - sx + p = 0$, where $s = a + a^\star$ and $p = a^\star a$. This means that D is left algebraic of bound degree 2 over K. According to [2, Theorem 1.3], we get that D is a centrally finite division ring with center F, and $[D : F] \leq 4$; that is, D is either a field or a quaternion division ring. At this point, it is reasonable to ask if the main results of the current paper should be also true if we replace the center of D by an arbitrary its subfield?

References

[1] **Amitsur, S.A.,** On rings with identities, *J. London Math. Soc*, **30** (1955), 464–470.
https://doi.org/10.1112/jlms/s1-30.4.464

[2] **Bell, J.P., V. Drensky and Y. Sharifi,** Shirshov's theorem and division rings that are left algebraic over a subfield, *J. Pure Appl. Algebra*, **217** (2013), 1605–1610.
https://doi.org/10.1016/j.jpaa.2012.11.015

[3] **Bien, M.H., B.X. Hai and D.T. Hue,** On the unit groups of rings with involution, *Acta Math. Hungar*, **166(2)** (2022), 432–452.
https://doi.org/10.1007/s10474-022-01223-4

[4] **Chacron, M.,** Commuting involution, *Commun. Algebra*, **44(9)** (2016), 3951–3965. https://doi.org/10.1080/00927872.2015.1087546

[5] **Chacron, M.,** Involution satisfying a local Engel or power commuting condition, *Commun. Algebra*, **45(5)** (2017), 2018–2028.
https://doi.org/10.1080/00927872.2016.1226879

[6] **Chacron, M.,** More on involutions with local Engel or power commuting conditions, *Commun. Algebra*, **45(8)** (2017), 3503–3514.
https://doi.org/10.1080/00927872.2016.1237641

[7] **Hai, B.X. and N.V. Thin,** On locally nilpotent subgroups of $\mathrm{GL}_1(D)$, *Commun. Algebra* , **37** (2009), 712–718.
https://doi.org/10.1080/00927870802255287

[8] **Jacobson, N.,** Structure theory for algebraic algebras of bounded degree, *Ann. of Math*, **46** (1945), 695–707.
https://doi.org/10.2307/1969205

[9] **Kaplansky, I.,** Rings with a polynomial identity, *Bull. Amer. Math. Soc*, **54** (1948), 575–580.
https://doi.org/10.1090/S0002-9904-1948-09049-8

[10] **Knus, M.-A., A. Merkurjev, M. Rost and J.-P. Tignol,** *The Book of Involutions*, Amer. Math. Soc. Colloquium Publications **44**, 1998.
https://doi.org/10.1090/coll/044

[11] **Scott, W.R.,** *Group Theory*, Dover Publications, Inc., New York, 1987.

[12] **Stuth, C.J.,** A generalization of the Cartan–Brauer–Hua theorem, *Proc. Amer. Math. Soc*, **15** (1964), 211–217.
https://doi.org/10.1090/S0002-9939-1964-0158899-0

Dau Thi Hue
Faculty of Mathematics and Computer Science
University of Science
Ho Chi Minh City
Vietnam

and

Vietnam National University
Ho Chi Minh City
Vietnam
dthue.sgddt@tphcm.gov.vn