A CLOSER LOOK AT SKEW-SYMMETRIC ELEMENTS OF RATIONAL GROUP ALGEBRAS

DISHARI CHAUDHURI

Abstract. Let $R G$ be the group ring of a finite group $G$ over a commutative ring $R$ with 1. An element $x$ in $R G$ is said to be skew-symmetric with respect to an involution $\sigma$ of $R G$ if $\sigma(x) = -x$. A structure theorem for the skew-symmetric elements of $Q G$ is given which generalizes some previously known results in this direction.

Keywords: Group Rings, Involution, Skew-Symmetric Elements, Lie ring.

2010 Mathematics Subject Classification: 16S34; 16W10.

1. Introduction

Let $R G$ be the group ring of a finite group $G$ over a commutative ring $R$ with 1 and let $\sigma$ be an involution of $R G$. That is, $\sigma: R G \rightarrow R G$ is such that for $x, y \in R G$, $\sigma$ satisfies the following conditions: (i) $\sigma(x + y) = \sigma(x) + \sigma(y)$, (ii) $\sigma(xy) = \sigma(y)\sigma(x)$ and (iii) $\sigma^2(x) = x$. Let $R G_+\sigma = \{\gamma \in R G \mid \sigma(\gamma) = \gamma\}$ and $R G_-\sigma = \{\gamma \in R G \mid \sigma(\gamma) = -\gamma\}$ be the set of symmetric and skew-symmetric elements of $R G$ respectively with respect to the involution $\sigma$. If $2 \in R^\times$, then $R G_-\sigma = \{\gamma - \sigma(\gamma) \mid \gamma \in R G\}$. If $\sigma$ is an $R$-linear extension of an involution of $G$, then $R G_-\sigma$ is generated by $\{g - \sigma(g) \mid g \in G\setminus G_\sigma\}$ as an $R$-module, where $G_\sigma$ denotes the set of fixed elements of $G$ with respect to $\sigma$. Note that $R G_+\sigma$ and $R G_-\sigma$ may not be subrings of $R G$ in general. Now, $R G$ may be viewed as a Lie ring with the help of the bracket operation $[x, y] = xy - yx$ for $x, y \in R G$. Then, $R G_-\sigma$ becomes a Lie subring of $R G$. There are some strong relations between the structure of $R G_-\sigma$ and $R G$ as Lie rings which have been studied by many authors (for example, [Ami69], [ZS81], [GS93]). Also there are some close relations between polynomial identities satisfied by the unitary units of $R G$ and the Lie algebra $R G_-\sigma$ ([GM03]). The question of when $R G_-\sigma$ is commutative has been completely answered in terms of the group elements of $G$ when characteristic of $R$ is different from 3 ([JM05], [JM06], [CM07]). Lie properties of $R G_-\sigma$ has been studied as well ([LSS09]). So we can see that the Lie algebra $R G_-\sigma$ has occupied a prominent position in the literature since a long time. Hence it is interesting to study closely the structure of $R G_-\sigma$ itself.
When \( R = \mathbb{C} \) and \( \sigma \) is the canonical involution of \( \mathbb{C}G \), that is, the \( \mathbb{C} \)-linear extension of \( g \mapsto g^{-1} \), the structure of \( \mathbb{C}G^-_{\sigma} \) is given as a direct sum of classical simple Lie algebras by Cohen and Taylor [CT07]. The Lie algebra \( \mathfrak{gl}(n) \) is the space of all linear transformations of \( \mathbb{C}^n \), where the Lie product is the usual bracket operation. If \( n \geq 1 \) and if \( b \) is a non-degenerate alternating or symmetric bilinear form on \( \mathbb{C}^n \), then the subspace of \( \mathfrak{gl}(n) \) consisting of all \( x \) such that \( b(xu,v)+b(u,xv) = 0 \) for all \( u,v \in \mathbb{C}^n \) is a Lie algebra. When \( b \) is skew-symmetric, \( n \) is necessarily even, and we have the symplectic Lie algebra \( \mathfrak{sp}(n) \). When \( b \) is symmetric, we have the orthogonal Lie algebra \( \mathfrak{o}(n) \). Let \( \chi \) be a character of \( G \). It was shown in [CT07] that \( \mathbb{C}G^-_{\sigma} \) admits the decomposition:

\[
(1.1) \quad \mathbb{C}G^-_{\sigma} \cong \bigoplus_{\chi \in \mathfrak{R}(1)} \mathfrak{o}(\chi(1)) \oplus \bigoplus_{\chi \in \mathfrak{sp}} \mathfrak{sp}(\chi(1)) \oplus \bigoplus_{\chi \in \mathfrak{c}} \mathfrak{gl}(\chi(1))
\]

where \( \mathfrak{R}, \mathfrak{Sp} \) and \( \mathfrak{c} \) are the sets of irreducible characters of \( G \) of real, symplectic and complex types, respectively. The prime signifies that there is just one summand \( \mathfrak{gl}(\chi(1)) \) for each pair \( \{\chi, \overline{\chi}\} \) from \( \mathfrak{c} \). A slightly more general setting has been taken into consideration by Marin [Mar10], where \( R = \mathbb{k} \), a field of characteristic zero such that each ordinary representation of \( G \) is defined over \( \mathbb{k} \) (for instance, any \( \mathbb{k} \) containing the field of cyclotomic numbers) and \( \sigma \) is the \( \mathbb{k} \)-linear extension of the map \( g \mapsto \alpha(g)g^{-1} \), where \( \alpha : G \to \mathbb{k}^\times \) is a multiplicative character of \( G \). Here also \( \mathbb{k}G^-_{\sigma} \) is shown to admit a similar kind of decomposition. Both the papers have used Frobenius-Schur Theory and concluded an analogue of Wedderburn decomposition for the corresponding Lie subalgebras. All these results motivated us to study these kinds of Lie algebras on a more general setting. We have considered the rational group algebra \( \mathbb{Q}G \) and its Lie subalgebra \( \mathbb{Q}G^-_{\sigma} \) with respect to any involution \( \sigma \) of \( \mathbb{Q}G \). Let us look at an example first.

**Example 1.1.** Let \( G = \mathbb{Q}S = \langle a, b \mid a^2 = b^2, a^4 = 1, b^{-1}ab = a^{-1} \rangle \), the quaternion group of order 8 and \( \sigma \) be the canonical involution \( g \mapsto g^{-1} \) on \( \mathbb{Q}S \). Applying Lemma 1.1 of [JM05] to \( (\mathbb{Q}S)_\sigma^- \), we can conclude that it is not commutative. Let \( \mathbb{H}_Q \) be the quaternion algebra over \( \mathbb{Q} \), that is, \( \mathbb{H}_Q = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Q}\} \), where \( i, j, k \) satisfy the relations \( i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik \). The Wedderburn decomposition of \( \mathbb{Q}Q_S \) is:

\[
\mathbb{Q}Q_S \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}_Q.
\]

under the map \( a \mapsto (1, -1, 1, -1, i) \), \( b \mapsto (1, -1, 1, -1, j) \) and \( c = ab \mapsto (1, 1, -1, 1, k) \). So \( a^{-1}a \mapsto (0, 0, 0, 0, 2i) \), \( b^{-1}b \mapsto (0, 0, 0, 0, 2j) \) and \( c^{-1}c \mapsto (0, 0, 0, 0, 2k) \). Thus we get \( (\mathbb{Q}Q_S)_\sigma^- \simeq \mathbb{H}_Q \).
As a result of study of skew-symmetric elements with respect to an involution $\sigma$ on rational group algebras of finite groups, we have obtained the following results:

**Theorem 1.2.** There exists a right $\mathbb{Q}$-vector space $M$ which is also a left $\mathbb{Q}G$ module and a nonsingular hermitian or skew-hermitian form $h : M \times M \to \mathbb{Q}$ on $M$ (with respect to the identity involution on $\mathbb{Q}$) such that $\sigma$ is the adjoint involution of $h$ and

$$QG_{\sigma}^- = \{ f \in \mathbb{Q}G | h(f(x), y) + h(x, f(y)) = 0 \text{ for all } x, y \in M \}.$$

A decomposition theorem for the above Lie algebra of skew-symmetric elements is obtained as follows:

**Theorem 1.3.** If $\mathbb{Q}G \simeq \bigoplus_{V \in \hat{G}} \operatorname{End}_D(V)$, where $\hat{G}$ denotes the set of irreducible left $\mathbb{Q}G$-modules up to isomorphism with $D$ being division algebras over $\mathbb{Q}$ and the degree of the central simple algebra $\operatorname{End}_D(V)$ over its center $Z$ is $n$, then

$$QG_{\sigma}^- \simeq \bigoplus_{V \in \hat{G}_o} \mathfrak{o}(V) \oplus \bigoplus_{V \in \hat{G}_{sp}} \mathfrak{sp}(V) \oplus \bigoplus_{V \in \hat{G}_u} \mathfrak{gl}(V),$$

where $\hat{G}_o$, $\hat{G}_{sp}$ and $\hat{G}_u$ are subsets of $\hat{G}$ such that

\begin{align*}
\hat{G}_o &= \{ V \mid \sigma(\operatorname{End}_D(V)) = \operatorname{End}_D(V), \dim_Z(\operatorname{End}_D(V))_{\sigma}^- = n(n-1)/2 \}, \\
\hat{G}_{sp} &= \{ V \mid \sigma(\operatorname{End}_D(V)) = \operatorname{End}_D(V), \dim_Z(\operatorname{End}_D(V))_{\sigma}^- = n(n+1)/2, \text{ } n \text{ is even} \}, \\
\hat{G}_u &= \{ V \mid \sigma(\operatorname{End}_D(V)) = \operatorname{End}_D(V) \text{ or } \sigma(\operatorname{End}_D(V)) = \operatorname{End}_D^{op}(V^{op}), \dim_Z(\operatorname{End}_D(V))_{\sigma}^- = n^2 \}.
\end{align*}

The prime signifies that there is just one summand $\mathfrak{gl}(V)$ for each pair $\{V, V^{op}\}$ from $\hat{G}$.

The manuscript has been divided into five sections. The second section has been added for clarity. It contains most of the background material needed for the proof of our main theorems. The third section contains a study of rational group algebras with involutions. The fourth section is devoted to the proof of the two main theorems. As a conclusion in the fifth and final section an application of Theorem 1.2 is added to characterize skew-symmetric elements of integral group rings.

## 2. Background

Let the pair $(A, \sigma)$ denote an algebra $A$ over a field $F$ with $\sigma$ being an involution on $A$ and is such that $F = Z(A) \cap A^{\sigma}$. We will assume throughout that char $F \neq 2$ and algebras are always finite dimensional over the corresponding fields. Note that
the map $\sigma$ preserves the center $\mathcal{Z}(A)$. It can be easily seen as for $\alpha \in \mathcal{Z}(A), x \in A$, we have $x\sigma(\alpha) = \sigma(\alpha\sigma(x)) = \sigma(\sigma(x)\alpha) = \sigma(\alpha)x$. Thus $\sigma(\mathcal{Z}(A)) \subseteq \mathcal{Z}(A)$. The restriction of $\sigma$ to $\mathcal{Z}(A)$ is therefore an automorphism which is either the identity or of order 2.

Now let us assume that $A$ has no non-trivial two sided ideal $I$ with $\sigma(I) = I$. Involutions which leave the center elementwise invariant (that is, $[\mathcal{Z}(A) : F] = 1$) are called involutions of the first kind. Involutions whose restriction to the center is an automorphism of order 2 (that is, $[\mathcal{Z}(A) : F] = 2$) are called involutions of the second kind. As long as the center $\mathcal{Z}(A)$ of $A$ is a field, it follows that $A$ is central simple as a $\mathcal{Z}(A)$-algebra. In the case of involutions of the second kind, the center $\mathcal{Z}(A)$ is a quadratic étale extension of $F$ (which means that $\mathcal{Z}(A)$ is either a field which is a separable quadratic extension of $F$ or, $\mathcal{Z}(A) \simeq F \times F$). We assume that $A$ is simple (if $\mathcal{Z}(A)$ is a field) or a direct product of two simple algebras (if $\mathcal{Z}(A) \simeq F \times F$).

The following remark is 1.2.7 of [Knu91].

**Remark 2.1.** For any ring $R$, let $R^{op}$ be the opposite ring, that is, the same additive group with reversed multiplication

$$a^{op}b^{op} = (ba)^{op},$$

where $a^{op}$ stands for $a$ as an element of $R^{op}$. Involutions on $R$ are isomorphisms $\phi : R \to R^{op}$ of rings such that $\phi^2 = 1_R$. For any ring $R$, the product $R \times R^{op}$ has an involution

$$(a, b^{op}) \mapsto (b, a^{op}).$$

This product is called the hyperbolic ring of $R$ and is denoted by $H(R)$. This involution is called the exchange involution.

With notations and assumptions as in the second paragraph in the beginning of this section, the following is Proposition 2.14 in [KMRT98].

**Lemma 2.2.** Let $A$ be an $F$-algebra (as above) with an involution $\sigma$ of the second kind such that $\mathcal{Z}(A) \simeq F \times F$, then there is a central simple $F$-algebra $E$ such that

$$(A, \sigma) \simeq (E \times E^{op}, \varepsilon),$$

where $\varepsilon$ is the exchange involution.

The following remark is 1.2.8 of [Knu91].
Remark 2.3. Let \((A, \sigma)\) be a semisimple ring with involution. We can decompose \(A\) as a product \(A_1 \times \cdots \times A_n \times B_1 \times \cdots \times B_m\), where \(A_i\) are simple and \(\sigma(A_i) = A_i\) and the \(B_j\) are products of two simple algebras \(A'_j \times A''_j\) with \(\sigma(A'_j) = A''_j\). The rings \(B_j\) are isomorphic to hyperbolic rings, \(B_j \simeq H(A'_j)\). Thus \(\sigma\) restricted to \(A'_i\)'s are either involutions of first kind or involutions of second kind when the corresponding center of the simple algebra is a field. And, \(\sigma\) restricted to \(B'_j\)'s are clearly involutions of the second kind when the corresponding center is a product of two factors.

Recall that finite dimensional central simple algebras \(A, B\) over a field \(F\) are called Brauer-equivalent if the \(F\)-algebras of endomorphisms of any simple left \(A\)-module \(M\) and any simple left \(B\)-module \(N\) are isomorphic, that is, \(\text{End}_A(M) \simeq \text{End}_B(N)\). Equivalently, \(A\) and \(B\) are Brauer-equivalent if and only if \(M_l(A) \simeq M_m(B)\) for some integers \(l, m\). The following is a well known result by A. A. Albert ([KMRT98], Theorem 3.1). Most of the remaining section can be found in the same.

Theorem 2.4. If a central simple algebra has an involution, then every Brauer-equivalent algebra has an involution of the same kind.

Let us recall the definition of a hermitian form with respect to an involution on a finite dimensional central simple algebra.

Definition 2.5 (Hermitian Forms). Let \(E\) be a central simple algebra over a field \(F\) with \(\text{char} F \neq 2\) and let \(M\) be a finitely generated right \(E\)-module. Suppose that \(\theta : E \to E\) is an involution (of any kind) on \(E\). A hermitian form on \(M\) (with respect to the involution \(\theta\) on \(E\)) is a bi-additive map \(h : M \times M \to E\) such that:

(1) \(h(\alpha x, \beta y) = \theta(\alpha) h(x, y) \beta\) for all \(x, y \in M\) and \(\alpha, \beta \in E\),

(2) \(h(y, x) = \theta(h(x, y))\) for all \(x, y \in M\).

If (2) is replaced by \(h(y, x) = -\theta(h(x, y))\) for all \(x, y \in M\), the form \(h\) is called skew-hermitian. If \(E = F\) and \(\theta = \text{Id}\), hermitian (resp. skew-hermitian) forms are the symmetric (resp. skew-symmetric) bilinear forms on the finite dimensional vector space \(M\) over \(F\).

The hermitian or skew-hermitian form \(h\) on the right \(E\)-module \(M\) is called nonsingular if the only element \(x \in M\) such that \(h(x, y) = 0\) for all \(y \in M\) is \(x = 0\).

The following is Proposition 4.1 in [KMRT98]. The notations used are from the above definition.
Lemma 2.6. For every nonsingular hermitian or skew-hermitian form \( h \) on \( M \), there exists a unique involution \( \sigma_h \) on \( \text{End}_E(M) \) such that \( \sigma_h(\alpha) = \theta(\alpha) \) for all \( \alpha \in F \) and
\[
h(x, f(y)) = h(\sigma_h(f)(x), y) \quad \text{for } x, y \in M.
\]
The involution \( \sigma_h \) is called the adjoint involution with respect to \( h \).

Involutions of the first kind can be divided into two categories.

Definition 2.7 (Orthogonal and Symplectic Involutions). Let \((A, \sigma)\) be a central simple \( F \)-algebra of degree \( n \) with involution of first kind and let \( L \) be a splitting field of \( A \) (that is, \( L \) is a field containing \( F \) such that \( A_L = A \otimes_F L \simeq M_n(L) \)). Then \( \sigma \) extends to an involution of first kind \( \sigma_L = \sigma \otimes \text{Id}_L \) on \( A_L \). Let \( V \) be an \( L \)-vector space of dimension \( n \). There is a nonsingular symmetric or skew-symmetric bilinear form \( b \) on \( V \) and \((A_L, \sigma_L) \simeq (\text{End}_L(V), \sigma_b)\), where \( \sigma_b \) is the adjoint involution of the form \( b \). (Proposition 2.1, [KMRT98]). If \( b \) is symmetric, we say the involution \( \sigma \) is of orthogonal type. If \( b \) is skew-symmetric, then \( \sigma \) is said to be of symplectic type. As a parallel terminology involutions of second kind are also sometimes said to be of unitary type.

Note. The property of an involution \( \sigma \) to be first or second is called its kind, whereas the property to be orthogonal, symplectic or unitary is called its type.

Next is Proposition 2.6 and Proposition 2.17 of ([KMRT98]).

Lemma 2.8. (i) Let \((A, \sigma)\) be a central simple \( F \)-algebra of degree \( n \) with involution of the first kind. If \( \sigma \) is of orthogonal type, then \( \dim_F A_{\sigma}^- = n(n-1)/2 \). If \( \sigma \) is of symplectic type, then \( \dim_F A_{\sigma}^- = n(n+1)/2 \). Moreover, in the latter case \( n \) is necessarily even.

(ii) Let \( B \) be an \( F \)-algebra with an involution \( \tau \) of second kind. We say degree of \( B \) is \( n \), which is equal to degree of \( B \) if the center of \( B \) is a field or, it is equal to degree of \( E \) (recall Lemma 2.2) if the center is \( F \times F \). Then \( \dim_F B_{\tau}^- = n^2 \).

A very important result about a one-to-one correspondence between involutions on central simple algebras and hermitian forms on vector spaces over division algebras is the following (Theorem 4.2, [KMRT98]).

Theorem 2.9. Let \( A = \text{End}_E(M) \).

(1) If \( \theta \) is of the first kind on \( E \), the map \( h \mapsto \sigma_h \) defines a one-to-one correspondence between nonsingular hermitian and skew-hermitian forms on \( M \) (with respect to \( \theta \)) upt to a factor in \( F^\times \) and involutions of the first kind on \( A \).
Moreover, the involution \( \sigma_h \) on \( A \) and \( \theta \) on \( E \) have the same type (orthogonal or symplectic) if \( h \) is hermitian and have opposite types if \( h \) is skew-hermitian.

(2) If \( \theta \) is of the second kind on \( E \), the map \( h \mapsto \sigma_h \) defines a one-to-one correspondence between nonsingular hermitian forms on \( M \) upto a factor in \( F^\times \) invariant under \( \theta \) and involutions \( \sigma \) of the second kind on \( A \) such that \( \sigma(\alpha) = \theta(\alpha) \) for all \( \alpha \in F \).

Throughout the remaining of this section we will use the following notations: Let \( Z/F \) be a finite extension of fields, \( E \) a central simple algebra over \( Z \) and \( T \) is a central simple \( F \)-algebra contained in \( E \). Suppose that \( \theta \) is an involution (of any kind) on \( E \) which preserves \( T \).

**Definition 2.10 (Involution trace).** An \( F \)-linear map \( s : E \to T \) is called an involution trace if it satisfies the following conditions:

1. \( s(t_1xt_2) = t_1s(x)t_2 \) for all \( x \in E \) and \( t_1, t_2 \in T \);
2. \( s(\theta(x)) = \theta(s(x)) \) for all \( x \in E \);
3. if \( x \in E \) is such that \( s(\theta(x)y) = 0 \) for all \( y \in E \), then \( x = 0 \).

**Example 2.11 (Reduced Trace).** Let us recall the definition of a reduced trace in a central simple algebra \( A \) over \( F \) of degree \( n \), that is, \( A \) is such that if \( \Omega \) denotes an algebraic closure of \( F \), then \( A_\Omega = A \otimes_F \Omega \simeq M_n(\Omega) \). We may therefore fix an \( F \)-algebra embedding \( A \hookrightarrow M_n(\Omega) \) and view every element \( a \in A \) as a matrix in \( M_n(\Omega) \). Its characteristic polynomial has coefficients in \( F \) and is independent of the embedding of \( A \) in \( M_n(\Omega) \). It is called the reduced characteristic polynomial of \( A \) and is denoted

\[
Prd_{A,a}(X) = X^n - s_1(a)X^{n-1} + s_2(a)X^{n-2} - \cdots + (-1)^ns_n(a).
\]

The reduced trace and reduced norm of \( a \) are denoted by \( Trd_A(a) = s_1(a) \) and \( Nrd_A(a) = s_n(a) \) respectively. The bilinear form \( T_A : A \times A \to F \) defined by: \( T_A(x,y) = Trd_A(xy) \) for \( x,y \in A \) is nonsingular (Theorem 9.9, [Rei03]). In the above definition 2.10, if \( T = F = Z \), the reduced trace \( Trd_E : E \to F \) is an involution trace. The first condition for \( Trd_E \) being an involution trace follows directly from the definition. The second condition follows from 2.2 in [KMRT98] if \( \theta \) is of first kind and 2.16 in [KMRT98] if \( \theta \) is of second kind. The third condition follows from the fact that the bilinear reduced trace form is nonsingular.

**Example 2.12 (Linear Forms).** In definition 2.10, if \( E = Z \) and \( T = F \), every nonzero linear map \( l : Z \to F \) which commutes with \( \theta \) is an involution trace. The first two conditions follow directly from the definition. For the third condition, if \( x \in Z \) is
such that $s(\theta(x)y) = 0$ for all $y \in Z$, then $x = 0$ since $s \neq 0$ and $Z = \{ \theta(x)y | y \in Z \}$ if $x \neq 0$. Nonzero linear forms $Z \to F$ always exist if the extension $Z/F$ is separable. For example, $\text{Trd}_L$, which will be an involution trace (that is, nonzero linear form) for the trivial involution if and only if $Z/F$ is a separable field extension ([Knu91], Chapter I, 7.3.2).

**Remark 2.13.** Using an involution trace $s : E \to T$, we may define a structure of hermitian module over $T$ on every hermitian module over $E$ as follows. Suppose that $M$ is a finitely generated right module over $E$. Since $T \subset E$, we may also consider $M$ as a right $T$-module, and $\text{End}_E(M) \subset \text{End}_T(M)$. Suppose now that $h : M \times M \to E$ is a hermitian or skew-hermitian form with respect to $\theta$. We define $s_*(h) : M \times M \to T$ by

$$s_*(h)(x, y) = s(h(x, y)) \text{ for } x, y \in M.$$ 

In view of the properties of $s$, the form $s_*(h)$ is clearly hermitian over $T$ (with respect to $\theta$) if $h$ is hermitian, and skew-hermitian if $h$ is skew-hermitian.

The following is Proposition 4.7 in [KMRT98].

**Lemma 2.14.** If $h$ is nonsingular, then $s_*(h)$ is nonsingular and the adjoint involution $\sigma_{s_*(h)}$ on $\text{End}_T(M)$ extends the adjoint involution $\sigma_h$ on $\text{End}_E(M)$:

$$(\text{End}_E(M), \sigma_h) \subset (\text{End}_T(M), \sigma_{s_*(h)}).$$

### 3. Rational Group Algebras with Involution

Let $G$ be a finite group and $\sigma$ be an involution of $\mathbb{Q}G$. As $\mathbb{Q}G$ is semisimple, by Wedderburn Structure Theorem, $\mathbb{Q}G$ can be written as a product of simple algebras in the following way:

$$\mathbb{Q}G \cong M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k),$$

where $D_i$ are division algebras over $\mathbb{Q}$ such that the center $Z(M_{n_i}(D_i)) = Z(D_i) = \mathbb{Z}_i$ is a finite dimensional field extension over $\mathbb{Q}$. Thus $M_{n_i}(D_i)$ are central simple algebras over $\mathbb{Z}_i$. Also, each $D_i^{n_i}$ is a simple $\mathbb{Q}G$-module. Now, according to Remark 2.3 ($\mathbb{Q}G, \sigma$) thus decomposes into

$$(\mathbb{Q}G, \sigma) \cong (M_{a_1}(D_1), \sigma_{a_1}) \times \cdots \times (M_{a_r}(D_r), \sigma_{a_r}) \times (M_{b_1}(D'_1) \times M_{b'_1}(D'_1)^{\text{op}}, \sigma_{b_1})$$

$$\times \cdots \times (M_{b_t}(D'_t) \times M_{b'_t}(D'_t)^{\text{op}}, \sigma_{b_t})$$

(3.1)
where $\sigma(M_i(D_i)) = M_i(D_i)$ and $\sigma(M_j(D_j)) = M_j(D_j)^{op}$, for $1 \leq i \leq r$, $1 \leq j \leq t$.

We call the restriction of $\sigma$ to $M_i(D_i)$ as $\sigma_{a_i}$ and to $(M_j(D_j)) \times M_j(D_j)^{op}$ as $\sigma_{b_i}$ respectively. Now, each $M_n(D_i) \simeq End_{D_i}(D_i^{n_i})$, where $D_i^{n_i}$ can be viewed as a right vector space over $D_i$. From now on, we will work with only $M_n(D_i)$. In case it is of the form $M_j(D_j) \times M_j(D_j)^{op}$, the corresponding results can similarly be extended to the right vector space $D_j \times (D_j)^{op}$.

Let us fix $i$ and denoting $n_i, D_i$ and $\sigma_{n_i}$ as $n, D$ and $\sigma$ respectively, we concentrate on $(M_n(D), \sigma) \simeq (End_D(D^n), \sigma)$. As $M_n(D)$ is Brauer equivalent to $D$, by Theorem 2.4 there exists an involution, say $\theta$ on $D$ which is of the same kind as $\sigma$. Thus, according to Theorem 2.9 there exists a nonsingular hermitian or skew-hermitian form $h : D^n \times D^n \rightarrow D$ with respect to $\theta$ such that $\sigma$ is the adjoint involution of $h$, that is, $\sigma = \sigma_h$ and it satisfies $h(x, f(y)) = h(\sigma_h(f)(x), y)$ for all $x, y \in D^n$ and $f \in End_D(D^n)$.

Let $Z$ denote the center of $D$. Then $D$ is a finite dimensional central simple algebra over $Z$ which is again a finite field extension over $\mathbb{Q}$, hence separable. In the beginning of section 2 we have seen that $\theta$ preserves $Z$, hence $\mathbb{Q}$ (in fact, it is the identity on $\mathbb{Q}$). Thus we can choose a nonzero linear form $l : Z \rightarrow \mathbb{Q}$ (by Example 2.12) that commutes with $\theta$ restricted to $Z$. Let $Trd_D : D \rightarrow Z$ be the reduced trace of the central simple algebra $D$ over $Z$. Now take the composition of these two maps to define the map $s : D \rightarrow \mathbb{Q}$ where $s = l \circ Trd_D$.

**Claim:** $s$ is an involution trace. We check the conditions one by one.

(i) $s(\alpha_1 x \alpha_2) = (l \circ Trd_D)(\alpha_1 x \alpha_2) = \alpha_1 s(x) \alpha_2$ for all $\alpha_1, \alpha_2 \in \mathbb{Q} \subseteq Z$ and $x \in D$ follows directly from the definition of $l$ and $Trd_D$.

(ii) $s(\theta(x)) = (l \circ Trd_D)(\theta(x)) = l(\theta(Trd_D(x))) = \theta(l(Trd_D(x))) = \theta(s(x))$ for all $x \in D$ as $Trd_D$ is an involution trace and $l$ is a nonzero linear form that commutes with $\theta$ restricted to $Z$.

(iii) Let $x \in D$ be such that $s(\theta(x)y) = 0$ for all $y \in D$. This means $l(Trd_D(\theta(x)y)) = 0$ for all $y \in D$. Since $l$ is a nonzero linear form on a finite dimensional vector space $Z$ over $\mathbb{Q}$, we must have $Trd_D(\theta(x)y) = 0$ for all $y \in D$, which in turn implies that $x = 0$ as $Trd_D$ is an involution trace. Thus $s$ satisfies the third condition as well for being an involution trace.
Now, applying Remark 2.13 and Lemma 2.14 to $E = D$, $T = \mathbb{Q}$ and $M = D^n$, we get a nonsingular hermitian or skew hermitian form (according as $h$) with respect to $\theta$ on $\mathbb{Q}$ which is the identity on $\mathbb{Q}$ as the only nonzero involution on $\mathbb{Q}$ is the identity. The nonsingular form can be written as the following:

$$s_*(h) : D^n \times D^n \to \mathbb{Q}$$

such that

$$s_*(h)(x, y) = s(h(x, y)) \text{ for } x, y \in D^n.$$  

Also, $D^n$ is a right vector space over $\mathbb{Q}$ and $\text{End}_D(D^n) \subset \text{End}_{\mathbb{Q}}(D^n)$. The adjoint involution $\sigma_{s_*(h)}$ on $\text{End}_D(D^n)$ extends the adjoint involution $\sigma = \sigma_h$ on $\text{End}_D(D^n)$, that is,

$$(\text{End}_D(D^n), \sigma_h) \subset (\text{End}_{\mathbb{Q}}(D^n), \sigma_{s_*(h)}).$$

In view of the above discussion 3.11 can be written as:

$$(\mathbb{Q}G, \sigma) \simeq \prod_{i=1}^r (\text{End}_{D_i}(D_i^{a_i}), \sigma_{a_i}) \times \prod_{j=1}^r \left( \text{End}_{D_j^{b_j \times D_j^{b_j}}} (D_j^{b_j} \times (D_j^{op})^{b_j}), \sigma_{b_j} \right)$$

$$\subset \prod_{i=1}^r (\text{End}_{\mathbb{Q}}(D_i^{a_i}), \sigma_{s_*(h_{a_i})}) \times \prod_{j=1}^r \left( \text{End}_{\mathbb{Q} \times \mathbb{Q}}(D_j^{b_j} \times (D_j^{op})^{b_j}), \sigma_{s_*(h_{b_j})} \right),$$

where $\sigma_{a_i} = \sigma_{h_{a_i}}$ are the adjoint involutions of the nonsingular hermitian or skew hermitian forms $h_{a_i} : D_i^{a_i} \times D_i^{a_i} \to D_i$ with respect to the involution $\theta_{a_i}$ (which is of the same kind as $\sigma_{h_{a_i}}$) on $D_i$ and $\sigma_{b_j} = \sigma_{h_{b_j}}$ are the adjoint involutions of the nonsingular hermitian forms $h_{b_j} : (D_j^{b_j} \times (D_j^{op})^{b_j}) \to D_j^{b_j} \times (D_j^{op})^{b_j}$ with respect to the involution (of second kind) $\theta_{b_j}$ on $D_j^{b_j} \times D_j^{op}$.

4. PROOF OF THE MAIN THEOREMS

Note. The set $\{x \in \text{End}_D(D^n) \mid h(xu, v) + h(u, xv) = 0 \text{ for all } u, v \in D^n\}$, where $h : D^n \times D^n \to D$ is a nonsingular hermitian or skew-hermitian form on $D^n$ with respect to some involution $\theta$ (of any kind) on $D$, is a Lie algebra over $\mathbb{Q}$.

Now, $D^n$ is a simple $\mathbb{Q}G$ module. Thus each $f \in \mathbb{Q}G$ acts on $D^n$. Thus the projection, say $f_i$ of $f$ on any of the factors $M_n(D) \simeq \text{End}_D(D^n)$ of $\mathbb{Q}G$ can be viewed as an element in $\text{End}_D(D^n)$. Now we prove the following characterization of the projection of the skew-symmetric elements on one of the summands of $\mathbb{Q}G$. 


Lemma 4.1. The image of $\mathbb{Q}G^-_r$ under the projection of $\mathbb{Q}G$ onto $M_n(D)$ consists of all linear transformations $f_i$ in $\text{End}_D(D^n)$ such that $s_*(h)(f_i(x), y) + s_* (h) (x, f_i(y)) = 0$ for all $x, y \in D^n$.

Proof. Recall that $\sigma = \sigma_h$ is the adjoint involution of the nonsingular hermitian or skew-hermitian form $h$ on $D^n$ with respect to $\theta$, that is, $h(x, f(y)) = h(\sigma_h(f)(x), y)$ for all $x, y \in D^n$ and $f \in \text{End}_D(D^n)$. If $f_i$ belongs to the image of $\mathbb{Q}G^-_r$ under the projection of $\mathbb{Q}G$ onto $M_n(D)$, then $\sigma(f_i) = -f_i$, by definition of $\mathbb{Q}G^-_r$. The involution $\sigma_{s_*(h)}$ of $\text{End}_D(D^n)$ extends the involution $\sigma_h$ on $\text{End}_D(D^n)$. That is, $\sigma_{s_*(h)}$ restricted to $\text{End}_D(D^n)$ is $\sigma_h$. Thus, as $f_i \in \text{End}_D(D^n)$, we have $\sigma_{s_*(h)}(f_i) = \sigma_h(f_i) = -f_i$. This implies $h(x, f_i(y)) = h(\sigma_h(f_i)(x), y) = -h(f_i(x), y)$. So we get

$$\sigma(f_i) = -f_i \iff s_*(h)(f_i(x), y) + s_* (h) (x, f_i(y)) = 0 \text{ for } x, y \in D^n.$$

4.1. Proof of Theorem 1.2 Let $M = \prod_{i=1}^r D_i^{a_i} \times \prod_{j=1}^t \left( D_j^{b_j} \times \left( D_j^{\text{op}}\right)^{b_j} \right)$. Then $M$ is a right vector space over $\mathbb{Q}$ and also a $\mathbb{Q}G$-module. Define $h : M \times M \rightarrow \mathbb{Q}$ by

$$h \left( \sum_{i=1}^r x_i + \sum_{j=1}^t x'_j, \sum_{i=1}^r y_i + \sum_{j=1}^t y'_j \right) = \bigoplus_{i=1}^r s_*(h_{a_i})(x_i, y_i) \oplus \bigoplus_{j=1}^t s_*(h_{b_j})(x'_j, y'_j),$$

where $x_i, y_i \in D_i^{a_i}$ and $x'_j, y'_j \in D_j^{b_j} \times \left( D_j^{\text{op}}\right)^{b_j}$.

Then $h$ is a nonsingular form (hermitian or skew-hermitian) on $M$ with respect to the trivial involution on $\mathbb{Q}$ such that the given involution $\sigma$ on $\mathbb{Q}G$ is the adjoint involution of $h$. With the above notations, we will show that Equation 1.2 of Theorem 1.2 holds.

Let $f \in \mathbb{Q}G^-_r \subset (\mathbb{Q}G, \sigma)$. Thus $f = \sum_{i=1}^r f_i + \sum_{j=1}^t f'_j$, where each $f_i$ (resp. $f_j$) belongs to the image of $\mathbb{Q}G^-_r$ under the projection of $\mathbb{Q}G$ onto $\text{End}_{D_i}(D_i^{a_i})$ (resp. $\text{End}_{D_j \times D_j^{\text{op}}}(D_j^{b_j} \times \left( D_j^{\text{op}}\right)^{b_j})$). Writing $x = \sum_{i=1}^r x_i + \sum_{j=1}^t x'_j$ and $y = \sum_{i=1}^r y_i + \sum_{j=1}^t y'_j$, and using Lemma 4.1 we have:

$$\sigma(f) = -f$$

$$\iff \bigoplus_{i=1}^r \sigma_{h_{a_i}}(f_i) \oplus \bigoplus_{j=1}^t \sigma_{h_{b_j}}(f'_j) = -\sum_{i=1}^r f_i - \sum_{j=1}^t f'_j$$

$$\iff \bigoplus_{i=1}^r (s_*(h_{a_i})(f_i(x_i), y_i) + s_* (h_{a_i}) (x_i, f_i(y_i)))$$
\[ \bigoplus_{j=1}^{t} (s_*(h_{b_j}) (f'_j(x'_j), y'_j) + s_*(h_{b_j}) (x'_j, f'_j(y'_j))) = 0 \]
\[ \iff h(f(x), y) + h(x, f(y)) = 0. \]

4.2. Proof of Theorem 1.3. It follows from the discussion in Section 3 and Lemma 4.1, the image of \( \mathbb{Q}G^- \) under the projection of \( \mathbb{Q}G \) onto \( M_n(D) \) is a Lie algebra. Let \( V = D^n \). Then \( V \) is an irreducible left \( \mathbb{Q}G \) module. From definition 2.7 and Theorem 2.9 it follows that if \( \sigma \) is of first kind on \( \text{End}_D(V) \), then \( \sigma \) restricted to \( \text{End}_D(V) \) is orthogonal (resp. symplectic) if the involution \( \theta \) on \( D \) is orthogonal (resp. symplectic) provided the corresponding nonsingular form \( h : V \times V \to D \) with respect to \( \theta \) on \( D \) is hermitian. If the nonsingular form \( h \) is skew-hermitian, then \( \sigma \) restricted to \( \text{End}_D(V) \) is orthogonal (resp. symplectic) if \( \theta \) is symplectic (resp. orthogonal). The degree of the central simple algebra \( \text{End}_D(V) \) over its center \( Z \) is \( n \). By Lemma 2.8 the dimension of the Lie algebra \( \text{End}_D(V)_{\sigma}^- \) is \( n(n-1)/2 \) if \( \sigma \) restricted to it is orthogonal and the dimension is \( n(n+1)/2 \) if \( \sigma \) restricted to it is symplectic. Whenever the involution \( \sigma \) is symplectic, \( n \) is even. If \( \sigma \) is of second kind (that is of unitary type) on \( \text{End}_D(V) \) or \( \text{End}_{D \times D^{op}}(V \times V^{op}) \), then the dimension is \( n^2 \). Denoting the Lie algebras \( \text{End}_D(V)_{\sigma}^- \) in the orthogonal, symplectic and unitary cases as \( \mathfrak{o}(V), \mathfrak{sp}(V) \) and \( \mathfrak{gl}(V) \) respectively, we get the decomposition structure of \( \mathbb{Q}G^-_{\sigma} \) as proposed.

5. Conclusion

An application of Theorem 1.2 is the following:

Remark 5.1. If \( \sigma_1 \) be an involution on \( \mathbb{Z}G \), it can be linearly extended to an involution \( \sigma \) of \( \mathbb{Q}G \). Then by Theorem 1.2, we will get a right vector space \( M \) on \( \mathbb{Q} \) which is a \( \mathbb{Q}G \)-module as well and a nonsingular hermitian or skew-hermitian form \( h : M \times M \to \mathbb{Q} \) such that \( \sigma \) is the adjoint involution of \( h \). Now, let \( \mathcal{O} \) be a full \( \mathbb{Z}G \)-lattice of the \( \mathbb{Q}G \)-module \( M \) (a \( \mathbb{Z}G \)-lattice by definition is a \( \mathbb{Z}G \)-module which is free and finitely generated as a \( \mathbb{Z} \)-module, that is, as an abelian group and such lattices always exist). Then \( h \) restricted to \( \mathcal{O} \times \mathcal{O} \) is a hermitian form, say, \( h_1 : \mathcal{O} \times \mathcal{O} \to \mathbb{Q} \) and we can see

\[ \mathbb{Z}G^-_{\sigma_1} = \{ f \in \mathbb{Z}G \mid h_1(f(x), y) + h_1(x, f(y)) = 0 \text{ for all } x, y \in \mathcal{O} \}. \]

Acknowledgements. The author is grateful to Professor I.B.S. Passi for helpful discussions and references. The author is also thankful to DAE (Government of India) and National Board for Higher Mathematics for providing fellowship and IISER Mohali for providing good research facilities when this project was carried out.
References

[Ami69] S.A. Amitsur. Identities in rings with involutions. Israel J. Math., 7:63–68, 1969.
[CM07] O.B. Cristo and C.P. Milies. Commutativity of skew elements in group rings. Proc. Edinburgh Math. Soc., 50:37–47, 2007.
[CT07] A.M. Cohen and D.E. Taylor. On a certain Lie algebra defined by a finite group. Amer. Math. Monthly, 114:633–639, 2007.
[GM03] A. Giambruno and C.P. Milies. Unitary Units and skew elements in group algebras. Manuscripta Math., 111:195–209, 2003.
[GS93] A. Giambruno and S.K. Sehgal. Lie nilpotence of group rings. Comm. Algebra, 21:4253–4261, 1993.
[JM05] E. Jespers and M. Ruiz Marín. Antisymmetric elements in group rings. J. Algebra Appl., 4:341–353, 2005.
[JM06] E. Jespers and M. Ruiz Marín. On symmetric elements and symmetric units in group rings. Comm. Algebra, 34:727–736, 2006.
[KMRT98] M.A. Knus, A. Merkurjev, M. Rost, and J.P. Tignol. The Book of Involutions. Colloquium Publications, Vol. 44, American Mathematical Society, 1998.
[Knu91] M.A. Knus. Quadratic and Hermitian Forms over Rings. Grundlehren der Mathematischen Wissenschaften, Vol. 294, Springer, 1991.
[LSS09] G.T. Lee, S.K. Sehgal, and E. Spinelli. Group algebras whose symmetric and skew elements are Lie solvable. Forum Math., 21:661–671, 2009.
[Mar10] I. Marin. Group algebras of finite groups as Lie algebras. Comm. Algebra, 38:2572–2584, 2010.
[Rei03] I. Reiner. Maximal Orders. London Mathematical Society Monographs New Series, Vol. 28, The Clarendon Press, Oxford University Press, 2003.
[ZS81] A.E. Zaleskii and M.B. Smirnov. Lie algebra associated with linear group. Comm. Algebra, 9:2075–2100, 1981.

Dishari Chaudhuri, Department of Mathematical Sciences, Indian Institute of Science Education and Research Mohali, Sector-81, Knowledge City, S.A.S. Nagar, Mohali-140306, Punjab, India

E-mail address: disharı@iisermohali.ac.in, disharı@iitg.ac.in