PORTUGALIAE MATHEMATICA
Vol. 53 Fasc. 2 – 1996

SEPARABLE GROUP-RING EXTENSIONS

Surjeet Singh and L.A.-M. Hanna

Introduction

Let G be a finite group and R be any ring with identity $1_R \neq 0$. The separability of the group-ring RG over certain subrings of RG has been studied by many authors (see [1], [2], [8], [9]). It is well known that RG is a separable extension of R if and only if $|G|\,1_R$ is invertible in R. If RG is a separable extension of R, then RG has unique separating idempotent over R if and only if G is abelian. Let G be an arbitrary group (not necessarily finite) and H be a subgroup of G. On similar lines as for the above mentioned results, we prove the following results

i) RG is a separable extension of RH if and only if $[G:H]$ is finite and $[G:H]\,1_R$ is invertible in R.

ii) Let RG be a separable extension of RH; then RG has only one separating idempotent over RH if and only if every finite conjugate class in G is an H-*orbit*, in the sense that if two elements $a,b \in G$ are in the same finite conjugate class, then $b = x^{-1}\,a\,x$ for some $x \in H$.

This leads to the following condition on a subgroup H of a finite group.

(S) Any conjugate class in G is an H-*orbit* .

There exist large number of pairs (G,H), such that H satisfies (S), but $G \neq HK$, for any normal subgroup K of G, with $H \cap K = 1$. Such pairs of *2-groups* were found by using *GAP*-computer package [6]. For all such pairs (G,H), with G a *2-group*, $|G| \leq 32$, we observed that $G = HZ(G)$. But we found three groups G, of order 64, having subgroups H, satisfying (S), $|H| = 32$, but $G \neq HZ(G)$; in fact $Z(H) = Z(G)$. In section 2, we endeavor to prove that for any group G of order less than 64, if a subgroup H of G satisfies (S) then $G = HZ(G)$.

Received: May 19, 1995; *Revised*: September 1, 1995.

Answer is given in the affirmative except for $|G| = 48$. However, in the results (3.2) through (3.5), some general, sufficient conditions on the orders of G and H are given under which $G = HZ(G)$, whenever H satisfies (S).

1 – Preliminaries

Let R be any ring with identity $1 \neq 0$ and S be any subring of R containing 1. Let $\varphi\colon R \otimes_S R \to R$ be the (R,R)-homomorphism such that $\varphi(\sum_i a_i \otimes b_i) = \sum a_i\, b_i$. As defined by Hirata and Sugano [3], R is called a separable extension of S, if there exists $z = \sum_i a_i \otimes b_i \in R \otimes_S R$ such that $\varphi(z) = 1$ and $r\,z = z\,r$ for every $r \in R$; such an element z is called a separating idempotent of R over S. The center of R will be denoted by $Z(R)$. Let G be any group and H be a subgroup of G. Any $a, b \in G$ are said to be in the same H-*orbit* if $b = x^{-1}\,a\,x$ for some $x \in H$. A set $\{g_\alpha\colon\ \alpha \in \Lambda\}$ of right coset representatives of H in G is called a right transversal of H in G ([4, p. 5]). $Z(G)$ and $\Delta(G)$ denote the center and the $F.C$ subgroup of G, respectively [4]. Let K be a non empty subset of G, then the subgroup of G generated by K and the centralizer of K are denoted by $\langle K\rangle$ and $\mathrm{Centl}(K)$, respectively. For $a, b \in G$, $[a,b]$, $N(a)$ and $o(a)$ denote the commutator $a^{-1}\,b^{-1}\,a\,b$, the centralizer of a and the order of a, respectively. Consider a non zero $x = \sum a_g\, g \in RG$, then the support of x, denoted by $\mathrm{supt}(x)$, is the set $\{g \in G\colon\ a_g \neq 0\}$. For any set X, $|X|$ denotes the cardinality of X. For some general concepts on rings and modules, one may refer to Stenström [7], and for group-rings to Passman [4].

2 – Group rings

Throughout H is a subgroup of a group G, $T = \{g_\alpha :\ \alpha \in \Lambda\}$ is a right transversal of H in G, with $g_1 = 1 \in T$, and R is any ring with identity $1 \neq 0$. Any element of $RG \otimes_{RH} RG$ is uniquely expressible as $\sum_\alpha a_\alpha \otimes g_\alpha$, $a_\alpha \in RG$, and $a_\alpha \neq 0$ for finitely many $\alpha \in \Lambda$. An $x \in RG \otimes_{RH} RG$ is called a commutant element if $a\,x = x\,a$ for every $a \in RG$. We write P for $RG \otimes_{RH} RG$. The proof of the following is on familiar lines, as for the special case of $H = 1$ (see proof of [8, Lemma 1]).

Lemma 2.1. *An $x = \sum_\alpha a_\alpha \otimes g_\alpha \neq 0$ in P, is a commutant element if and only if, $[G:H] < \infty$, $a_\beta = g_\beta^{-1}\, a_1$, for every $\beta \in \Lambda$ and $a_1 = \sum_g r_g\, g \in Z(R)\,\Delta(G)$ such that for $g \in \mathrm{supt}(a_1)$, $r_g = r_{g'}$ whenever g' is in the H-orbit of g.*

For any finite non empty subset X of G, y_x denotes the sum in RG, of elements of X. Clearly, $y_{\{1\}} = 1$. Consider a non zero commutant element $x \in P$, then $x = \sum_\beta g_\beta^{-1}\, a_1 \otimes g_\beta$. The above lemma gives

$$a_1 = r_1 + \sum_{i=2}^{k} r_{A_i}\, y_{A_i} \ ,$$

where A_i are finitely many finite H-*orbits* in G none equal to $\{1\}$, and $r_1, r_{A_i} \in Z(R)$.

Lemma 2.2. *Let C be a conjugate class in G, $b, b' \in C$, and A be any H-orbit in C. Then*

$$B = \Big\{\alpha \in \Lambda \colon\ g_\alpha^{-1}\, u\, g_\alpha = b \ \text{ for some } u \in A\Big\}$$

and

$$B' = \Big\{\alpha \in \Lambda \colon\ g_\alpha^{-1}\, u\, g_\alpha = b' \ \text{ for some } u \in A\Big\}$$

have the same cardinality.

Proof: Now, $b' = x^{-1}\, b\, x$ for some $x \in G$. Let $\alpha \in B$, then for some $u \in A$, $g_\alpha^{-1}\, u\, g_\alpha = b$. Now, $g_\alpha\, x = h_{t(\alpha)}\, g_{t(\alpha)}$ for some $h_{t(\alpha)} \in H$ and $t(\alpha) \in \Lambda$,

$$u' = h_{t(\alpha)}^{-1}\, u\, h_{t(\alpha)} \ \in\ A \ ,$$

and

$$b' = g_{t(\alpha)}^{-1}\, u'\, g_{t(\alpha)} \ .$$

This gives $t(\alpha) \in B'$. The mapping $t \hookrightarrow t(\alpha)$ is a one-to-one mapping of B into B'. So that, $|B| \le |B'|$. Similarly, $|B'| \le |B|$. Hence, $|B| = |B'|$. ∎

Henceforth, let $|\Lambda| < \infty$. Let C be a finite conjugate class in G. Consider an H-*orbit* A in C. The above lemma gives a positive integer λ_A which for any $b \in C$, equals

$$\Big|\Big\{\alpha \in \Lambda \colon\ g_\alpha^{-1}\, u\, g_\alpha = b \ \text{ for some } u \in A\Big\}\Big| \ .$$

Let us call λ_A, the weight of C relative to A. If $C = \{b_1, b_2, ..., b_t\}$, and $C = A_1 \cup A_2 \cup ... \cup A_k$ is the decomposition of C into H-*orbits*, then for any $r_i \in R$,

$$\sum_\alpha \sum_i g_\alpha^{-1}\, r_i\, y_{A_i}\, g_\alpha = \sum_{j=1}^{t} \Big(\sum_i \lambda_{A_i}\, r_i\Big)\, b_j = \Big(\sum_i \lambda_{A_i}\, r_i\Big)\, y_C \ .$$

The following theorem generalizes [8, Theorem 2] and some other results in [9].

Theorem 2.3. *Let H be any subgroup of a group G, and R be any ring. The following hold.*

i) *RG is a separable extension of RH if and only if $[G:H]<\infty$ and $[G:H]\,1_R$ is invertible in R.*

ii) *If RG is separable over RH, then RG has a unique separating idempotent over RH if and only if each finite conjugate class in G is an H-orbit.*

Proof: **i)** Let RG be a separable extension of RH. So, there exists $z \in RG \otimes_{RH} RG$ such that under the *RG-bimodule* homomorphism $\varphi : RG \otimes_{RH} RG \to RG$, such that $\varphi(a \otimes b) = a\,b$, we have $\varphi(z) = 1$ and $a\,z = z\,a$ for any $a, b \in RG$. By (2.1), $[G:H] = n < \infty$ and $z = \sum_\alpha g_\alpha^{-1}\,a_1 \otimes g_\alpha$ with $a_1 = r_1 + \sum_i r_i\,y_{A_i}$, where A_i are some finite H-orbits other than $\{1\}$; $r_1, r_i \in Z(R)$. Then

$$1 = \varphi(z) = n\,r_1 + \sum_{i,\alpha} g_\alpha^{-1}\,r_i\,y_{A_i}\,g_\alpha$$

yields $n\,r_1 = 1$. Thus, $n\,1_R$ is invertible in R. Conversely, if $s = n\,1_R$ is invertible in R, then

$$z_0 = \frac{1}{s}\sum_\alpha g_\alpha^{-1} \otimes g_\alpha$$

is a separating idempotent of RG over RH.

ii) Let RG be separable over RH. Let RG have only one separating idempotent over RH. This one is $z' = \frac{1}{s}\sum_\alpha g_\alpha^{-1} \otimes g_\alpha$. Suppose there exists a finite conjugate class C in G, such that $C = A_1 \cup A_2 \cup \ldots \cup A_k$, where A_i are disjoint H-*orbits*, and $k \geq 2$. If one of λ_{A_1} and λ_{A_2} is non zero in R, then

$$z = \sum_\alpha g_\alpha^{-1}(\lambda_{A_2}\,y_{A_1} - \lambda_{A_1}\,y_{A_2}) \otimes g_\alpha \neq 0\ ,$$

and

$$\varphi(z) = (\lambda_{A_1}\,\lambda_{A_2} - \lambda_{A_2}\,\lambda_{A_1})\,y_C = 0\ .$$

This gives a separating idempotent $z_0 + z$ different from z_0. If $\lambda_{A_1} = 0 = \lambda_{A_2}$ in R, then

$$z_0 + \sum_\alpha g_\alpha^{1}(y_{A_1} + y_{A_2}) \otimes g_\alpha$$

is a separating idempotent other than z_0. This is a contradiction. Hence every finite conjugate class in G is an H-*orbit*. Conversely, let every finite conjugate class in G be an H-*orbit*, then any non zero commutant element in $RG \otimes_{RH} RG$ is of the form

$$z = \sum_\alpha g_\alpha^{-1}\, a_1 \otimes g_\alpha$$

where $a_1 = \sum_i r_i\, y_{C_i}$, for some finitely many distinct finite conjugate classes C_i in G and $r_i \neq 0$ in $Z(R)$, $\varphi(z) = n \sum_i r_i\, y_{C_i}$, $n = [G : H]$, gives $\varphi(z) \neq 0$. Hence, R has only one separating idempotent over RH. ∎

3 – Finite groups

Throughout G is a finite group, and H is a subgroup of G. We consider the condition

(S) Any conjugate class in G is an H-*orbit* .

If R is any ring such that $|G|$ is invertible in R, by (2.3) RG has only one separating idempotent over RH if and only if H satisfies (S). This observation motivates us to study the above condition. If $G = HZ(G)$, obviously, H satisfies (S). There exist groups G having subgroups H satisfying (S), but $G \neq HZ(G)$. Some such groups of order 64 were found by using GAP [6]. One such a group is described at the end of this paper. We endeavor to prove that for any group G of order less than 64, if a subgroup H satisfies (S), then $G = HZ(G)$. We shall give a number of sufficient conditions on $|H|$ and $|G|$ under which $G = HZ(G)$, whenever H satisfies (S). We start with the following obvious results.

Lemma 3.1. *Let H be a subgroup of a finite group G. Then:*

i) *H satisfies (S) if and only if $G = HN(a)$ for every $a \in G$.*

ii) *If H satisfies (S), then* $\mathrm{Centl}(H) \leq Z(G)$, *and $Z(G) \cap H = Z(H)$.*

iii) *If H satisfies (S), then G/H is an abelian group, $G' = [H, G] = H'$; further if H is abelian, then G is abelian.*

iv) *If H satisfies (S), then any normal subgroup of H is a normal subgroup of G.*

Proposition 3.2. *If $|G| = p\,q\,s$, where p and q are two distinct primes, and H is a non abelian subgroup of G of order $p\,q$, satisfying (S), then $G = HZ(G)$.*

Proof: $Z(H) = 1$. Let $a, b \in H$, such that $o(a) = p$, $o(b) = q$. To be definite, let $p < q$. As $G = HN(a)$, by (3.1), $|N(a)| = p\,s$. Similarly, $|N(b)| = q\,s$. As $\langle b \rangle$ is a normal subgroup of H, by (3.l) iv), $\langle b \rangle$ is a normal subgroup of G. So, $N(b)$ is a normal subgroup of G. Then $p\,q \,|\, |N(a)\,N(b)|$ yields $s \,|\, |N(a) \cap N(b)|$. Obviously, $N(a) \cap N(b) = \mathrm{Centl}(H)$. So, $N(a) \cap N(b) \leq Z(G)$, by (3.1) ii). However, $N(a) \cap N(b) \cap H = 1$. This yields, $Z(G) = N(a) \cap N(b)$, and $G = HZ(G)$. ∎

Theorem 3.3. *Let $|G| = p^2\,q\,s$, where p and q are primes, such that $p < q$, and H he a subgroup of G of order $p^2\,q$, satisfying (S), then $G = HZ(G)$.*

Proof: Let $K = \langle c \rangle$, be a *Sylow q-subgroup* of H. Consider $q > 3$. Then, K is a normal subgroup of H, hence by (3.1) iv) it is normal in G. Now $|Z(H)|$ is 1 or p. Let P be a *Sylow p-subgroup* of H.

Case (I): $Z(H) = 1$. Then P is cyclic. Let $P = \langle d \rangle$. As $G = HN(d)$, $|N(d)| = p^2\,s$. Also, $|N(c)| = q\,s$. $H = \langle c, d \rangle$, yields $N(c) \cap N(d) = \mathrm{Centl}(H) \leq Z(G)$, $H \cap (N(c) \cap N(d)) = 1$. Also $H \leq N(c)\,N(d)$, yields $G = N(c)\,N(d)$. So that $p^2\,q\,s = |N(d)\,N(c)|$, $|N(d) \cap N(c)| = s$. Hence, $G = HZ(G)$.

Case (II): $|Z(H)| = p$. Then, $|N(c)| = p\,q\,s$. Let P be cyclic. Then $|N(c) \cap N(d)| = p\,s$, and once again $G = HZ(G)$. Suppose P is not cyclic, then $H = Z(H) \times L$, where $|L| = p\,q$. Then for any $x \in G$, $G = HN(x) = LN(x)$. So by (3.2), $G = LZ(G) = HZ(G)$.

We now consider $q = 3$. Then $p = 2$, $|H| = 12$. If a *Sylow 2-subgroup* of H is cyclic, on similar lines as when $q > 3$, we get $G = HZ(G)$. Let *Sylow 2-subgroup* of H be not cyclic. Suppose *Sylow 3-subgroup* of H is not normal. We get another *Sylow 3-subgroup* $K' = \langle c' \rangle$ of H. Then $|N(c)| = |N(c')| = 3s$, $N(c) \cap N(c') \cap H = 1$. Then, $|N(c)\,N(c')| \leq 12\,s$, yields $|N(c) \cap N(c')| \geq \frac{3}{4}\,s$ and hence, $|H(N(c) \cap N(c'))| \geq \frac{3}{4}|G|$. Consequently, $G = H(N(c) \cap N(c'))$. However, $H = \langle c, c' \rangle$. Thus, $N(c) \cap N(c') \leq Z(G)$. If *Sylow 3-subgroup* of H is normal, then $H = L \times L_1$, $|L| = 6$, $|L_1| = 2$. Once again by (3.2), $G = HZ(G)$. ∎

Theorem 3.4. *Let $|G| = p^2\,q\,s$, where p, q and s are prime numbers and $p > q$, then for any nonabelian subgroup H of G of order $p^2\,q$, satisfying (S), $G = HZ(G)$.*

Proof: Let P be a *Sylow p-subgroup* of H, and $K = \langle c \rangle$ be a *Sylow q-subgroup* of H. Now P is a normal subgroup of G.

Case (I): P, a cyclic group. So for some $a \in P$, $P = \langle a \rangle$; then $Z(H) = 1$. By using (3.1), we get $|N(a)| = p^2\,s$, $|N(c)| = q\,s$, and $|N(a) \cap N(c)| \geq s$. However, $H \cap N(a) \cap N(c) = 1$ and $N(a) \cap N(c) \leq Z(G)$. This yields $G = H \times Z(G)$.

Case (II): P is not cyclic. If $Z(H) \neq 1$, then $H = Z(H) \times L_1$ with $|L_1| = p\,q$. By (3.2), $G = L_1 Z(G) = HZ(G)$. Let $Z(H) = 1$. If for some $a \in H$ with $o(a) = p$, $H = \langle a, c\rangle$, as in Case (I), we get $G = HZ(G)$. Suppose $H \neq \langle a, c\rangle$, for any $a \in H$ with $o(a) = p$, then $H = \langle a, b, c\rangle$ for some $a, b \in H$ satisfying $o(a) = p = o(b)$, $c^{-1}\,a\,c = a^{\lambda}$, $c^{-1}\,b\,c = b^{\lambda}$ for some λ, satisfying $2 \leq \lambda \leq p-1$, $c^{1}\,x\,c = x^{\lambda}$ for any $x \in P$. If $N(a) = N(b)$, then $N(a) \cap N(c) \leq Z(G)$ and $|N(a) \cap N(c)| \geq s$. So, $G = HZ(G)$.

Let $N(x) \neq N(y)$ for any $x, y \in H$ for which $P = \langle x, y\rangle$. As $[G : N(a)] = q$, $G = N(a)\,N(b)$, and $|N(a) \cap N(b)| = p^2(\frac{s}{q})$. So, $s = q$, $|G| = p^2\,q^2$, $|N(c)| = q^2$, $|N(a)| = p^2\,q$, $P = N(a) \cap N(b)$, and $|N(a) \cap N(c)| = q = |N(b) \cap N(c)|$. Suppose $N(c)$ is cyclic, then $N(a) \cap N(c)$ being the unique subgroup of $N(c)$ of order q, give $N(a) \cap N(c) = \langle c\rangle = N(b) \cap N(c)$. This gives H is abelian. This is a contradiction. Hence $N(c)$ is not cyclic. If $N(a) \cap N(c) = N(b) \cap N(c)$, then for some $d \in N(c)$, such that $d \notin \langle c\rangle$, $d \in N(a) \cap N(b)$. This gives $N(a) = P\langle d\rangle = N(b)$. This is a contradiction. So, $N(a) \cap N(c) \neq N(b) \cap N(c)$. We get $g \in (N(a) \cap N(c)) \backslash (N(b) \cap N(c))$. Then $N(c) = \langle c, g\rangle$, $g^{-1}\,b\,g = b^{j}$ for some j, with $2 \leq j \leq p-1$. Then $N(ab) \cap N(c) = 1$. On the other hand, as for a, $|N(ab) \cap N(c)| = q$. This is a contradiction. Hence the result follows. ∎

Proposition 3.5. *If $|G| = p^3\,s$, for some prime number p, and H is a nonabelian subgroup of G of order p^3, satisfying (S), then $G = HZ(G)$.*

Proof: Now, $H = \langle a, b\rangle$, for some a, b not in $Z(H)$, and $|Z(H)| = p$. By using (3.1) we get $|N(a)| = p^2\,s = |N(b)|$, $|H \cap N(a) \cap N(b)| = p$ and $N(a) \cap N(b) \leq Z(G)$. As $|N(a) \cap N(b)| \geq p\,s$, it is immediate that $G = HZ(G)$. ∎

Let n be any positive integer less than 64, other than 32, 48 and 60. Let G be a group of order n, then any proper subgroup of G is either abelian or of order of the form given in (3.2) to (3.5), so $G = HZ(G)$. Let $|G| = 60$, in view of (3.2) to (3.5), we consider a nonabelian subgroup H of G of order 30, satisfying (S). H has a normal cyclic subgroup $L = \langle a\rangle$ of order 15. Let $b \in H$ be of order 2. Then $|N(a)| = 30$, $4 \,|\, |N(b)|$. So that $2 \,|\, |Z(G)|$. If $Z(G) \not\leq H$, then $G = HZ(G)$. If $Z(G) \leq H$, then $H = LZ(G)$, and L satisfies (S). By (3.2), $G = LZ(G)$. This is a contradiction. Hence, $Z(G) \not\leq H$, and $G = HZ(G)$. We get:

Lemma 3.6. *Let $|G| = 60$, then for any subgroup H of G satisfying (S), $G = HZ(G)$.*

Lemma 3.7. *Let $|G| = 32$, then for any nonabelian subgroup H of G, satisfying (S), $G = HZ(G)$.*

Proof: In view of (3.5) we only consider the case $H=16$. Suppose $Z(G) \leq H$. Then by (3.1), $Z(H) = Z(G)$. By Scott, [6.5.1, p. 146], H has an abelian subgroup L of order 8. Suppose H has another abelian subgroup L_1 of order 8. Then $|L \cap L_1| = 4$, $Z(H) = L \cap L_1$ and $L/Z(H) = \langle \overline{x} \rangle$ for some $x \in L \backslash Z(H)$. Then for any a, b in $L \backslash Z(H)$, $N(a) = N(b)$, and by (3.1) $|N(a)| = 16$. Thus, $T = \mathrm{Centl}(L) = N(a)$ for any $a \in L \backslash Z(H)$. Similarly, $T_1 = \mathrm{Centl}(L_1)$ is of order 16. Further T and T_1 are abelian, $T \cap T_1 \leq Z(G)$ and $|T \cap T_1| \geq 8$. This is a contradiction. Hence H has a unique abelian subgroup L of order 8. This in turn yields, $|Z(H)| = 2$. Suppose $\overline{H} = H/Z(H)$ has an element $\overline{a}$ of order 4. Then $|N(a)| = 16$, $\langle Z(H), a \rangle \leq Z(N(a))$, gives $N(a)$ is abelian. Choose $a, b \in H$ such that $a\,b \neq b\,a$. Then $|N(b)| \geq 8$. As $\langle Z(H), b \rangle \leq Z(N(b))$, we get a subgroup T of $N(b)$ of order 8 such that $\langle Z(H), b \rangle \leq T$. As $N(a)$ is an abelian normal subgroup of order 16, $G = N(a)\,T$, $|N(a) \cap T| = 4$ and $N(a) \cap T \leq Z(G)$. This is a contradiction, as $|Z(G)| = 2$. Hence, $\overline{H}$ is elementary abelian. Let $Z(H) = \{e, d\}$. We can find $\overline{a}, \overline{b}, \overline{c} \in \overline{H}$ such that $\overline{H} = \langle \overline{a}, \overline{b}, \overline{c} \rangle$, $L = \langle a, b, d \rangle$. Then $a\,b \neq b\,a$, $a\,c \neq c\,a$, otherwise we get an abelian subgroup of H of order 8, other than L. Now $N(a) \cap L = \{e, d\}$, $|N(a)| \geq 8$, gives $G = LN(a)$. As $\overline{a}\,\overline{b} = \overline{b}\,\overline{a}$, we get $b\,a = a\,b\,d$. Similarly, $c\,a = a\,c\,d$. Then, $c\,b\,a = c\,a\,b\,d = a\,c\,d\,b\,d = a\,c\,b$. Thus, $c\,b \in N(a) \cap L$. This is a contradiction. Hence, $Z(G) \not\leq H$ and $G = H\,Z(G)$. ∎

Thus, we get the following

Theorem 3.8. *Let G be any group of order less than 64, and different from 48. If a subgroup H of G satisfies (S), then $G = HZ(G)$.*

For $|G| = 48$, we require to discuss only the case when $|H| = 24$. However, there are large number of possibilities for this case. This case is left untackled for the time being.

There exist large number of pairs (G, H), where H satisfies (S), but $G \neq HZ(G)$. Such pairs of *2-groups* have been found by using *GAP-computer* package [6]. Here we describe a pair (G, H) with $|G| = 64$, $|H| = 32$, $Z(G) = Z(H)$; so that $G \neq HZ(G)$. We could discover three different groups G, of order 64, numbered as 257, 258, and 259, in the 2-*group* library of the package. In each of them we could find six subgroups H of order 32, satisfying (S) and containing $Z(G)$. One such is the following. This is numbered 257.

Example: $C = \langle a, b, c, d \rangle$ with relations $a^2 = b^2 = c^2 = d^2 = 1$, $ac = ca$, $ad = da$, $bc = cb$, $bd = db$, $[d,c] = [b,a]^2 = [[b,a],\, a]$, $[d,c]c = c[d,c]$, $[d,c]\, d = d[d,c]$, $[d,c]^2 = 1$. Here, $Z(G) = \{I, [d,c]\}$, $|G| = 64$, $H = \langle b, d, [b,a], [d,c], ac \rangle$, $|H| = 32$.

ACKNOWLEDGEMENT – This research was partially supported by the Kuwait University Research Grant No. SMO75. We thank the referee for his suggestions.

REFERENCES

[1] De Meyer, F.R. and Ingraham, E. – *Separable algebras over commutative rings*, Lecture Notes in Mathematics, Vol. 181, Springer-Verlag, 1971.

[2] De Meyer, F.R. and Janusz, G.J. – Group rings which are Azumaya Algebras, *Trans. Amer. Math. Soc.,* 279 (1983), 389–395.

[3] Hirata, K. and Sagano, K. – On semi-simple extensions and separable extensions over noncommutative rings, *J. Math. Soc. Japan,* 18 (1966), 360–373.

[4] Passman, D.S. – *The Algebraic Structure of Group Rings*, John Wiley and Sons, 1977.

[5] Scott, W.R. – *Group Theory*, Prentice-Hall Inc., 1964.

[6] Schonert, M. et al – *GAP, Groups, Algorithm, Programming*, Lehrstuhl D für Mathematik, RWTH Achen, 1992.

[7] Stenström, B. – *Rings of Quotients*, Die Grundlehren der mathematischen Wissenschaften, 2l7, Springer-Verlag, 1975.

[8] Szeto, G. – On separable extensions of group rings and quaternion rings, *Internat. J. Math. & Math. Sci.,* 1 (1978), 433–438.

[9] Szeto, G. and Wong, Y.E. – A general Maschke Theorem, *Nanta Math.,* 12 (1979), 1–4.

Surjeet Singh and L.A.-M. Hanna,
Department of Mathematics, Kuwait University,
P.O. Box 5969, Safat 13060 – KUWAIT