

## CONJUGATES IN PRIME RINGS

BY  
CHARLES LANSKI

**Abstract.** Let  $R$  be a prime ring with identity, center  $Z \neq GF(2)$ , and a nonidentity idempotent. If  $R$  is not finite and if  $x \in R - Z$ , then  $x$  has infinitely many distinct conjugates in  $R$ . If  $R$  has infinitely many  $Z$ -independent elements then  $x \in R - Z$  has infinitely many  $Z$ -independent conjugates.

Herstein [3] has shown that any noncentral element in a division ring has infinitely many distinct conjugates. In this paper we extend his result to prime rings with idempotent. We show that no noncentral normal subgroup can centralize a noncentral element, and then use Herstein's approach and the proof of a theorem of Martindale [5, Theorem 2] to obtain the result. We also obtain results on the independence of these conjugates over the center.

1. All rings are assumed to be associative.  $R$  will generally denote a prime ring with center  $Z$  and group of units  $U$ . If  $G$  is a normal subgroup of  $U$  we will write  $G \triangleleft U$ . We will always assume that  $R$  contains an identity element 1, that  $Z \neq GF(2)$ , and that  $R$  contains a nonidentity idempotent. When we denote an idempotent by a symbol other than 1, we shall assume that that idempotent is not 1. If  $e$  is an idempotent  $e'$  will denote the idempotent  $1 - e$ . If  $S$  is any ring with  $a, b \in S$ , we denote  $ab - ba$  by  $[a, b]$ . Thus if  $K$  is a subset of  $S$ ,  $a \in K$ , and  $[a, K] = 0$ , then  $K$  centralizes  $a$ .

We will need some conditions on elements to enable us to conclude that they are in the center of  $R$ . We begin with

**LEMMA 1.** *Let  $R$  be prime and  $U \neq 0$  be an ideal of  $R$ . If  $a \in R$  and  $[a, U] = 0$  then  $a \in Z$ .*

**Proof.** Let  $r \in R, u \in U$ .  $a(ru) = (ru)a = r(ua) = (ra)u$ . Hence  $[a, r]u = 0$  for all  $u \in U$ . Thus  $[a, R]U = 0$  which forces  $[a, R] = 0$  as  $R$  is prime.

**LEMMA 2.** *Let  $R$  be prime and let  $E$  be the subring generated by all the idempotents of  $R$ . Then  $E$  contains a nonzero ideal of  $R$ .*

**Proof.** It is well known and easily shown that  $E$  is a Lie ideal of  $R$ . If  $e$  is an idempotent then  $[e, E] \neq 0$ , for otherwise, since  $e + exe'$  is an idempotent for all  $x$  in  $R$ , we would have  $[e, exe'] = 0$ . This would imply that  $eRe' = 0$ , which is

---

Received by the editors March 31, 1970.

AMS 1969 subject classifications. Primary 16S3; Secondary 1660.

Key words and phrases. Prime ring, conjugates, independence.

Copyright © 1971, American Mathematical Society

impossible in a prime ring. Since  $E$  is not commutative it contains a nonzero ideal of  $R$  [4, Lemma 1.3].  $\square$

Combining Lemma 1 and Lemma 2 we obtain

**LEMMA 3.** *If  $R$  is prime and if  $a \in R$  commutes with every idempotent of  $R$ , then  $a \in Z$ .*

We recall that, for  $R$  prime,  $Z$  is a commutative integral domain whose nonzero elements are not zero divisors in  $R$ . Our assumption that  $Z \neq GF(2)$  allows us to conclude that there is some  $z \in Z$  with  $z^2 - z \neq 0$ , and so  $z^2 - z$  is not a zero divisor in  $R$ . Suppose we have two functions  $f$  and  $g$  from  $R$  to itself satisfying:

- (i)  $f(zr) = zf(r)$ ,
- (ii)  $g(zr) = z^2g(r)$ ,
- (iii)  $f(r) + g(r) = 0$ .

Since  $f(zr) + g(zr) = zf(r) + z^2g(r) = 0$  and  $z(f(r) + g(r)) = 0$ , we obtain  $(z^2 - z)g(r) = 0$ . Hence  $g(r) = 0$  and also  $f(r) = 0$ . We will make use of this eliminating procedure and also a well-known result of Levitzki which we state as

**LEMMA 4.** *Assume  $S$  has no nonzero nilpotent ideals. If for  $a \in S$  the left (right) ideal  $Sa$  ( $aS$ ) satisfies  $(sa)^k = 0$  ( $(as)^k = 0$ ) for some fixed integer  $k$  and all  $s$  in  $S$ , then  $a = 0$ .*

**Proof.** [4, p. 1].  $\square$

**LEMMA 5.** *Let  $R$  be prime and suppose  $G \triangleleft U$  with  $ege' = 0$  for some idempotent  $e$  and all  $g \in G$ . Then  $[e, G] = 0$ ,  $[eRe', g] = 0$ , and  $[e'Re, g] = 0$  for all  $g \in G$ .*

**Proof.** Choose  $x \in R$  with  $exe' \neq 0$ . This is possible since  $R$  is prime. The  $1 + exe' \in U$  and so for  $g \in G$  we have  $h = (1 + exe')g(1 - exe') \in G$ . Since  $ehe' = 0$  we obtain  $exe'ge' - egexe' - exe'ge' = 0$ . This relation clearly holds for all  $x \in R$ . Using the elimination procedure described above we get  $exe'ge' = 0$ . Thus  $(xe'ge)^3 = 0$  for all  $x$  in  $R$ . By Lemma 4,  $e'ge = 0$ . Since  $ege' = 0$  we have  $[e, G] = 0$ . As  $exe'ge' = 0$ , we also have  $exe'ge' = egexe'$ . But  $g = ege + e'ge'$  and so  $[eRe', g] = 0$ . Starting our argument with  $e'xe$  and using  $e'ge = 0$  would yield  $[e'Re, g] = 0$  in a similar manner.  $\square$

**THEOREM 6.** *If  $R$  is prime and  $G \triangleleft U$  with  $eGe' = 0$  for some idempotent  $e$ , then  $G \subset Z$ .*

**Proof.** By Lemma 5,  $[e, G] = 0$ . Let  $F$  be the ring generated by all idempotents  $f$  with  $[f, G] = 0$ . Since, by Lemma 5,  $[g, fRf'] = [g, f'Rf] = 0$  for each idempotent  $f \in F$ , it follows that  $[g, f + fxf'] = [g, f + f'xf] = 0$  for all  $x \in R$ . Thus  $f + fxf$  and  $f + f'xf$  are in  $F$ .

Now  $[f, x] = (f + fxf') - (f + f'xf)$ , and so  $[f, x] \in F$ . Assume that for idempotents  $f_1, f_2, \dots, f_{k-1} \in F$  we have  $[f_1f_2 \cdots f_{k-1}, x] \in F$  for all  $x \in R$ . But then

$$[f_1f_2 \cdots f_k, x] = f_1f_2 \cdots f_{k-1}[f_k, x] + [f_1f_2 \cdots f_{k-1}, x]f_k$$

is in  $F$ . Hence  $F$  is a Lie ideal of  $R$ , and as in Lemma 2 we can conclude that  $F$  contains a nonzero ideal of  $R$ . By Lemma 1 we must have  $G \subset Z$ .  $\square$

**THEOREM 7.** *Let  $R$  be prime and  $w \in R$ . If  $[w, G] = 0$  for  $G \triangleleft U$ , then either  $w \in Z$  or  $G \subset Z$ .*

**Proof.** Let  $a \in eRe'$  for  $e$  an idempotent of  $R$ . Then  $(1-a)g(1+a) \in G$ , and so  $(1-a)g(1+a)w = w(1-a)g(1+a)$ . Hence  $gw - agw + gaw - agaw = wg - wag + wga - waga$ . But  $gw = wg$  which implies

$$gaw + wag - agw - wga = agaw - waga.$$

Clearly, if  $a = exe'$  then we could repeat the argument with  $az = ezxe'$ . So in this situation we can use our element  $z \in Z$  with  $z^2 \neq z$ , as in Lemma 5, to obtain

$$(i) \quad agaw = waga,$$

$$(ii) \quad gaw + wag - agw - wga = 0.$$

Multiply (i) on the left by  $b \in eRe'$  to get

$$(iii) \quad bwaga = 0.$$

Let  $b, c \in eRe'$  and consider  $c(ii)b = 0$ . This implies that  $cgawb + cwagb = 0$ . Multiply this expression on the right by  $gb$  to obtain  $cgawbgb + cwagbgb = 0$ . By (iii)  $awbgb = 0$  and so  $cwagbgb = 0$ . Since  $c$  and  $a$  are arbitrary, for  $w, g$  and  $b$  fixed this says  $eRe'weR(e'gbgb) = 0$ .

Since  $R$  is prime either  $eRe'we = 0$  or  $e'gbgb = 0$ . If  $eRe'we = 0$  then  $e'we = 0$ . If  $eRe'we \neq 0$ , then  $e'gbgb = 0$  for each  $g \in G$  and  $b \in eRe'$ . But  $e'gbgb = 0$  implies that  $((e'ge)r)^3 = 0$  which gives  $e'ge = 0$  by Lemma 4. But then  $e'Ge = 0$  which implies that  $G \subset Z$  by Theorem 6. We have shown that for any idempotent  $e$  of  $R$ , either  $e'we = 0$  or  $G \subset Z$ . If  $G \not\subset Z$  then  $e'we = 0$  for every idempotent  $e$ , including  $e' = 1 - e$ . Thus  $G \not\subset Z$  implies that  $[w, e] = 0$  and so  $w \in Z$  by Lemma 3.  $\square$

**COROLLARY 8.** *Let  $R$  be prime and  $w \in R$  with  $[w, eRe'] = 0$  for all idempotents  $e$  of  $R$ . Then  $w \in Z$ .*

**Proof.** Let  $e$  be an idempotent of  $R$  and  $u \in U$ . Then  $ueu^{-1}$  is an idempotent of  $R$ . Hence the group  $G$  generated by all  $1 + exe'$  for all idempotents  $e$  of  $R$  is normal in  $U$  and not in  $Z$ . Clearly  $[w, G] = 0$  and the result follows from Theorem 7.  $\square$

**COROLLARY 9.** *Let  $R$  be prime and  $w \in R$  with  $[w, a] = 0$  for all  $a \in R$  with  $a^2 = 0$ . Then  $w \in Z$ .*

**THEOREM 10.** *Let  $R$  be prime with  $x \in R - Z$ . Then  $x$  has infinitely many distinct conjugates in  $R$  unless  $R$  is finite.*

**Proof.** We begin as Herstein does in [3]. Suppose that  $x$  has only finitely many conjugates  $x^{a_1}, x^{a_2}, \dots, x^{a_n}$ . Let  $C$  be the subgroup of units of  $R$  which centralizes  $x$ . Then the index of  $C$  in  $U$  is finite,  $C$  has only finitely many conjugates in  $U$ , and each conjugate is of finite index in  $U$ . Hence if  $G$  is the intersection of all the distinct conjugates of  $C$ , then  $G \triangleleft U$ ,  $G$  is of finite index in  $U$ , and  $G$  centralizes  $x$ ,

since  $G \subset C$ . As  $x \notin Z$  we must have  $G \subset Z$  by Theorem 7. Thus  $U \cap Z$  is of finite index in  $U$ . Given any idempotent  $e$  in  $R$ , choose  $s$  with  $ese' \neq 0$ . Then  $1 + ezs e'$  are distinct units in  $U$  for distinct  $z \in Z$ . If two such were in the same coset of  $Z \cap U$ , we would have  $(1 + ez_1 s e')(1 - ez_2 s e') \in Z$ . But this implies that  $(z_1 - z_2)ese' \in Z$ . Since  $ese' \neq 0$  we must have  $z_1 = z_2$ . Thus  $Z$  is finite and so is a field. Further,  $eRe'$  and  $e'Re$  are finite subsets of  $R$ , for  $(1 + ere')(1 - ese') \in Z$  implies that  $e(r - s)e' \in Z$ , which in turn implies that  $ere' = ese'$ .

We can now assume that for any idempotent  $e$  of  $R$ , that  $eRe'$  is a nonzero finite-dimensional algebra over  $Z$ . Here we employ an argument of Martindale [5, Theorem, p. 578]. Since  $R$  is prime there exists an  $s \in R$  with  $eRe'se \neq 0$ . Hence  $eRe's \neq 0$ . If  $v_1, v_2, \dots, v_k$  is a vector space basis of  $eRe'$  over  $Z$ , then clearly  $v_1s, v_2s, \dots, v_k s$  span  $eRe's$  over  $Z$ . Hence  $eRe's$  is a nonzero, finite-dimensional algebra over  $Z$ . By the definition of  $s$  and the fact that  $R$  is prime we have that  $eRe's$  is not nilpotent. Thus  $eRe's$  is unequal to its (nilpotent) radical  $N$ . So  $eRe's/N$  is a nonzero finite-dimensional semisimple algebra over  $Z$ , and so has an identity element. As  $N$  is nilpotent it follows that  $eRe's$  contains an idempotent  $f$ . Hence  $fRf \subset eRe's$  is a nonzero finite-dimensional prime algebra over  $Z$ . Since  $Z$  is finite it follows that  $fRf$  is isomorphic to  $Z_n$ , the complete ring of  $n \times n$  matrices over  $Z$ . Choose a primitive idempotent  $h$  in  $fRf$ . Then  $h(fRf)h = hRh$  is isomorphic to  $Z$ , and so,  $hR$  is a faithful irreducible module for  $R$ . Thus  $R$  can be considered as a dense ring of  $Z$ -linear transformations acting on  $hR$  as a vector space over  $Z$ . As a vector space over  $Z$ ,  $hR$  can be written as  $hR = hRh + hRh'$ . But since  $h$  is an idempotent of  $R$ ,  $hRh'$  is finite dimensional over  $Z$ . Since  $hRh$  is isomorphic to  $Z$  we must have  $hR$  finite dimensional over  $Z$ . Thus  $R$  must be isomorphic to  $Z_n$ , and so  $R$  is finite.

We state two immediate corollaries, in each case assuming that  $R$  is not a finite ring.

**COROLLARY 11.** *If  $R$  is prime then  $U$  is infinite and  $U \cap Z$  is not of finite index in  $U$ .*

**COROLLARY 12.** *Let  $R$  be prime and  $f(x) \neq 0 \in Z[x]$ . Then*

- (i) *if  $f(x)$  has a root in  $R - Z$ , it has infinitely many distinct roots in  $R$ ,*
- (ii) *if  $\deg f(x) = n$  and if  $f(x)$  has  $n + 1$  roots in  $R$  then it has infinitely many.*

2. We turn our attention to the  $Z$ -independence of the set of conjugates of elements of  $R$ . For definiteness we make the following definition:

**DEFINITION.** A subset  $S$  of  $R$  is called  $Z$ -dependent if for some finite subset  $\{x_i\}$  of  $S$  there exist  $z_i \in Z$  not all zero with  $\sum z_i x_i = 0$ . Otherwise  $S$  is called  $Z$ -independent.

**LEMMA 13.** *Let  $R$  be prime,  $e$  an idempotent of  $R$ , and  $w \in R$  with  $e'we \neq 0$ . If  $\{(1 + er_i e')w(1 - er_i e')\}$  for  $r_i \in R$  is a  $Z$ -dependent set, then  $\{er_i e'w - wer_i e' - er_i e'wer_i e'\}$  is  $Z$ -dependent.*

**Proof.** Suppose that for some finite subset we have  $\sum z_j(1 + er_je')w(1 - er_je') = 0$  with not all  $z_j = 0$ . Multiply on the left and right by  $ere'$ . We obtain  $(\sum z_j)ere'were' = 0$ . Since  $e'we \neq 0$ , by Lemma 4 there must exist an  $r \in R$  with  $ere'were' \neq 0$ . Thus  $\sum z_j = 0$ . Expanding  $\sum z_j(1 + er_je')w(1 - er_je') = 0$  gives the result.  $\square$

LEMMA 14. *Let  $R$  be prime. Suppose that for some idempotent  $e$  of  $R$  that  $ewe'Re$  or  $eRe'we$  contains an infinite collection of  $Z$ -independent elements. Then  $w$  has infinitely many  $Z$ -independent conjugates in  $R$ .*

**Proof.** Let  $\{ewe'r_i e\}$  be an infinite  $Z$ -independent set. If for some finite collection of  $r_j$  we have

$$\sum z_j(e'r_j ew - we'r_j e - e'r_j ewe'r_j e) = 0,$$

then left multiplication by  $e$  yields  $\sum z_j ewe'r_j e = 0$  contradicting the  $Z$ -independence of  $\{ewe'r_j e\}$  unless  $z_j = 0$  for all  $j$ . Thus  $\{e'r_i ew - we'r_i e - e'r_i ewe'r_i e\}$  is  $Z$ -independent, and so, by Lemma 13,  $\{(1 + e'r_i e)w(1 - e'r_i e)\}$  is an infinite  $Z$ -independent collection of conjugates of  $w$ . A similar argument gives the result assuming that  $eRe'we$  contains an infinite collection of  $Z$ -independent elements.  $\square$

Before proceeding we require certain facts about  $R \otimes_Z K$  where  $K$  is the field of quotients of  $Z$ . For details see [2, §2 and §4]. Since  $R$  is a torsion free  $Z$  module and  $K$  is a field of quotients of  $Z$  we have the following facts for  $M \subset N$ ,  $Z$  submodules of  $R$ :

1. If  $a \in M \otimes_Z K$  then  $a = m \otimes 1/t$ ,  $m \in M$ ,  $t \in Z$  [2, §2, No. 2, Remark 2].
2. If  $a \in M \otimes_Z K$  and  $a = m \otimes 1/t = 0$ , then  $m = 0$  [2, §2, No. 2, Proposition 4].
3. There exists a unique  $K$  linear transformation of  $M \otimes_Z K$  into  $N \otimes_Z K$  sending  $m \otimes 1/t \mapsto i(m) \otimes 1/t$ , where  $i: M \rightarrow N$  is the injection of  $M$  into  $N$  [2, §2, No. 2, Proposition 5].
4.  $K$  is a flat  $Z$  module [2, §2, No. 4, Theorem 1].

From these facts it follows that

- (i)  $R \otimes_Z K$  is a prime algebra over  $K$  with nonidentity idempotent,
- (ii) if  $\{m_i\}$  is a  $Z$ -independent subset of  $M$  then  $\{m_i \otimes 1\}$  is a  $K$ -independent subset of  $M \otimes_Z K$ ,
- (iii)  $M \otimes_Z K$  is finite dimensional over  $K$  if and only if there is a finite maximal  $Z$ -independent subset of  $M$ , and
- (iv) the injection of  $M \otimes_Z K$  into  $R \otimes_Z K$  is  $K$  linear and the dimension of  $M \otimes_Z K$  over  $K$  is the same as the dimension over  $K$  of its injection into  $R \otimes_Z K$ .

We note that (ii) and (iii) imply that  $M \otimes_Z K$  is finite dimensional over  $K$  exactly when  $M$  contains no infinite  $Z$ -independent subsets. Henceforth we denote  $M \otimes_Z K$  by  $M_K$ .

THEOREM 15. *Let  $R$  be prime and let  $\dim_K R_K$  be infinite. If  $w \in R - Z$  then  $w$  has infinitely many  $Z$ -independent conjugates in  $R$ .*

**Proof.** By Lemma 14 we are done unless  $eRe'we$  and  $ewe'Re$  fail to contain an infinite collection of  $Z$ -independent elements for every idempotent  $e \in R$ . Thus we

may assume that  $(eRe'we)_K$  and  $(ewe'Re)_K$  are finite-dimensional vector spaces over  $K$  and are not zero unless  $e'we=0$  or  $ewe'=0$  respectively. But then, as  $w \notin Z$ , by Lemma 3 there is an idempotent  $e$  with  $(eRe'we)_K$  a nonzero finite-dimensional subalgebra of  $R_K$  over  $K$ . Further, since  $R$  is prime,  $(eRe'we)_K$  is not nilpotent. As in Theorem 10 we conclude that there is an idempotent  $f \in (eRe'we)_K$  and so  $fR_Kf \subset (eRe'we)_K$  is a finite-dimensional prime algebra over  $K$ . Thus  $fR_Kf$  is isomorphic to the complete ring of  $n \times n$  matrices over  $D$ , a finite-dimensional division algebra over  $K$ . Again as in Theorem 10, taking a primitive idempotent  $h$  in  $fR_Kf$  and considering  $h(fR_Kf)h = hR_Kh$  yields the fact that  $R_K$  is a primitive ring acting on a faithful irreducible module  $M$  which is a vector space over a division algebra  $D$  finite dimensional over  $K$ . Now if  $M$  is finite dimensional over  $D$ , then  $R_K$  is finite dimensional over  $K$ , contradicting our hypothesis. Thus  $M$  must be infinite dimensional over  $D$ . In what follows we will usually identify  $R$  with its image in  $R_K (r \rightarrow r \otimes 1)$  [2, §2, No. 2, Remark 4].

Since  $R_K$  is dense on  $M$ , if  $e$  is an idempotent of  $R$ , then  $eR_Ke = (eRe)_K$  is dense on  $Me$  into itself. If  $ewe'Re$  is not zero then for some  $m \in M$  we have  $m(ewe'Re)_K \neq 0$  and  $m(ewe'Re)_K = m(ewe'R_Ke) = (mewe')R_Ke = Me$ . If  $Me$  is an infinite-dimensional subspace of  $M$  then  $(ewe'Re)_K$  cannot be a finite-dimensional subspace of  $R_K$ ; we must have  $ewe'Re=0$ , and so  $ewe'=0$ . Thus if for an idempotent  $e$  of  $R$  we have  $ewe' \neq 0$  then  $Me$  must be a finite-dimensional subspace of  $M$ . Since  $M = Me + Me'$ ,  $Me'$  is infinite dimensional and so  $e'we=0$ .

Since  $w \notin Z$  there is an idempotent  $e$  with  $ewe' \neq 0$ , and so  $Me'$  is an infinite-dimensional subspace of  $M$ . Let  $x = (1 + e're)w(1 - e're) = w + e'rew - we're - e'rewe're$ . If  $e'xe \neq 0$ , then as we have seen above  $(e'xeRe')_K$  must be infinite dimensional. But then by Lemma 14,  $x$ , and so  $w$ , has an infinite collection of  $Z$ -independent conjugates. Hence we may assume that  $e'xe=0$  for every  $r \in R$ . Thus  $0 = e'xe = e'we + e'rewe - e'were' - e'rewe're$ . Since  $e'we=0$  we have  $e'rewe - e'were' - e'rewe're = 0$  for all  $r \in R$ .

We now employ our element  $z \in Z$  with  $z^2 \neq z$  as in Lemma 5 to obtain  $e'rewe're = 0$  for all  $r \in R$ . As we have seen before, by Lemma 4 we can conclude that  $ewe' = 0$  which contradicts our assumption that  $ewe' \neq 0$ . Since our original assumption that  $(ewe'Re)_K$  and  $(eRe'we)_K$  are finite dimensional over  $K$  forces us to conclude that  $ewe' = 0$ , for all  $e$ , and so, that  $w \in Z$ , it must be that for some idempotent  $e$ , either  $(ewe'Re)_K$  or  $(eRe'we)_K$  is infinite dimensional over  $K$ . Our result follows from Lemma 14.  $\square$

If we examine the proof of Theorem 15 we see that the existence of infinitely many distinct conjugates of  $w \in R - Z$  guaranteed by Theorem 10 is not used. Thus for  $\dim_K R_K$  infinite, Theorem 15 gives at once the existence and independence of an infinite set of conjugates for  $w \in R - Z$ .

If  $R$  happens to be a simple ring we can say more about the number of independent conjugates of noncentral elements. The case we consider will be an easy consequence of a theorem of Amitsur [1] and provides a proof of existence

and independence at one time as in Theorem 15. Let us denote by  $[R, R]$ , the additive subgroup of  $R$  generated by all  $[a, b]$  for  $a, b \in R$ . If  $R$  is simple then the ring generated by  $[R, R]$  is  $R$  itself, since  $R$  is not commutative (we still are assuming  $R$  contains a nonidentity idempotent) [4, p. 9]. Hence  $\dim_Z [R, R] = \dim_Z R$  if  $\dim_Z R = j$  is infinite.

**THEOREM 16** (AMITSUR [1]). *Let  $R$  be simple and let  $W$  be a subspace of  $R$  invariant with respect to conjugation by the group of units of  $R$ . Then  $W \subseteq Z$  or  $W \supseteq [R, R]$ .*

**THEOREM 17.** *Let  $R$  be simple with  $\dim_Z R = j$ , infinite. If  $w \in R - Z$  then  $w$  has  $j$   $Z$ -independent conjugates in  $R$ .*

**Proof.** Let  $W$  be the subspace of  $R$  generated by the conjugates of  $w$ . Since  $W$  is invariant with respect to conjugation by the units of  $R$ ,  $W \subseteq Z$  or  $W \supseteq [R, R]$  by Theorem 16. But  $w \notin Z$  so  $W \supseteq [R, R]$ . Hence  $\dim_Z W$  must be  $j$ . Since the conjugates of  $w$  span  $W$  there must be  $j$  independent such conjugates.  $\square$

3. In this section we discuss some examples relevant to possible extensions of our results. To begin with, it is easy to see that Theorem 10 is false for semiprime rings with idempotents. If  $S$  is any prime ring for which Theorem 10 holds, then consider  $R = S \otimes A$ , where  $A$  is any finite matrix ring.  $R$  is semiprime, the identity of  $A$  is an idempotent in  $R$ , but any element of  $A$  has only a finite number of conjugates in  $R$ .

Extensions of our results to domains fail in general, as is seen by considering the free algebra generated by more than one indeterminant over any domain. If the domain is a division ring, then the units will not be central but will commute with all the indeterminants. If one desires an example in which the group of units is "arbitrarily large" and does not commute with all nonunits, one can begin with  $K = F[[Y]]$  the formal power series over any field in some well ordered set  $\{y_i\}$  of indeterminants. Now let  $\sigma$  be the monomorphism of  $K$  sending  $y_i$  into  $y_{i+1}$  and consider the algebra  $K\{X, S, \sigma\}$  defined like the free algebra in a set of indeterminants  $X$  over  $K$  except that for a proper nonempty subset  $S$  of  $X$  we have  $xk = (k)\sigma x$  for  $x \in S$  and  $k \in K$ .

If we consider prime rings with zero divisors but without idempotents then our results also fail. As an example consider the algebra  $K\{X, S, \sigma\}$  above where  $X = \{x, y\}$ ,  $S = \{y\}$  and set  $R = K\{X, S, \sigma\}/(x^2)$ . Then in  $R$ ,  $x^2 = 0$ , so  $R$  is not a domain. One can show that if  $a, b \in R$  then  $ayb = 0$  implies that  $a = 0$  or  $b = 0$ , and so,  $R$  is a prime ring. Representing a typical element of  $R$  as  $k + ax + by$  one can show, using the fact that  $y$  is not a zero divisor in  $R$  and by examining degrees, that any unit of  $R$  is of the form  $v + xax$  for  $a \in R$  and  $v$  a unit in  $K$ . Thus  $x$  has no conjugate except itself, while  $y$  has infinitely many  $F$  independent conjugates of the form

$$(1 + xy^k x)y(1 - xy^k x) = y + xy^k xy - yxy^k x - xy^k xyxy^k x.$$

Also note in this example that  $F$  is the center of  $R$  and there are arbitrarily large numbers of independent units over  $F$  for suitable choices of  $K$ , so  $\dim_F R$  can be arbitrarily large.

Lastly we show that for prime rings with idempotents it is not necessarily true that the number of independent conjugates of a noncentral element is maximal. Let  $F$  be any field and consider the ring  $R$  of all countable by countable matrices over  $F$  such that each row and each column contains at most a finite number of nonzero elements of  $F$ . We can consider  $R$  as a ring of linear transformations on a countable-dimensional vector space  $V$  over  $F$ . Clearly,  $V$  is a faithful, irreducible  $R$ -module, and so  $R$  is a primitive ring. We note that the dimension over  $F$  of all possible first columns for elements of  $R$  is countable, but that  $\dim_F R$  is not countable. Let  $e \in R$  be the idempotent with the identity of  $F$  in the first row and first column and zeros elsewhere. Then if  $ueu^{-1}$  is a conjugate of  $e$ ,  $ueu^{-1}$  is a matrix with only a finite number of nonzero columns and each is a multiple of the first column of  $U$ . Hence the number of independent such conjugates is countable.

#### REFERENCES

1. S. A. Amitsur, *Invariant submodules of simple rings*, Proc. Amer. Math. Soc. **7** (1956), 987–989. MR **18**, 557.
2. N. Bourbaki, *Algèbre commutative, Chapter 2: Localisation*, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961. MR **36** #146.
3. I. N. Herstein, *Conjugates in division rings*, Proc. Amer. Math. Soc. **7** (1956), 1021–1022. MR **18**, 557.
4. ———, *Topics in ring theory*, Univ. of Chicago Press, Chicago, Ill., 1969.
5. W. S. Martindale, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576–584. MR **39** #257.

UNIVERSITY OF SOUTHERN CALIFORNIA,  
LOS ANGELES, CALIFORNIA 90007