

# ON THE COMMUTATOR SUBGROUP OF THE GENERAL LINEAR GROUP

O. LITOFF

**1. Introduction.** The theory of the general linear group has been developed most extensively for the case in which the matrix elements are elements of a field or division ring (e.g. [3; 4]). A few other cases have also been considered, particularly those in which the matrix elements are integers [5] or integers mod  $p^r$ ,  $p$  a prime [1] and [2]. In each of these cases mentioned above it is possible to characterize the commutator subgroup (with an exception for the two-dimensional case) in two other ways:

(i) It is generated by the set of transvections of the group (matrices which correspond to the addition of multiples of one row or column to another).

(ii) It consists of the set of all matrices of the group with determinant one (except for the case of noncommutative division rings).

It seems natural to ask whether these results can be extended to cases in which the matrix elements are allowed to lie in other rings, and, if so, to what extent the results depend upon the ring structure.

In this paper the extension is made for two classes of rings, viz., Euclidean rings and rings with the property that the set of nonunits forms an ideal. The result for the former class subsumes the theorem of Hua and Reiner [5] that the commutator subgroup is characterized by (ii) when the matrix elements are integers. (Their proof differs from the one here.) The latter class of rings includes division rings and rings of integers mod  $p^r$  as special cases, as well as valuation rings and local rings.

**2. Definitions and notation.** The general linear group  $GL_n(R)$  is defined as the multiplicative group of  $n \times n$  invertible matrices with elements in an associative ring  $R$  containing an identity element. Adopting the terminology of Dieudonné [4], we define a transvection  $T_{ij}(\lambda)$  to be the matrix differing from the identity only in the  $ij$ th place where  $\lambda$  stands instead of 0. We note that  $T_{ij}^{-1}(\lambda) = T_{ij}(-\lambda)$  and that left (right) multiplication of any matrix by a transvection has the effect of adding a multiple of one row (column) to another. A combination of transvections which will prove useful is the matrix  $P_{ij} = T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ .  $P_{ij}A$  is the matrix formed by replacing

Presented to the Society, June 21, 1952 under the title *On the equality of three subgroups of the general linear group*; received by the editors July 21, 1954.

the  $i$ th row by the  $j$ th row and the  $j$ th row by the negative of the  $i$ th row.  $AP_{ij}$  is the matrix formed by replacing the  $j$ th column by the  $i$ th column and the  $i$ th column by the negative of the  $j$ th column.

The group generated by the transvections of  $GL_n(R)$  will be denoted by  $\mathcal{T}_n(R)$ , the commutator subgroup by  $\mathcal{C}_n(R)$ , and the unimodular group of elements of determinant one by  $\mathcal{U}_n(R)$ . When no ambiguity can arise the notation for the general linear group and these three subgroups will be simplified to  $\mathcal{G}$ ,  $\mathcal{T}$ ,  $\mathcal{C}$ , and  $\mathcal{U}$ . Since in general the determinant of a matrix with elements in a noncommutative ring is not defined, we shall always assume the commutativity of  $R$  whenever referring to  $\mathcal{U}_n(R)$ .<sup>1</sup>

3. We first direct our attention to those inclusion relations which hold for all rings  $R$ .

**THEOREM 1.** *For any commutative ring  $R$ ,  $\mathcal{T} \subset \mathcal{U}$  and  $\mathcal{C} \subset \mathcal{U}$ .*

The proof is immediate.

**THEOREM 2.** *For any ring  $R$ ,  $\mathcal{T} \subset \mathcal{C}$  except when  $n=2$  and 2 is not invertible.*

**PROOF.** *Case 1.  $n \geq 3$ .  $T_{ij}(\lambda) = T_{ik}(\lambda)T_{kj}(1)T_{ik}^{-1}(\lambda)T_{kj}^{-1}(1)$  for  $i, j, k$  all distinct. This computation was exhibited by Iwasawa [6] for  $R$  a field. The special case when  $\lambda=1$  was used earlier by Brenner [1].*

*Case 2.  $n=2$ , 2 invertible in  $R$ .*

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda/2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -\lambda/2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

A similar relation holds for

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}.$$

In particular, if  $R$  is a valuation ring, Theorem 2 may be slightly sharpened as follows:

**THEOREM 3.** *If  $R$  is a valuation ring, then  $\mathcal{T} \subset \mathcal{C}$  except when  $n=2$  and  $R$  modulo its radical is the field of two elements.*

**PROOF.** If  $R$  is a valuation ring such that the quotient ring is not the field of two elements, then there must exist a unit  $\lambda$  in  $R$  such that

<sup>1</sup> Dieudonné in [4] extended the definition of determinant to the case in which  $R$  is a noncommutative division ring, but with this definition the proof of Theorem 9 fails to go through. (If the determinant of  $D(\mu)$  is 1, one can conclude only that  $\mu$  is a commutator in  $R$ .) Dieudonné himself did not consider the subgroup  $\mathcal{U}$ .

$\lambda - 1$  is also a unit. If  $\mu$  is any arbitrary element of  $R$ , then

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & (\lambda - 1)^{-1}\mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & (\lambda - 1)^{-1}\mu \\ 0 & 1 \end{pmatrix}^{-1}.$$

A similar relation holds for

$$\begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

Thus for any ring  $R$ ,  $\mathfrak{G} \subset \mathcal{C} \subset \mathcal{U}$  (with the exception noted when  $n = 2$ ).

4. A crucial step in Dieudonné's proof [4] that  $\mathfrak{G} \supset \mathcal{C}$  when  $R$  is a division ring is the fact that any element  $A$  of  $\mathcal{G}$  can be written

$$(1) \quad A = TD(\mu)$$

where  $D(\mu) = (d_{ij})$  is a diagonal matrix such that  $d_{ii} = 1$  for  $i \neq n$ ,  $d_{nn} = \mu$ , a unit of  $R$ . Indeed Dieudonné's proof goes through for any ring  $R$  which has decomposition (1). We show below that  $\mathcal{G}$  has this property if  $R$  is Euclidean or if the set of nonunits of  $R$  forms an ideal.

**THEOREM 4.** *If the set of nonunits of  $R$  forms an ideal, then  $A = TD(\mu)$ .*

**PROOF.** The condition that the set of nonunits of  $R$  forms an ideal insures the existence of at least one unit in every row and column of any matrix  $A$  in  $\mathcal{G}$  (otherwise the product of  $A$  by its inverse would have a row or column without units). The only necessary modification in the proof of Dieudonné is the substitution of the word "unit" for the word "nonzero." The plan of the proof is to multiply  $A$  on the left by suitable elements of  $\mathfrak{G}$  until the product is of the form  $D(\mu)$ . Let  $A = (a_{ij})$ . Since  $A$  is nonsingular, at least one element of the first column is a unit. We may as well assume  $a_{21}$  is a unit (otherwise multiply by  $P_{2i} \in \mathfrak{G}$ ). If now we add to the first row  $(1 - a_{11})a_{21}^{-1}$  times the second row (multiplying on the left by  $T_{12}[(1 - a_{11})a_{21}^{-1}]$ ) we get a matrix  $B = (b_{ij})$  such that  $b_{11} = 1$ . Now by adding to each row a suitable multiple of the first row we eventually obtain a matrix  $C = (c_{ij})$  where  $c_{11} = 1$  and  $c_{i1} = 0$ ,  $i \neq 1$ . Now consider the second column of  $C$ . There must exist a unit  $c_{i2}$  for  $i \neq 1$ . Repeat the process. Eventually a matrix of the form  $D(\mu)$  is reached.

**THEOREM 5.** *If  $R$  is Euclidean, then  $A = TD(\mu)$ .*

**PROOF.** Since  $A$  is invertible, there must exist a nonzero element in

the first column. If there actually exists a unit, then we may proceed as in Theorem 4. This will be the case if any one element is a right divisor of all the others. However, if there is no unit in the first column, then the greatest common right divisor of the nonzero elements is a unit (it is a right divisor of the product of the first row of  $A^{-1}$  by the first column of  $A$ ), and, if  $A$  is multiplied on the left by suitable transvections, a new matrix can be obtained which has this unit in its first column. Suppose that  $a_{21} \neq 0$  and not a unit. There must be another nonzero element in the first column, so we may assume  $a_{11} \neq 0$ . We show first that  $A$  can be multiplied on the left by a finite product of transvections to obtain a matrix  $A'$  where either  $a'_{11}$  or  $a'_{21}$  is the greatest common right divisor of  $a_{11}$  and  $a_{21}$  and  $a'_{11} = a_{11}$  for  $t > 2$ . Suppose  $|a_{21}| \leq |a_{11}|$ . (If not, multiply by  $P_{12}$ .) By the Euclidean algorithm we may subtract from the first row of  $A$  a suitable left multiple of the second row to obtain a matrix  $B$  where  $|b_{11}| < |b_{21}|$  ( $b_{21} = a_{21}$ ). If  $b_{11}$  is not the g.c.r.d. of  $a_{11}$  and  $a_{21}$ , then continue by subtracting a suitable left multiple of the first row from the second, obtaining a matrix  $C$  where  $|c_{21}| < |c_{11}|$ . Continuing in this way, we obtain after a finite number of steps the matrix  $A'$ . Suppose  $a'_{21}$  is the g.c.r.d. of  $a_{11}$  and  $a_{21}$ . If there were any other nonzero elements in the first column of  $A$ , say  $a_{31} \neq 0$ , then again by successive applications of the Euclidean algorithm we can obtain a matrix  $A''$  where  $a''_{21}$  is the g.c.r.d. of  $a_{11}$ ,  $a_{21}$ , and  $a_{31}$  and  $a''_{11} = a_{11}$  for  $t > 3$ . We continue this process until we reach a matrix which has in its first column the g.c.r.d. of all the nonzero elements in the first column of  $A$ . Since this element is a unit, we may now proceed as in Theorem 4.

For the remainder of this paper we assume  $R$  is any ring with the decomposition (1).

The proofs of Lemma 1 and Theorem 6 below can now be taken from Dieudonné without change. We repeat them here for completeness.

LEMMA 1.  $\mathfrak{G}$  is a normal subgroup of  $\mathcal{G}$ .

PROOF. We need to show that for any transvection  $T_{ij}(\lambda)$ ,  $AT_{ij}(\lambda)A^{-1} \in \mathfrak{G}$  for any  $A \in \mathcal{G}$ . By (1) it is sufficient to show this when  $A = D(\mu)$ . But

$$\begin{aligned}
 D(\mu)T_{ij}(\lambda)D^{-1}(\mu) &= T_{ij}(\lambda) && (i \neq n, j \neq n), \\
 D(\mu)T_{in}(\lambda)D^{-1}(\mu) &= T_{in}(\lambda\mu^{-1}), \\
 D(\mu)T_{nj}(\lambda)D^{-1}(\mu) &= T_{nj}(\mu\lambda).
 \end{aligned}$$

THEOREM 6.  $\mathfrak{G} \supset \mathcal{C}$ .

PROOF. We prove this by showing  $\mathcal{G}/\mathcal{T}$  is abelian. By (1) we need to show that  $D(\lambda)D(\mu) = D(\mu)D(\lambda) \pmod{\mathcal{T}}$ . There is no loss of generality in assuming  $n = 2$ .

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} = \begin{pmatrix} 0 & \mu \\ -\lambda & 0 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ -\lambda & 0 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & \lambda\mu \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \lambda\mu \end{pmatrix} \pmod{\mathcal{T}}.$$

Similarly,

$$\begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \mu\lambda \end{pmatrix} \pmod{\mathcal{T}}.$$

Hence

$$D(\lambda)D(\mu) = D(\lambda\mu) = D(\mu\lambda) = D(\mu)D(\lambda) \pmod{\mathcal{T}}.$$

Combining Theorems 2 and 6, we obtain

THEOREM 7.  $\mathcal{T} = \mathcal{C}$  except when  $n = 2$  and 2 is not invertible.

In the special case when  $R$  is a valuation ring we have

THEOREM 8. For  $R$  a valuation ring,  $\mathcal{T} = \mathcal{C}$  except when  $n = 2$  and  $R$  modulo its radical is the field of two elements.

We now turn our attention to  $\mathcal{U}$ .

THEOREM 9.  $\mathcal{T} = \mathcal{U}$ .

PROOF.  $\mathcal{T} \subset \mathcal{U}$  by Theorem 1. By assumption any  $U \in \mathcal{U}$  is of the form  $TD(\mu)$  where the determinant of  $D(\mu) = 1$ . Therefore  $\mu = 1$  and  $U \in \mathcal{T}$ .

5. We have shown that a sufficient condition for  $\mathcal{C}_n(R)$  to be characterized by (i) and (ii) is that every element  $A$  of  $R$  can be written  $A = TD(\mu)$ . If  $R$  is commutative, then it is easy to see that this condition is also necessary. Suppose the determinant of  $A$  is  $\mu$ . Write  $A = BD(\mu)$ .  $B$  must have determinant 1 and since  $\mathcal{T} = \mathcal{U}$ ,  $B \in \mathcal{T}$ .

### BIBLIOGRAPHY

1. J. Brenner, *The linear homogeneous group*, Ann. of Math. vol. 39 (1938) pp. 472-493.
2. ———, *The linear homogeneous group II*, Ann. of Math. vol. 45 (1944) pp. 100-109.
3. L. E. Dickson, *Linear groups*, Leipzig, Teubner, 1901.
4. J. Dieudonné, *Les déterminants sur un corps non commutatif*, Bull. Soc. Math. France vol. 71 (1943) pp. 27-45.
5. L. K. Hua and I. Reiner, *Automorphisms of the unimodular group*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331-348.

6. K. Iwasawa, *Über die Einfachheit der speziellen projectiven Gruppen*, Proc. Imp. Acad. Tokyo vol. 17 (1941) pp. 57-59.

7. F. A. Lewis, *The linear congruence group modulo  $n$* , Proc. Amer. Math. Soc. vol. 3 (1952) pp. 367-368.

8. B. L. van der Waerden, *Gruppen von linearen Transformationen*, Berlin, Springer, 1935.

9. S. Wang, *On the commutator group of a simple algebra*, Amer. J. Math. vol. 72 (1950) pp. 323-334.

UNIVERSITY OF CONNECTICUT

---

## A NOTE ON INVARIANT SUBRINGS

GERTRUDE EHRLICH

The problem of invariant subrings has been studied in detail for certain types of rings satisfying the descending chain condition on one-sided ideals.

We prove here two theorems concerning invariant subrings of a ring  $R$  without assuming the descending chain condition.

**THEOREM 1.** *Let  $R$  be a ring with identity 1. If  $S$  is a subring of  $R$  with identity 1, and  $S$  has a representation as the complete matrix ring of order  $n \geq 2$  over a ring with identity, then  $S$  cannot be a proper invariant subring of  $R$ .*

**PROOF.** Let  $E = \{e_{ij}\}$  be a set of  $n^2$  matrix units contained in  $S$ , and let  $B$  be the centralizer of  $E$  relative to  $S$ . Then  $S = B_n$ . Let  $A$  be the centralizer of  $E$  relative to  $R$ . Then  $R = A_n$ , and  $B \leq A$ . If  $t$  is an arbitrary element of  $A$ , we obtain (following Hattori [1]) that  $e_{ii}(1 + e_{ij}t)e_{ji}(1 - e_{ij}t)e_{ii} = te_{ii}$  belongs to  $S$  for arbitrary  $i \neq j$ . Hence  $t = \sum_{i=1}^n te_{ii}$  belongs to  $S$ , and  $A \leq S$ . But then  $A = B$ , and  $S = R$ .

**THEOREM 2.** *Let  $R$  be a ring with identity 1, and not of characteristic 2. Assume that  $R$  has a representation as the complete matrix ring of order  $n \geq 2$  over a ring with identity. Let  $S$  be an invariant sub-field of  $R$ , with identity 1. Then  $S$  is a subfield of the center of  $R$ .*

**PROOF.** Let  $E = \{e_{ij}\}$  be a set of  $n^2$  matrix units contained in  $R$ , and let  $A$  be the centralizer of  $E$  relative to  $R$ , so that  $R = A_n$ . We note first that for every noncentral element  $x$  contained in  $R$ , there exists a square-nilpotent element  $p \neq 0$  ( $p^2 = 0$ ) such that  $xp \neq px$ . (For, if  $x$  commutes with every square-nilpotent element, then  $x$  commutes in