Integral Similarity and Commutators of Integral Matrices

Thomas J. Laffey and Robert Reams
(University College Dublin, Ireland)

Abstract

Let F be a field, $M_n(F)$ the algebra of $n \times n$ matrices over F and $A \in M_n(F)$ with $\text{trace}(A) = 0$. The following facts are well-known

(i) if A is not a scalar, then A is similar over F to a matrix with zero diagonal

(ii) $A = [P, Q] = PQ - QP$ for some P, $Q \in M_n(F)$.

In this paper we consider the situation when F is replaced by the ring of integers $\mathbf{Z}$. We show that (ii) holds in this case for every $n \geq 1$. This result has been proved for $n = 2$ by Lissner and Vaserstein (independently). We show also that (i) holds if F is replaced by $\mathbf{Z}$ for $n > 2$ provided $A \not\equiv aI \bmod p$ for all integers a and primes p.

1. Introduction

Let $\mathbf{Z}$ denote the ring of integers and $M_n(\mathbf{Z})$ the ring of $n \times n$ matrices with entries in $\mathbf{Z}$ and $GL(n, \mathbf{Z})$ the subset of those elements B in $M_n(\mathbf{Z})$ with $\det B = \pm 1$. Two elements A_1, $A_2 \in M_n(\mathbf{Z})$ are *integrally similar* if there exists $T \in GL(n, \mathbf{Z})$ with $T^{-1}A_1T = A_2$. Of course if A_1, A_2 are integrally similar, then they are similar as matrices over the rational field $\mathbf{Q}$ but the converse is not true in general. An excellent account of the relationship between integral similarity and other classical number theory concepts can be found in that appendix by Olga Taussky in Cohn's book [3]. A proof that given two k-tuples $(A_1, \ldots, A_k)$, $(B_1, \ldots, B_k)$ of elements A_i, $B_i \in M_n(\mathbf{Z})$, there is an effective procedure to determine whether there exists an element $X \in GL(n, \mathbf{Z})$ with $X^{-1}A_iX = B_i$

$(i = 1, 2, \ldots, k)$ has been achieved by Grunewald [5]. See also Grunewald and Segal [6] for extensions to other arithmetic groups. The case $k = 1$ includes the result (in group-theoretical terms) that the conjugacy problem is solvable in $GL(n, \mathbf{Z})$. (We are grateful to Mike Boyle for these two references.)

In this paper we consider the extension to matrices in $M_n(\mathbf{Z})$ of two results which are well-known for matrices over fields. We prove that if $A \in M_n(\mathbf{Z})$ has trace 0, then $A = PQ - QP$ for some P, $Q \in M_n(\mathbf{Z})$. The corresponding result for the field of complex numbers was proved by Shoda [9] and extended to all fields by Albert and Muckenhoupt [1].

A simple inductive argument shows that if F is a field and A an $n \times n$ matrix over F with $\mathrm{trace}(A) = 0$ and A is non-scalar (the last condition is obviously an immediate consequence of the others if $A \neq 0$ and F has characteristic 0 or relatively prime to n) then A is similar over F to a matrix B with zero diagonal. When F is replaced by the ring of integers $\mathbf{Z}$ and similarity is replaced by integral similarity, the corresponding result clearly fails if $A \equiv aI \bmod p$ for some prime p and integer $a \equiv 0 \bmod p$ and it is easy to show that it fails more generally if $n = 2$. However we prove here that if $n > 2$ and $A \not\equiv aI \bmod p$ for all primes p and integers $a \not\equiv 0 \bmod p$, and $\mathrm{trace}(A) = 0$, then A is integrally similar to a matrix with zero diagonal.

The proofs of the results in this paper are largely self-contained, modulo standard results on similarity of matrices over fields. We obtain a simple criterion which ensures that if A, P are given elements of $M_n(\mathbf{Z})$ with $\mathrm{trace}(A) = 0$, then there exists $Q \in M_n(\mathbf{Z})$ with $A = [P, Q]$. The corresponding observation for matrices over fields, while easier, also appears to be new and simplifies the problem of writing matrices of trace 0 over fields as commutators.

2. Integral similarity to a matrix with zero diagonal.

Let $A \in M_2(\mathbf{Z})$ have trace 0 and determinant $-p$ where $p \equiv 1 \bmod 4$ is prime. If A is integrally similar to a matrix B with zero diagonal, then B is integrally similar to a companion matrix $\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$. But by the Latimer-MacDuffee theorem ([7], [10]), there are h_p integral similarity classes of such A where h_p is the (ideal) class number of $\mathbf{Q}(\sqrt{-p})$ and by results of Goldfeld and Oesterlé (see [4]), $h_p > \frac{\log p}{55}$. So A is not in general integrally similar to a matrix with zero diagonal. Our first three propositions show that this phenomenon cannot occur for $n > 2$.

Proposition 1. *Let $A \in M_3(\mathbf{Z})$ be non-scalar. Then A is integrally similar to a matrix $B = (b_{ij}) \in M_3(\mathbf{Z})$ such that $b_{12} > 0$ and b_{12} divides all b_{ij} $(i \neq j)$ and $b_{ii} - b_{jj}$ $(1 \leq i, j \leq 3)$.*

Proof. We may write $A = aI + bC$ where a, b are integers, $b \neq 0$, and where if $C = (c_{ij})$, the highest common factor of the numbers $c_{ii} - c_{jj}, c_{ij}$ $1 \leq i \neq j \leq 3$ is 1. Note C is non-scalar and the proposition will follow if we can show that C is integrally similar to a matrix $D = (d_{ij})$ with $d_{12} = 1$. Thus we may assume $a = 0$, $b = 1$ and $C = A$.

Since A is not scalar, A is integrally similar to a non-diagonal matrix and hence to a matrix $B = (b_{ij})$ with $b_{12} > 0$. If all off-diagonal entries of B are even, then some $b_{ii} - b_{jj}$ is odd $(i \neq j)$ by our choice of a, b at the outset. Using the equation

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b_{ii} & b_{ij} \\ b_{ji} & b_{jj} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b_{ii} + b_{ji} & b_{ij} + b_{jj} - b_{ii} - b_{ji} \\ b_{ji} & b_{jj} - b_{ji} \end{pmatrix}$$

we see that B is integrally similar to a matrix with its (i, j) entry odd. Hence A is integrally similar to a matrix $B = (b_{ij})$ with $b_{12} > 0$ and odd.

Among all such matrices B choose one for which the number of distinct primes which divides b_{12} is least possible and subject to this for which b_{12} is least possible. We now aim to show that b_{12} divides all b_{ij} $(i \neq j)$ and all $b_{ii} - b_{jj}$ $(1 \leq i, j \leq 3)$ from which it follows that $b_{12} = 1$. The proof uses repeatedly the fact that if the off-diagonal entries on a row (or column) of an integer matrix X have highest common factor d, then X is integrally similar to a matrix Y in which the corresponding row (or column) has off-diagonal entries $(d, 0, \ldots, 0)$.

We may assume

$$B = \begin{pmatrix} b_{11} & b_{12} & 0 \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$$

and, for the sake of contradiction, that $b_{12} > 1$. Suppose first that $b_{23} \neq 0$. For an integer x, consider the effect of the similarity

$$B \to \begin{bmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} B \begin{bmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = Y, \qquad \text{say.}$$

This replaces the $(1, 2)$, $(1, 3)$ entries of B by y_{12}, y_{13} where $y_{12} = b_{12} + x(b_{22} - b_{11}) - x^2 b_{21}$, $y_{13} = x b_{23}$.

Claim 1. *Every prime divisor of b_{12} divides b_{23}.*

First take x to be the product of all primes dividing b_{23} which do not divide b_{12} (take $x = 1$ if no such primes occur). Then the highest common factor $h = (y_{12}, y_{13})$ involves

only primes occurring in b_{12} and b_{23}. Hence if some prime divisor p of b_{12} does not occur in b_{23}, h has fewer distinct prime divisors than b_{12} and $h > 0$ and odd. But then replacing row 1 of Y by $(y_{11}, h, 0)$ via an integral similarity leads to a contradiction to our choice of b_{12}. So Claim 1 holds.

Claim 2. *Every prime divisor of b_{12} divides $b_{11} - b_{22}$ and b_{21}.*

Let x_0 be the product of all distinct primes occurring in b_{23} which do not occur in b_{12} ($x_0 = 1$ if none arise) and let $x = x_0x_1$, x_1 to be specified. By our choice of b_{12} and the argument above, all primes p which divide b_{12} divide

$$x_0x_1(b_{22} - b_{11}) - x_0^2x_1^2b_{21} = x_0x_1\big((b_{22} - b_{11}) - x_0x_1b_{21}\big)$$

for all integers x_1 relatively prime to b_{12}. So all primes dividing b_{12} divide

$$(b_{22} - b_{11}) - x_0b_{21}$$

and

$$(b_{22} - b_{11}) - 2x_0b_{21}$$

(since b_{12} is odd) and thus b_{21} and $b_{22} - b_{11}$ as claimed.

Next, considering the second column of B we see that b_{12} must equal the highest common factor (b_{12}, b_{32}) and thus b_{12} divides b_{32}. Using an integral similarity, we may assume $b_{32} = 0$.

Using a similarity of the form

$$B \longrightarrow \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} B \begin{bmatrix} 1 & 0 & -y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (*)$$

the $(1,2)$, $(1,3)$ entries of B are replaced by b_{12}, $y(b_{33} - b_{11}) - y^2b_{31}$ and arguing as before, it follows that every prime divisor of b_{12} divides $b_{33} - b_{11}$ and b_{31}. Hence we have shown that every prime divisor of b_{12} divides all b_{ij} $(i \neq j)$ and all $b_{ii} - b_{jj}$ $(1 \leq i, j \leq 3)$ and hence $b_{12} = 1$. This completes the discussion if $b_{23} \neq 0$.

Suppose $b_{23} = 0$. Using the earlier arguments we may assume $b_{32} = 0$ and then considering the effect of a similarity of the form $(*)$, we find b_{12} divides $b_{33} - b_{11}$ and b_{31}.

Observe that

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} B \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & 0 \\ b_{21} & b_{22} & 0 \\ b_{31} + b_{11} - b_{33} & b_{12} & b_{33} \end{bmatrix} = B_1,$$

say, and that

$$\begin{bmatrix} 1 & 0 & 0 \\ z & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} B_1 \begin{bmatrix} 1 & 0 & 0 \\ -z & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{pmatrix} b_{11} - zb_{12} & b_{12} & 0 \\ b_{21} + z(b_{11} - b_{22}) - z^2 b_{12} & b_{22} + zb_{12} & 0 \\ b_{31} + b_{11} - b_{33} - zb_{12} & b_{12} & b_{33} \end{pmatrix}$$

and choosing $z = (b_{31} + b_{11} - b_{33}) \,/\, b_{12}$ (which we know is an integer), it follows that B is integrally similar to a matrix of the form

$$B_0 = \begin{pmatrix} b'_{11} & b_{12} & 0 \\ b'_{21} & b'_{22} & 0 \\ 0 & b_{12} & b_{33} \end{pmatrix}$$

and thus to

$$B_1 = J^{-1} B_0 J = \begin{pmatrix} b_{33} & b_{12} & 0 \\ 0 & b'_{22} & b'_{21} \\ 0 & b_{12} & b'_{11} \end{pmatrix}$$

where

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

If $b'_{21} \neq 0$, the matrix B_1 has its $(2,3)$ entry not zero and thus by the first case analysed, $b_{12} = 1$. Suppose $b'_{21} = 0$. Then a similarity of the form

$$B_0 \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & t & 1 \end{bmatrix} B_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -t & 1 \end{bmatrix}$$

replaces the second column of B_0 by

$$\big(b_{12}, b'_{22}, b_{12} + t(b'_{22} - b_{33})\big)^T$$

and hence, as before, it follows that b_{12} divides $b'_{22} - b_{33}$. By a previous argument, b_{12} divides $b'_{11} - b_{33}$. Hence b_{12} divides all the off-diagonal entries and the differences of the diagonal entries of B_0. Hence $b_{12} = 1$ as desired.

Proposition 2. *Let $A \in M_n(\mathbf{Z})$ $(n \geq 3)$ be non-scalar. Then A is integrally similar to a matrix $B = (b_{ij}) \in M_n(\mathbf{Z})$ where $b_{12} > 0$ and b_{12} divides all entries b_{ij} $(i \neq j)$ and all $b_{ii} - b_{jj}$ $(1 \leq i, j \leq n)$. In addition B may be chosen with $b_{ij} = 0$ for $j \geq i + 2$ $(1 \leq i \leq n - 2)$.*

Proof. As in the proof of Proposition 1, we may assume that the highest common factor of the numbers a_{ij} $(i \neq j)$, $a_{ii} - a_{jj}$ $(1 \leq i, j \leq n)$ is 1. Among all matrices in the integral

similarity class of A choose one, $B = (b_{ij})$, such that b_{12} is positive and odd and subject to this has the smallest possible number of distinct prime divisors and subject to these conditions, b_{12} is least possible. If for some i, j, b_{12} does not divide $b_{ii} - b_{jj}$, then b_{12} does not divide $b_{11} - b_{jj}$ for some j and using a permutation similarity, we may assume b_{12} does not divide $b_{11} - b_{22}$ or $b_{11} - b_{33}$. But now applying the result of Proposition 1 to

$$B_0 = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$$

$\big($noting that any integral similarity $B_0 \longrightarrow X^{-1}B_0X$ may be achieved by $B \longrightarrow (X \oplus I_{n-3})^{-1}B(X \oplus I_{n-3})\big)$ yields a contradiction.

Using the minimality property of b_{12}, it is clear that b_{12} divides all b_{1j} and all b_{i2} $(j \neq 1, i \neq 2)$.

Given any (i, j) with $i \neq 1, 2$, $i \neq j$, using an integral similarity by an elementary matrix we may replace b_{12} by $b_{12} + xb_{1i}$ and then b_{j2} is replaced by $b_{j2} + xb_{ij}$ for some integer x. Then by our choice of b_{12} (and considering the 2nd column) we see that b_{12} divides b_{ij}.

Replacing B by

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & Z^{-1} \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & Z \end{pmatrix}$$

for a suitable $Z \in GL(n-1, \mathbf{Z})$, we may replace the first row $(b_{11}b_{12} \cdots b_{1n})$ of B by $(b_{11}, d, 0, \ldots, 0)$ where $d = b_{12}$ is the highest common factor of $b_{12}, b_{13}, \ldots, b_{1n}$. Conjugating B_1 by a matrix of the form $\begin{pmatrix} I_2 & 0 \\ 0 & Z_1 \end{pmatrix}$ where $Z_1 \in GL(n-2, \mathbf{Z})$, we can replace the second row of B_1 by a row of the form $(c_{21}, c_{22}, c_{23}, 0, \ldots, 0)$ without changing row 1. Proceeding by induction in this way, we see that B may be replaced by a matrix of the form $Y = (y_{ij})$ where $y_{ij} = 0$ for $j \geq i + 2 (i = 1, 2, \ldots, n-2)$, and $y_{12} = b_{12}$. But now note that $B \equiv b_{11}I \bmod b_{12}$; hence $Y \equiv b_{11}I \bmod b_{12}$. Thus Y has the desired form.

We conclude this section with the following result quoted in the Introduction.

Proposition 3. *Let $A \in M_n(\mathbf{Z})$ $(n \geq 3)$ have* trace 0 *and suppose that $A \not\equiv aI \bmod p$ for all integers a and primes p. Then A is integrally similar to a matrix $B \in M_n(\mathbf{Z})$ with zero diagonal.*

Proof Using Proposition 2, we may assume $a_{12} = 1$. The result now follows from the following result.

Lemma 4. *Let $A = (a_{ij}) \in M_n(\mathbf{Z})$ with $a_{12} = 1$. Then A is integrally similar to $B = (b_{ij}) \in M_n(\mathbf{Z})$ where $b_{ii} = 0$ $(i = 1, 2, \ldots, n-1)$.*

Proof. We prove the result by induction on n. If $n = 2$, conjugating A by $\begin{pmatrix} 1 & 0 \\ -a_{11} & 1 \end{pmatrix}$ yields the result. If $n > 2$, conjugating A by a matrix of the form $I + \alpha E_{n1}$ ($\alpha \in \mathbf{Z}$) we may assume $a_{n2} = 1$ and now conjugating A by a matrix of the form $I + \beta E_{21}$ ($\beta \in \mathbf{Z}$) we may further assume that $a_{11} = 0$. Thus we may assume A is of the form

$$\begin{pmatrix} 0 & x \\ y^T & A_1 \end{pmatrix}$$

where $x, y \in \mathbf{Z}^{n-1}$ and $A_1 = (b_{ij}) \in M_{n-1}(\mathbf{Z})$ with $b_{n-1,1} = 1$. Conjugating A_1 by a suitable element of $GL(n-1, \mathbf{Z})$, we may move its $(n-1, 1)$ entry to the $(1, 2)$ position. So by induction, there exists $Q \in GL(n-1, \mathbf{Z})$ with $Q^{-1}A_1Q = B_1 = (b_{ij})$ where $b_{11} = b_{22} = \cdots = b_{n-2,n-2} = 0$. But then

$$B = \big((1) \oplus Q\big)^{-1} A \big((1) \oplus Q\big)$$

has the desired form.

3. A sufficient criterion for a matrix to be a commutator.

Let F be a field and let $P \in M_n(F)$ be nonderogatory. Then since I, P, $P^2, \ldots, P^{n-1}$ are linearly independent, the subspace

$$V = \big\{ A \in M_n(F) \;\big|\; \text{trace}\,(P^i A) = 0 \quad \text{for } i = 0, 1, \ldots, n-1 \big\}$$

has dimension $n^2 - n$. Furthermore the subspace $W = \big\{ [P, Q] \;\big|\; Q \in M_n(F) \big\}$ has dimension $n^2 - n$ since it is the image of the linear map $T : Q \longrightarrow [P, Q] \big(Q \in M_n(F)\big)$ and its kernel, $\ker(T)$, being the centralizer of P, has dimension n. But if $A \in W$, then $\text{trace}(P^i A) = \text{trace}\big(P^i(PQ - QP)\big)$ (for some Q) $= \text{trace}(P^{i+1}Q) - \text{trace}(P^i QP) = 0$, so $A \in V$. Thus $W \subseteq V$ and since $\dim V = \dim W$, we conclude that $V = W$. This proves

Proposition 4. *Let F be a field and $P \in M_n(F)$ be nonderogatory. Let $A \in M_n(F)$. Then $A = [P, Q]$ for some $Q \in M_n(F)$ if and only if* $\text{trace}(P^i A) = 0$ *for* $i = 0, 1, \ldots, n-1$.

Remark. Note that if A in Proposition 4 has rank one, then using a similarity we may assume $A = E_{12}$, the matrix with its $(1, 2)$ entry equal to 1 and all other entries 0. The equation $\text{trace}(P^i A) = 0$ for $i = 0, 1, \ldots, (n-1)$ yields that $p_{21}^{(i)} = 0$ where $P^i = (p_{rs}^{(i)})$ and thus span $\{e_1, Pe_1, P^2e_1, \ldots\} \neq F^n$ where $e_1 = (1, 0, 0, \ldots, 0)^T$, so in particular, the characteristic polynomial of P cannot be irreducible. This gives another proof of Uhlig's

rank one theorem ([11] Lemma 2, p.48) which states that if $P \in M_n(F)$ has an irreducible characteristic polynomial, then rank $[P, Q] \neq 1$ for all $Q \in M_n(F)$.

We now extend this result to matrices over $\mathbf{Z}$. For $A \in M_n(\mathbf{Z})$, $A \bmod p$ denotes A regarded as a matrix in $M_n(\mathbf{Z}_p)$. Also $\big[A, M_n(\mathbf{Z})\big]$ denotes the subgroup $\big\{[A, B] \;\big|\; B \in M_n(\mathbf{Z})\big\}$. Our first result is

Theorem 1. *Let $A \in M_n(\mathbf{Z})$ be such that $A \bmod p$ is nonderogatory for all primes p. Suppose $Q \in M_n(\mathbf{Q})$ is such that $[A, Q] \in M_n(\mathbf{Z})$. Then there exists $P \in M_n(\mathbf{Z})$ with $[A, Q] = [A, P]$. Alternatively, in group theoretic terms, $[A, M_n(\mathbf{Z})]$ is a direct summand of $M_n(\mathbf{Z})$.*

Proof. There exists an integer $k \geq 1$ and an element B in $M_n(\mathbf{Z})$ such that $B = [A, C]$ for some $C \in M_n(\mathbf{Z})$. Let d be the least such integer. If $d > 1$, let p be a prime divisor of d. Then $[A, C] \bmod p \equiv 0$, so $C \bmod p$ commutes with $A \bmod p$. But since $A \bmod p$ is nonderogatory, this implies that $C \equiv f(A) \bmod p$ for some $f(x) \in \mathbf{Z}[x]$. Hence $C - f(A) = pD$ for some $D \in M_n(\mathbf{Z})$. But this implies $dB = p[A, D]$ and thus $(d/p)B \in \big[A, M_n(\mathbf{Z})\big]$, giving a contradiction. Hence $d = 1$.

We now prove

Theorem 2. *Let $P \in M_n(\mathbf{Z})$ be such that $P \bmod p$ is nonderogatory for all primes p. Let $A \in M_n(\mathbf{Z})$. Then $A = [P, Q]$ for some $Q \in M_n(\mathbf{Z})$ if and only if $\operatorname{trace} P^i A = 0$ for $i = 0, 1, 2, \ldots, n-1$.*

Proof. Clearly the condition $\operatorname{trace} P^i A = 0$ for all $i \geq 0$ is necessary for A to be of the form $[P, Q]$. Conversely the set of trace conditions and the fact that P is nonderogatory as an element of $M_n(\mathbf{Q})$ implies $A = [P, Q_0]$ for some $Q_0 \in M_n(\mathbf{Q})$. But now the result follows from Theorem 1.

4. Main Theorem

In this section we prove that every integer matrix A of $\operatorname{trace} 0$ is a commutator $[P, Q]$ of integer matrices P, Q. For a large class of matrices it is shown that P can be chosen integrally similar to the Jordan canonical form $J_k(1) \oplus J_{n-k}(0)$ where $k = [n/2]$ and $J_r(a)$ denotes the $r \times r$ lower Jordan block with eigenvalue a. Such a P cannot work for every A since for example if $A \equiv bI \bmod p$ where p is a prime and $b \not\equiv 0 \bmod p$ (e.g. $A = \operatorname{diag}(1, 1, -2), p = 3$), and if $A = [X, Y]$ for $X, Y \in M_n(\mathbf{Z})$, then over $\mathbf{Z}_p$, the Jordan form of $P \bmod p$ must have blocks occurring with multiplicity p (see Anderson and Parker [2]) which does not hold for P here if n is odd.

Theorem 3. *Let $A \in M_n(\mathbf{Z})$ have trace zero. Then $A = PQ - QP$ for some $P, Q \in M_n(\mathbf{Z})$.*

Proof. If $n = 2$, the result has been proved by Lissner[8] and Vaserstein[12]. However since the proof of the theorem for $n > 2$ is not related to their proof, we first provide a proof for $n = 2$ by our methods, since it will help to motivate and explain the methods for $n > 2$.

Suppose then that $n = 2$. Since there exist rational matrices R, S with $A = RS - SR$, there exists a positive integer m such that $mA = PQ - QP$ for some $P, Q \in M_2(\mathbf{Z})$. Among all such representations, assume P, Q have been chosen so that m is least possible. Suppose for the sake of contradiction that $m > 1$ and let p be a prime divisor of m. Now $P \bmod p$, $Q \bmod p$ commute as elements of $M_2(\mathbf{Z}_p)$. If $P \bmod p$ is non-scalar, then $P \bmod p$ is nonderogatory over $\mathbf{Z}_p$ (since $n = 2$), so $Q \bmod p = f(P) \bmod p$ for some polynomial $f(x) \in \mathbf{Z}[x]$. But now $Q - f(P) \in M_2(\mathbf{Z})$ is of the form pQ_1 for some $Q_1 \in M_2(\mathbf{Z})$ and $mA = [P, Q] = p[P, Q_1]$ forcing $(m/p)A = [P, Q_1]$, contradicting the minimality of m. Hence $m = 1$ as desired. If $P \bmod p$ is scalar, then $P = \alpha I + pP_1$, some $\alpha \in \mathbf{Z}$, $P_1 \in M_2(\mathbf{Z})$, and $(m/p)A = [P_1, Q]$, giving a contradiction also.

Suppose now that $n > 2$. We may replace A by a matrix integrally similar to A and hence, using Proposition 2, we may assume $A = (a_{ij})$ where $a_{12} \geq 1$ and a_{12} divides all $a_{ij} (i \neq j)$ and $a_{ii} - a_{jj}$ $(1 \leq i, j \leq n)$ and $a_{kl} = 0$ for $l \geq k + 2$ $(k = 1, 2, \ldots, n - 2)$. If the highest common factor $h = (a_{11}, a_{12}) \neq 1$, then the result for A follows from that for the integral matrix $\left(\frac{1}{h}\right) A$. So we assume $(a_{11}, a_{12}) = 1$. Using a similarity of the form

$$A \longrightarrow X^{-1}AX \quad \text{where } X = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \oplus I_{n-2}$$

and $x \in \mathbf{Z}$ replaces a_{22} by $a_{22} - xa_{12}$ while preserving a_{jj} $(j > 2)$ and all the other properties of A noted above. Let $k = [n/2]$. Let $c(A) = a_{22} + a_{44} + \cdots + a_{2k2k}$. Then $c(X^{-1}AX) = a_{22} - xa_{12} + a_{44} + \cdots + a_{2k2k}$. Choose x if possible to make $c(X^{-1}AX) = 0$. Note that this choice is possible if a_{12} divides $c(A)$ and in particular if $a_{12} = 1$. Assume then that $c(A) = 0$. Let $P = (p_{ij})$ be the $(0, 1)$ matrix defined as follows:

$$\begin{aligned} p_{ii} &= 1 \quad \text{for } i = 2, 4, \ldots, 2k \\ p_{i,i-2} &= 1 \quad \text{for } i = 3, 4, \ldots, n \\ p_{ij} &= 0 \quad \text{otherwise} \end{aligned}$$

[For example, if $n = 5$,

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}].$$

Observe that for $m \geq 1$, P^m has the same diagonal as P and that P^m has its (i,j) entry 0 if $i \neq j$ and $i - j < 2$. Also $\operatorname{trace}(PA) = c(A)$ and $\operatorname{trace}(P^m A) = 0$ for $m = 0, 1, 2, \ldots$, since $c(A) = 0$ ensures that the diagonal of P^m contributes 0 to the trace of $P^m A$ while $E_{ij}A = 0$ for $i - j \geq 2$ since $a_{ji} = 0$ in this case, so the off-diagonal entries of P^m also contribute 0 to $\operatorname{trace} P^m A$.

Let $R = J_k(1) \oplus J_{n-k}(0)$ and let Y be the permutation matrix

$$\begin{array}{r} k\left\{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right. \\ n-k\left\{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right. \end{array} \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & & & \ddots & \\ \vdots & & & & & & & & \ddots \\ 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots \\ & & & & & & \ddots & & \\ & & & & & & & \ddots & \\ & & & & & & & & \ddots \end{pmatrix}$$

of the permutation

$$i \longrightarrow 2i \quad (1 \leq i \leq k)$$
$$k + i \longrightarrow 2i - 1 \quad (1 \leq i \leq n - k).$$

Observe that $YPY^{-1} = R$. Hence P is integrally similar to R and thus $P \bmod p$ is nonderogatory for all primes p. But then the equations $\operatorname{trace}(P^i A) = 0$ for $i = 0, 1, \ldots, n-1$ imply that $A = [P, Q]$ for some $Q \in M_n(\mathbf{Z})$, by Theorem 1.

Suppose then that x cannot be chosen to make $c(X^{-1}AX) = 0$. Put

$$d(A) = a_{12} + a_{23} + \cdots + a_{n-1\,n}.$$

Suppose that $d(A) = 0$. Let P be the $n \times n$ lower Jordan block with eigenvalue 0. So $P = (p_{ij})$ where $p_{i,i-1} = 1$ for $i = 2, 3, \ldots, n$ and all other $p_{ij} = 0$. Note that $\operatorname{trace}(PA) = d(A) = 0$ and that $\operatorname{trace}(P^i A) = 0$ for $i > 1$ since $a_{rs} = 0$ for $s \geq r + 2$. Hence $\operatorname{trace}(P^m A) = 0$ for all non-negative integers m and since $P \bmod p$ is nonderogatory for all primes p, Theorem 1 ensures that $A = [P, Q]$ for some $Q \in M_n(\mathbf{Z})$.

Consider next the case where $d(A) \neq 0$ but x can be chosen so that $c(X^{-1}AX)$ (where $X = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \oplus I_{n-2}$ as before) divides $d(A)$. [Observe that since $a_{ij} = 0$ for $j \geq i + 2$, $d(X^{-1}AX) = d(A)$ for all such X]. Replacing A by $X^{-1}AX$, we may thus

assume that $d(A) = -wc(A)$ where w is an integer. Define $P = (p_{ij})$ as follows: $p_{ii} = w$ for $i = 2, 4, \ldots, 2k$, $p_{j,j-1} = 1$ for $j = 2, 3, \ldots, n$ and all other $p_{ij} = 0$. Note that P^t is not contained in the span of $I, P, P^2, \ldots, P^{t-1}$ for $t = 1, 2, \ldots, n-1$ modulo any prime, since P^t has its $(t+1, 1)$ entry equal to 1 while $P^s (s < t)$ has its $(t+1, 1)$ entry equal to 0. Note also that $\text{trace}(PA) = d(A) + wc(A) = 0$. Observe that $P^2 - wP$ is lower triangular and that its (r, s) entry is 0 for $s \geq r - 1$. It then follows that $\text{trace}\, P^m(P^2 - wP)A = 0$ for all integers $m \geq 0$. Hence by induction $\text{trace}\, P^m A = 0$ for all integers $m \geq 0$. So by Theorem 1, $A = [P, Q]$ for some $Q \in M_n(\mathbf{Z})$.

Suppose that n is even. Write $n = 2m$. The fact that $\text{trace}(A) = 0$ and $(a_{11}, a_{12}) = 1$ implies that a_{12} divides $2m$. If a_{12} divides m, then we can choose X as in an earlier part of the proof to ensure that $c(X^{-1}AX) = 0$. Suppose a_{12} does not divide m. Write $a_{12} = 2t$, $m = st$. So s is odd. Now $c(A)$ is of the form $ma_{11} + ka_{12} = t(sa_{11} + 2k)$ while $d(A)$ is divisible by $a_{12} = 2t$. Hence we can choose X as in the last paragraph to ensure that $c(X^{-1}AX) = t$ and hence that $c(X^{-1}AX)$ divides $d(X^{-1}AX)$. It remains to consider the case where n is odd.

Suppose that x cannot be chosen to ensure that $c(X^{-1}AX)$ divides $d(A)$. Consider the Diophantine equation

$$xa_{12} + a_{23} + \cdots + a_{n-1\,n} = yc(A).$$

Since a_{12} divides $a_{23}, \ldots, a_{n-1\,n}$, this may be written

$$a_{12}(x + l) = yc(A) \qquad (**)$$

We wish to find a solution of $(**)$ with the highest common factor $(x, y) = 1$. Write $n = 2m + 1$. The fact that $\text{trace}(A) = 0$ yields $na_{11} + va_{12} = 0$ for some integer v and thus, using $(a_{11}, a_{12}) = 1$, that a_{12} divides n. Hence $(m, a_{12}) = 1$. Hence a_{12} divides y and thus $(x, a_{12}) = 1$.

Write $y = a_{12}z$. So $x = cz - l$ where $c = c(A)$. We wish to choose z so that $(cz - l, a_{12}z) = 1$. Let $l_0 = (l, c)$ and write $l = l_0 l_1$, $c = l_0 c_1$.

Then $(cz - l, a_{12}z) = \big(l_0(c_1 z - l_1), a_{12}z\big)$.

Take z to be the product of all primes dividing a_{12} which do not divide l. (If no such primes occur, take z to be a prime not dividing l.)

Then $(cz - l, a_{12}z) = 1$. Thus $x = cz - l$, $y = a_{12}z$ satisfy

$$xa_{12} + a_{23} + \cdots + a_{n-1\,n} = yc(A)$$

and $(x, y) = 1$. Conjugating A by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a_{32}/a_{12} & 0 & 1 \end{pmatrix} \oplus I_{n-3} \in GL(n, \mathbf{Z})$$

does not change $d(A)$ or $c(A)$ but replaces the $(3, 2)$ entry of A by 0. Hence we assume $a_{32} = 0$. Note that

$$x^2 a_{12} + xy(a_{11} - a_{22}) - y^2(a_{21} + y a_{31}) \neq 0,$$

since a_{12} divides y and $a_{11} - a_{22}$ while $(x, a_{12}) = 1$ and $a_{12} = 1$ implies that X could have been chosen above to make $c(A) = 0$, contrary to hypothesis. Choose an integer q such that $p = |x + qy|$ is an odd prime greater than $\left|x^2 a_{12} + xy(a_{11} - a_{22}) - y^2(a_{21} + y a_{31})\right|$. (Dirichlet's theorem on the existence of primes in arithmetic progression guarantees the existence of q).

Note that $\begin{vmatrix} x & -y \\ q & 1 \end{vmatrix} = \epsilon p$ where $\epsilon = \pm 1$. Let $P = (p_{ij})$ be the following matrix

$$\begin{aligned} p_{ii} &= -y \quad \text{for } i = 2, 4, \ldots, 2k \\ p_{21} &= \quad x \\ p_{31} &= \quad q \\ p_{j\,j-1} &= \quad 1 \quad \text{for } j = 3, 4, \ldots, n \\ p_{rs} &= \quad 0 \quad \text{otherwise} \end{aligned}$$

[For example, if $n = 5$

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ x & -y & 0 & 0 & 0 \\ q & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -y & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}].$$

Note that $\operatorname{trace}(PA) = 0$ since the contribution of the diagonal of P to it is $-yc(A)$ while the off-diagonal part of P contributes $xa_{12} + a_{23} + \cdots + a_{n-1\,n} = a_{12}(x + l)$. (Note the entry q does not contribute since $a_{rs} = 0$ for $s \geq r + 2$). Next, note that $P^2 + yP$ is lower triangular and that its (r, s) entry is 0 if $s \geq r - 1$. Since $\operatorname{trace} E_{rs} A = 0$ if $s < r - 1$ (since $a_{sr} = 0$), it follows that $\operatorname{trace}(P^2 + yP)A = 0$ and more generally, using the fact that P is lower triangular, we have $\operatorname{trace}(P^m A) = 0$ for all integers $m \geq 0$. If P were nonderogatory modulo all primes, then we could conclude $A = [P, Q]$, as required. However this is not the case. We observe however that $P \bmod \pi$ is nonderogatory for all primes $\pi \neq p$. To see

this note that the $(n,1)$ entry of $P^a (1 \leq a \leq n-2)$ is 0 while the $(n,1)$ entry of P^{n-1} is $\epsilon p \not\equiv 0 \bmod \pi$. So the minimal polynomial of $P \bmod \pi$ has degree n.

Since P is nonderogatory as a matrix in $M_n(\mathbf{Q})$ and $\operatorname{trace}(P^m A) = 0$ for all nonnegative integers m, we can write $A = [P, Q]$ for some $Q \in M_n(\mathbf{Q})$ and thus clearing denominators in Q, we find that there is a positive integer t such that $tA = [P, Q_1]$ for some $Q_1 \in M_n(\mathbf{Z})$. Assume that Q_1 has been chosen so that the corresponding t is least possible. We first claim that t must be a power of p. For if some prime $\pi \neq p$ divides t, the fact that $tA = [P, Q_1]$ implies $[P, Q_1] \equiv 0 \bmod \pi$, so $Q_1 \equiv g(P) \bmod \pi$ for some $g(x) \in \mathbf{Z}[x]$ and then $(t/\pi)A = [P, Q_2]$ for some $Q_2 \in M_n(\mathbf{Z})$, as in the proof of Theorem 1. This contradicts the minimality of t. Hence we have $t = p^b$ for some integer $b \geq 0$ and $p^b A = [P, Q_1]$ for some $Q_1 \in M_n(\mathbf{Z})$. Assume that b is chosen least possible subject to this. If $b = 0$ the theorem is proved. Suppose $b > 0$. Then $Q_1 \bmod p$ commutes with $P \bmod p$. The strategy is now to show that P may be replaced by a matrix P_1 which is nonderogatory mod p and then use the argument of Theorem 1. For ease of calculation, we may perform an integral similarity on A, replacing A by $Y^{-1}AY = A_0$, P by $Y^{-1}PY = P_0$, and Q_1 by $Y^{-1}Q_1Y = Q_0$, say, where $Y = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} \oplus I_{n-2}$. Note

$$P_0 \bmod p = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & -y & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & -y & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & \ddots & & & & \\ \vdots & & & & & \ddots & & & \\ \vdots & & & & & & \ddots & & 0 \\ 0 & 0 & 0 & 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix}$$

So

$$P_0 \bmod p = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & S & \\ 0 & & & \end{pmatrix}$$

where $S \in M_{n-1}(\mathbf{Z}_p)$ is nonderogatory. Hence the Jordan form of $P_0 \bmod p$ is

$$J_m(-y) \oplus J_1(0) \oplus J_m(0) = J, \qquad \text{say}$$

A matrix

$$H = \begin{pmatrix} H_{11} & H_{12} & H_{13} \\ H_{21} & h_{22} & H_{23} \\ H_{31} & H_{32} & H_{33} \end{pmatrix}$$

where H_{11}, H_{33} are $m \times m$ blocks and h_{22} is a 1×1 block and the other blocks are of compatible sizes, commutes with J if and only if $H_{11}J_m(-y) = J_m(-y)H_{11}$, $H_{12} = 0$, $H_{13} = 0$, $H_{21} = 0$, $H_{31} = 0$, $H_{23}J_m(0) = 0$, $J_m(0)H_{32} = 0$ and $H_{33}J_m(0) = J_m(0)H_{33}$ (since $y \not\equiv 0 \bmod p$). Since $J_m(0)$ has just a 1-dimensional eigenspace corresponding to the eigenvalue 0, it follows that the centralizer $\mathcal{C}$ of P_0 in $M_n(Z_p)$ has dimension $m+1+1+1+m = n+2$ [This also follows from a general formula due to Frobenius.]

We now find a basis for $\mathcal{C}$. First of all $\mathbf{Z}_p[P_0] \subseteq \mathcal{C}$ and $\mathbf{Z}_p[P_0]$ has dimension $n-1$, (Here $\mathbf{Z}_p[P_0]$ means the algebra of all polynomials in P_0 with coefficients in the field of p elements). Also E_{11} and $E_{12}+yE_{13}$ (where $\{E_{ij}\}$ is the set of basic matrix units) are in $\mathcal{C}$ and are linearly independent of $\mathbf{Z}_p[P_0]$, since P_0 is lower-triangular. Also $E_{n1} \in \mathcal{C}$, since n is odd. Note that all elements in $\mathbf{Z}_p[P_0]$ have their $(n,1)$ entries equal to 0. It follows that $\mathcal{C}$ is spanned over $\mathbf{Z}_p$ by

$$\mathbf{Z}_p[P_0] \bigcup \{E_{11}, E_{12}+yE_{13}, E_{n1}\}$$

In $M_n(\mathbf{Q})$, the centralizer of P_0 is $\mathbf{Q}[P_0]$. Note that E_{n1} (interpreted as an integer matrix) is in $\mathbf{Q}[P_0]$.

We have $p^bA_0 = [P_0, Q_0]$ and $b \geq 1$, so $Q_0 \bmod p \in \mathcal{C}$. Hence

$$Q_0 \bmod p \equiv \big(f(P_0) + \alpha E_{11} + \beta(E_{12}+yE_{13}) + \gamma E_{n1}\big) \bmod p$$

for some $\alpha, \beta, \gamma \in \mathbf{Z}$, $f(x) \in \mathbf{Z}[x]$. Hence over $\mathbf{Z}$,

$$Q_0 = f(P_0) + \alpha E_{11} + \beta(E_{12}+yE_{13}) + \gamma E_{n1} + pW$$

for some $W \in M_n(\mathbf{Z})$.

Now

$$\begin{aligned}[P_0, Q_0] &= [P_0, \alpha E_{11} + \beta(E_{12}+yE_{13}) + \gamma E_{n1}] + p[P_0, W] \\ &= \big[P_0, \alpha E_{11} + \beta(E_{12}+yE_{13})\big] + p[P_o, W]\end{aligned}$$

since $[P_0, E_{n1}] = 0$. If α, β are both divisible by p then $[P_0, Q_0] = p[P_0, W_1]$ for some $W_1 \in M_n(\mathbf{Z})$ and this contradicts the minimality of b. Hence at least one of α, β is not divisible by p. If $\alpha \not\equiv 0 \bmod p$ choose t so that $\alpha t \not\equiv 0, -y \bmod p$ and let

$$P_1 = P_0 + t\big(\alpha E_{11} + \beta(E_{12}+yE_{13}) + pW\big).$$

(Such a choice of t is possible since $p > 2$). Note that $P_1 \bmod p$ is similar to $(\alpha t \bmod p)E_{11} \oplus S$ where S (as above) is nonderogatory with no eigenvalue equal to $(\alpha t \bmod p)$. So $P_1 \bmod p$ is nonderogatory.

Thus we conclude that

$$p^b A = [P_0, Q_0] = [P_1, R]$$

where

$$R = \alpha E_{11} + \beta(E_{12} + yE_{13}) + pW$$

and $P_1 \bmod p$ is nonderogatory. Hence $R = f(P_1) + pR_1$ where $f(x) \in \mathbf{Z}[x]$ and $R_1 \in M_n(\mathbf{Z})$. Thus

$$\begin{aligned} p^b A &= \big[P_1, f(P_1) + pR_1\big] \\ &= p[P_1, R_1] \end{aligned}$$

and thus $p^{b-1}A = [P_1, R_1]$. But if $b > 1$, we can repeat the argument to obtain

$$p^{b-2}A = [P_1, R_2]$$

for some $R_2 \in M_n(\mathbf{Z})$ and so on by induction. Hence we conclude that $A = [P_1, Q_1]$ for some $Q_1 \in M_n(\mathbf{Z})$, as required.

It thus remains to consider the case where $\alpha \equiv 0 \bmod p$, $\beta \not\equiv 0 \bmod p$. We show this cannot arise. From

$$\begin{aligned} p^b A_0 &= [P_0, Q_0] \\ &= [P_0, R] \end{aligned}$$

where

$$R = \alpha E_{11} + \beta(E_{12} + yE_{13}) + pW$$

and $\alpha \equiv 0 \bmod p$, $\beta \not\equiv 0 \bmod p$, we conclude from $\operatorname{trace}(RA_0) = 0$ that

$$\operatorname{trace}\big((E_{12} + yE_{13})A_0\big) \equiv 0 \bmod p.$$

But $A_0 = Y^{-1}AY$ where $Y = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} \oplus I_{n-2}$. Hence we obtain

$$-q^2 a_{12} + q(a_{11} - a_{22}) + a_{21} + ya_{31} \equiv 0 \bmod p$$

and thus

$$-q^2 y^2 a_{12} + qy^2(a_{11} - a_{22}) + y^2(a_{21} + ya_{31}) \equiv 0 \bmod p.$$

Writing $qy \equiv -x \bmod p$, this becomes

$$-x^2 a_{12} - xy(a_{11} - a_{22}) + y^2(a_{21} + ya_{31}) \equiv 0 \bmod p$$

But by our choice of p,

$$p > \big|-x^2 a_{12} - xy(a_{11} - a_{22}) + y^2(a_{21} + y_{31})\big| > 0$$

so this situation cannot arise. Thus the proof is complete.

5. Concluding Remarks

The problem of extending the Main Theorem to more general rings is an interesting one. The proofs of Lissner [8] and Vaserstein [12] for $n = 2$ hold for principal ideal domains. Much of the proof given here holds for principal ideal domains also and to obtain the result for, in particular, Euclidean rings would be possible if one could find a replacement for the argument which used Dirichlet's Theorem on the existence of primes in Arithmetic progressions. It is an easy exercise however to show that if F is a field and $R = F[x, y, z]$ the ring of polynomials in the (commuting) indeterminates x, y, z over F, then $\begin{bmatrix} x & y \\ z & -x \end{bmatrix} \in M_2(R)$ is not a commutator in $M_2(R)$. Other examples can be found in Lissner and Vaserstein. Thus the result does not hold for unique factorization domains in general.

6. Acknowledgements

We wish to thank Mike Boyle for carefully reading and especially for detecting an error in an earlier version of this paper. We also wish to thank the referee for a number of helpful comments.

References

[1.] A.A. Albert and B. Muckenhoupt. "On matrices of trace zero". Michigan Math. J. **4**:1–3 (1957).

[2.] J. Anderson and J. Parker "Choices for A in the Matrix Equation $T = AB - BA$." Linear Multilinear Alg. **2**: 203–209 (1974).

[3.] H. Cohn. "A Classical Invitation to Algebraic Numbers and Class Fields". Springer-Verlag. New York. Heidelberg. Berlin (1978).

[4.] D. Goldfeld. "Gauss' class number problem for imaginary quadratic fields." Bull. Amer. Math. Soc. **13**:23–36 (1985).

[5.] F. Grunewald. "Solution of the conjugacy problem in certain arithmetic groups." in *"Word Problems II"*, (ed Adian, Boone, Higman). North-Holland, Amsterdam 1980, pp 101–139.

[6.] F. Grunewald and D Segal. "Some general algorithms." I:Arithmetic Groups. Annals Math, **112**: 531–583 (1980)

[**7.**] C. G. Latimer and C. C. MacDuffee. "A correspondence between classes of ideals and classes of matrices." Ann. Math. **34**:313–316 (1933).

[**8.**] D. Lissner. "Matrices over polynomial rings". Trans. Amer. Math. Soc. **98**:285–305 (1961)

[**9.**] K. Shoda. "Einige Sätze über Matrizen." Japan J. Math. **13**:361–365 (1937)

[**10.**] O. Taussky. "On a theorem of Latimer and MacDuffee." Can. J. Math. **1**:300–302 (1949).

[**11.**] F. Uhlig. "A rational canonical pair form for a pair of symmetric matrices over an arbitrary field F with char $F \neq 2$ and applications to finest simultaneous block diagonalizations." Linear Multilinear Alg. **8**:41–67 (1979).

[**12.**] L. N. Vaserstein. "Noncommutative number theory, algebraic K-theory and algebraic number theory." Amer. Math. Soc. Contemp. Math. **83**:445–449 (1989).