32. On the Stabilizer of Companion Matrices

By Javier GOMEZ-CALDERON

Departmemt of Mathematics, The Pennsylvania State University, U. S. A

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1993)

Let R denote a commutative ring with identity. Let $f(x) = x^n - \sum_{i=0}^{n-1} b_i x^i$ denote a monic polynomial with coefficients in R. Let $C(f)$ denote the companion matrix of $f(x)$ defined by

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & b_0 \\ 1 & 0 & \cdots & 0 & b_1 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & b_{n-1} \end{pmatrix}.$$

In this note we describe the set of $n \times n$ matrices with entries in R that commute with $C(f)$. If $R = GR(p^t, m)$ denote the Galois ring (see note) of order p^{tm} and $f(x)$ is irreducible over the residue field $GR(p, m)$, then we show that there are p^{tmn} $n \times n$ matrices that commute with $C(f)$ and that $p^{(t-1)mn}(p^{mn} - 1)$ of these matrices are invertible.

We now state and prove our main result.

Theorem 1. *Let R denote a commutative ring with identity. For $n \geq 2$, let $M = M_{n\times n}(R)$ denote the ring of $n \times n$ matrices with entries in R. Let $f(x) = x^n - \sum_{i=0}^{n-1} b_i x^i$ denote a monic polynomial in $R[x]$. Let $C(f)$ denote the companion matrix of $f(x)$. Then, $A = (a_{ij}) \in M$ commutes with $C(f)$ if and only if $a_{1j} = b_0 a_{n,j-1}$ and $a_{ij} = a_{i-1,j-1} + b_{i-1} a_{n,j-1}$ for all $2 \leq i, j \leq n$.*

Proof. We have

$$AC(f) = (a_{ij})C(f) = \begin{pmatrix} a_{12} & a_{13} & \cdots & a_{1n} & \sum_{j=1}^{n} b_{j-1} a_{1j} \\ a_{22} & a_{23} & \cdots & a_{2n} & \sum_{j=1}^{n} b_{j-1} a_{2j} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{n2} & a_{n3} & \cdots & a_{nn} & \sum_{j=1}^{n} b_{j-1} a_{nj} \end{pmatrix}$$

and

$C(f)A = C(f)(a_{ij}) =$

$$\begin{pmatrix} b_0 a_{n1} & b_0 a_{n2} & \cdots & b_0 a_{nn} \\ a_{11} + b_1 a_{n1} & a_{12} + b_1 a_{n2} & \cdots & a_{1n} + b_1 a_{nn} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n-1,1} + b_{n-1} a_{n1} & a_{n-1,2} + b_{n-1} a_{n2} & \cdots & a_{n-1,n} + b_{n-1} a_{nn} \end{pmatrix}.$$

Therefore, defining $a_{0j} = 0$ for $1 \leq j \leq n$, $A = (a_{ij})$ commutes with $C(f)$ if and only if

(1) $$a_{ij} = a_{i-1,j-1} + b_{i-1} a_{n,j-1}$$

and

$$\sum_{k=1}^{n} a_{ik}b_{k-1} = a_{i-1,n} + b_{i-1}\, a_{nn} \tag{2}$$

for $1 \leq i \leq n$ and $2 \leq j \leq n$. Therefore, we will complete the proof of the theorem if we show that (1) implies (2).

We now proceed by induction on n.

(a) $n=2$.

$$\sum_{k=1}^{2} a_{1k}b_{k-1} = a_{11}\, b_0 + a_{12}\, b_1 = a_{11}\, b_0 + (a_{01} + b_0 a_{21}) b_1 = a_{11}\, b_0 + a_{21}\, b_0 b_1,$$

$$\sum_{k=1}^{2} a_{2k}b_{k-1} = a_{21}\, b_0 + a_{22}\, b_1 = a_{21}\, b_0 + (a_{11} + b_1 a_{21}) b_1 = a_{11}\, b_1 + a_{21}(b_0 + b_1^2),$$

$a_{02} + b_0\, a_{22} = b_0(a_{11} + b_1\, a_{21}) = a_{11}\, b_0 + a_{21}\, b_0 b_1$, and

$a_{12} + b_1\, a_{22} = a_{01} + b_0 a_{21} + b_1(a_{11} + b_1\, a_{21}) = a_{11}\, b_1 + a_{21}(b_0 + b_1^2)$.

Therefore, $\sum_{k=1}^{2} a_{1k}b_{k-1} = a_{i-1,2} + b_{i-1}a_{22}$ for $1 \leq i \leq 2$.

(b) Assume that the theorem is true for $n-1$.

For $1 \leq i,\ j \leq n-1$ define $a'_{0j}=0$, $b'_j = b_{j+1}$ and a'_{ij} by

$$a'_{ij} = \begin{cases} a_{i+1,j} & \text{if } i > j-1 \\ a_{i+1,i+1} - a_{11} & \text{if } i = j-1. \\ a_{i+1,j} - b_0 a_{n,j-i-1} & \text{if } i < j-1 \end{cases}$$

Thus,

$$a'_{ij} = \begin{cases} a_{i+1,j} = a_{i,j-1} + b_i a_{n,j-1} & \text{if } i > j-1 \\ a_{i+1,i+1} - a_{11} = a_{ii} + b_i a_{ni} - a_{11} & \text{if } i = j-1 \\ a_{i+1,j} - b_0 a_{n,j-i-1} = a_{i,j-1} + b_i\, a_{n,j-1} - b_0 a_{n,j-i-1} & \text{if } i < j-1 \end{cases}$$

$$= a'_{i+1,j-1} + b'_{i-1}\, a'_{n-1,j-1} \quad \text{for all} \quad 1 \leq i \leq n-1 \text{ and } 1 < j \leq n-1.$$

Therefore, we can apply our induction assumption on $n-1$ to obtain

$$\sum_{k=1}^{n-1} a'_{ik}\, b'_{k-1} = a'_{i-1,n-1} + b'_{i-1}\, a'_{n-1,n-1} \text{ for } 2 \leq i \leq n-1.$$

We are ready to prove (2). Our work follows:

$$\begin{aligned}
\sum_{k=1}^{n} a_{ik}\, b_{k-1} &= a_{i1}\, b_0 + \sum_{k=2}^{i-1} a_{ik}\, b_{k-1} + a_{ii}\, b_{i-1} + \sum_{k=i+1}^{n} a_{ik}\, b_{k-1} \\
&= a_{i1}\, b_0 + \sum_{k=2}^{i-1} a'_{i-1,k}\, b'_{k-2} + (a'_{i-1,i} + a_{11}) b_{i-1} \\
&\qquad + \sum_{k=i+1}^{n} (a'_{i-1,k} + b_0\, a_{n,k-i}) b_{k-1} \\
&= a_{i1}\, b_0 + a_{11}\, b_{i-1} + \sum_{k=2}^{n} a'_{i-1,k}\, b'_{k-2} + b_0 \sum_{k=i+1}^{n} a_{n,k-i}\, b_{k-1} \\
&= a_{i1}\, b_0 + a_{11} b_{i-1} + \sum_{k=2}^{n} (a'_{i-2,k-1} + b'_{i-2}\, a'_{n-1,k-1})\, b'_{k-2} \\
&\qquad + b_0 \sum_{k=i+1}^{n} a_{n,k-i}\, b_{k-1} \\
&= a_{i1}\, b_0 + a_{11} b_{i-1} + \sum_{k=1}^{n-1} a'_{i-2,k}\, b'_{k-1} + b'_{i-2} \sum_{j=1}^{n-1} a'_{n-1,j}\, b'_{j-1} \\
&\qquad + b_0 \sum_{k=i+1}^{n} (a_{k,k-i+1} - a_{k-1,k-i})
\end{aligned}$$

$$= a_{i1}\, b_0 + a_{11} b_{i-1} + a'_{i-3,n-1} + b'_{i-3}\, a'_{n-1,n-1}$$
$$+ b'_{i-2}(a'_{n-2,n-1} + b'_{n-2}\, a'_{n-1,n-1}) + b_o(a_{n,n-i+1} - a_{i1})$$
$$= a_{11}\, b_{i-1} + a_{i-2,n-1} - b_0\, a_{n,n-i+1} + b_{i-2}\, a_{n,n-1} + b_{i-1}\, a_{n-1,n-1}$$
$$- b_{i-1}\, a_{11} + b_{i-1} b_{n-1}\, a_{n,n-1} + b_0 a_{n,n-i+1}$$
$$= a_{i-1,n} + b_{i-1}\, a_{nn}.$$

This completes the proof of the Theorem 1.

The following operators D and L_B will simplify our next result.

$$D\begin{pmatrix} a_1 \\ a_2 \\ \cdot \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ a_1 \\ \cdot \\ a_{n-1} \end{pmatrix} \text{and } L_B\begin{pmatrix} a_1 \\ a_2 \\ \cdot \\ a_n \end{pmatrix} = \begin{pmatrix} b_0 a_n \\ b_1 a_n \\ \cdot \\ b_{n-1} a_n \end{pmatrix} \quad \text{where} \quad B = \begin{pmatrix} b_0 \\ b_1 \\ \cdot \\ b_{n-1} \end{pmatrix}.$$

Corollary 2. *With notation as in Theorem* 1, $A \in M$ *commutes with* $C(f)$ *if and only if* $A = \mathrm{Col}[A_1, A_2, \ldots, A_n]$ *for some* $A_1 \in R^n$ *and* $A_i = DA_{i-1} + L_B A_{i-1}$ *for* $i = 2,3,\ldots,n$.

Corollary 3. *Let* F *denote the finite field of order* q. *Let* $f(x) = x^n - \sum_{i=0}^{n-1} b_i x^i$ *denote a monic irreducible polynomial with coefficients in* F. *Then, all nonzero matrices that commute with* $C(f)$ *are invertible.*

Proof. By Corollary 2, there are exactly q^n distinct $n \times n$ matrices that commute with $C(f)$. Now, according to L. E. Dickson in [1 : p. 235], the number of $n \times n$ nonsingular matrices over F that commute with $C(f)$ is $q^n - 1$. Therefore, all nonzero matrices commuting with $C(f)$ are invertible.

Corollary 4. *Let* F *denote the finite field of order* q. *Assume that* $f(x) = x^n - b \in F[x]$ *is irreducible. Let* $H = H(a_1, a_2, \ldots, a_n\,; b)$ *denote a* $n \times n$ *matrix of the form*

$$H = \begin{pmatrix} a_1 & ba_n & \cdots & ba_3 & ba_2 \\ a_2 & a_1 & \cdots & ba_4 & ba_3 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{n-1} & a_{n-2} & \cdots & a_1 & ba_n \\ a_n & a_{n-1} & \cdots & a_2 & a_1 \end{pmatrix}.$$

Then, H *is singular if and only if* $a_1 = a_2 = \ldots = a_n = 0$.

Corollary 5. *Let* F *denote the finite field of order* q. *Assume that* $f(x) = x^3 - b \in F[x]$ *is irreducuble. Then the equation*

$$x^3 + by^3 + b^2 z^3 = 3bxyz$$

has only the trivial solution $x = y = z = 0$ *over the field* F.

Proof. This follows from

$$\det\begin{pmatrix} x & bz & by \\ y & x & bz \\ z & y & x \end{pmatrix} = x^3 + by^3 + b^2 z^3 - 3bxyz.$$

Corollary 6. *Let* $GR(p^t, m)$ *denote the Galois ring (see note below) with order* p^{tm}. *Let* $f(x) = x^n - \sum_{i=0}^{n-1} b_i x^i$ *denote a monic polynomial over* $GR(p^t, m)$. *Assume* $\overline{f(x)}$ *is irreducible over the field* $GR(p, m)$. *Then. there are* p^{tmn} *distinct* $n \times n$ *matrices with entries in* $GR(p^t, m)$ *that commute with* $C(f)$ *and* $p^{(t-1)mn}(p^{mn} - 1)$ *of these matrices are invertible.*

Proof. By Corollary 2, there are p^{tmn} distinct matrices that commute with

$C(f)$. Further, each of these matrices A are determined by their first column values $a_1, a_2, \ldots, a_n$. So, we write $A = A(a_1, a_2, \ldots, a_n)$. Now by Corollary 3, $\bar{A} = \bar{A}(\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n) = \bar{0}$ if and only if det $\bar{A} = 0$. Hence, $A = A(a_1, a_2, \ldots, a_n)$ is invertible if and only if $\bar{a}_i \neq \bar{0}$ for some i, $1 \leq i \leq n$. Therefore, there are $p^{tmn} - p^{(t-1)mn}$ invertible matrices over the ring $GR(p^t, m)$ that commute with $C(f)$.

Note. Galois rings are finite extensions of the residue class ring Z/p^tZ of integers. In particular, if p is a prime and t, $m \geq 1$ are integers, $GR(p^t, m)$ denotes the Galois ring of order p^{tm} which can be obtained as a Galois extension of Z/p^tZ of degree m. Hence $GR(p^t, m)$ can be viewed as $(Z/p^tZ)[x]/(f)$ where f is a monic basic irreducible in $(Z/p^tZ)[x]$ of degree m. Thus $GR(p^t, 1) = Z/p^tZ$ and $GR(p, m) = GF(p^m)$, the finite field of order p^m. Further details concerning Galois rings can be found in Chapter XVI of McDonald [2].

References

[1] L. E. Dickson: Linear Groups. Leipzig (1901).
[2] B. R. McDonald: Finite Rings with Identity. Marcel Dekker, Inc., New York (1974).