Internat. J. Math. & Math. Sci.
VOL. 19 NO. 2 (1996) 327-334

INVARIANCE OF RECURRENCE SEQUENCES UNDER A GALOIS GROUP

HASSAN AL-ZAID and SURJEET SINGH
Department of Mathematics
Kuwait University
P O Box 5969, Safat 13060, KUWAIT

(Received October 25, 1993 and in revised form May 9,1995)

ABSTRACT. Let F be a Galois field of order q, k a fixed positive integer and $R = F^{k\times k}[D]$ where D is an indeterminate Let L be a field extension of F of degree k We identify L_F with $F^{k\times 1}$ via a fixed normal basis B of L over F The F-vector space $\Gamma_k(F)\,(=\Gamma(L))$ of all sequences over $F^{k\times 1}$ is a left R-module For any regular $f(D)\in R$, $\Omega_k(f(D)) = \{S\in\Gamma_k(F) : f(D)S = 0\}$ is a finite $F[D]$-module whose members are ultimately periodic sequences The question of invariance of a $\Omega_k(f(D))$ under the Galois group G of L over F is investigated

KEY WORDS AND PHRASES. Galois field, normal basis, recurrence sequences
1991 AMS SUBJECT CLASSIFICATION CODES. Primary 11B39, Secondary 15A24, 16R20

1. INTRODUCTION.

Let F be a Galois field of order q and $R = F^{k\times k}[D]$, for a fixed positive integer k The set $\Gamma_k(F)$ of all sequences over $F^{k\times 1}$ is a left R-module such that for any $S = (s_n)_{n\geq 0}\in\Gamma_k(F)$ and $f(D) = \sum_i a_i D^i \in R$, $a_i\in F^{k\times k}$, $f(D)S = (s'_n)$ with $s'_n = \sum_i a_i s_{n+i}$ [3] For any regular $f(D)\in R$, the set $\Omega_k(f(D)) = \{S\in\Gamma_k(F) : f(D)S = 0\}$ is a finite $F[D]$-module, whose members are ultimately periodic sequences Let L be the field extension of F of degree k Fix a normal basis $B = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}}\}$ of L over F such that $\sum_{i=0}^{k-1}\alpha^{q^i} = 1$ Through this basis we identify L_F with $F^{k\times 1}$ The Galois group $G(L/F)$ is generated by $\sigma : L\to L$ such that $\sigma(a) = a^q$, $a\in L$ The matrix of σ relative to B is the companion matrix M of $X^k - 1$ We get the inner automorphism $\eta : R\to R$ such that $A^\eta = M^{-1}AM, A\in R$ Then $\Omega_k(f(D))$ is said to be σ-invariant (or invariant under the Galois group $G(L/F)$) if for any $S = (s_n)\in\Omega_k(f(D))$, $S^\sigma = (\sigma(s_n))\in\Omega_k(f(D))$ A brief outline of an application of a σ-invariant $\Omega_k(f(D))$ to the construction of recurring planes is given at the end of this paper Given a regular $f(D)\in R$, if $f^\eta(D) = f(D)$ or $f(D)$ is a left circulant matrix, then $\Omega_k(f(D))$ *is* σ-invariant Here we consider the converse in the sense that if $\Omega(f(D))$ is σ-invariant, does there exist a $g(D)\in R$ such that $g^\eta(D) = g(D)$ and $\Omega(f(D)) = \Omega(g(D))$? In this paper we give a complete answer for the case $k = 2$, in Theorems (2) and (3) We also give an explicit construction of a generating set and the dimension of an $\Omega_2(f(D))$ if $f^\eta(D) = f(D)$, in Theorem 4 An illustration of Theorem 4 is given in Example 15 The case, for any $k > 3$ remains unsolved

2. PRELIMINARIES

Let F be a Galois field of order q and $\Gamma(F)$ be a left $F[D]$-module of all sequences over F, [2] For any $f(D)\neq 0$ in $F[D]$, $\Omega(f(D)) = \{S\in\Gamma(F) : f(D)S = 0\}$ is an $F[D]$-submodule of $\Gamma(F)$ isomorphic to $F[D]/F[D]f(D)$ For any two non-zero polynomials $f(D), g(D)\in F[D]$, $f(D)\wedge g(D)$ and $f(D)\vee g(D)$ will denote their gcd and lcm respectively, $0\wedge f(D)$ is the monic factor of $f(D)$ of degree same as deg $f(D)$ The following is well known (see [1] or [2])

THEOREM 1. For any two non-zero polynomials $f(D)$, $g(D)$ in $F[D]$

(i) $\Omega(f(D)) + \Omega(g(D)) = \Omega(f(D) \vee g(D))$

(ii) $\Omega(f(D)) \cap \Omega(g(D)) = \Omega(f(D) \wedge g(D))$

(iii) $f(D)\Omega(g(D)) = \Omega(g(D)/d(D))$, where $d(D) = f(D) \wedge g(D)$

For a fixed positive integer k, we consider $R = F^{k\times k}[D] = F[D]^{k\times k}$ Let L be the field extension of $F$of degree k and σ be the F-automorphism of L given by $\sigma(a) = a^q, a \in L$ We fix a normal basis $B = \{\alpha, \alpha^q, ..., \alpha^{q^k}\}$ of L over F satisfying $\sum_{i=0}^{k-1} \alpha^{q^i} = 1$ By using this we identify L with $F^{k\times 1}$ Then $Hom_F(L, L) = F^{k\times k}$ and σ is given by the $k \times k$-matrix

$$M = \begin{bmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

the companion matrix of $X^k - 1$ Then

$$M^{-1} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

For any $A = [a_{ij}] \in R$

$$M^{-1}AM = \begin{bmatrix} a_{22} & a_{23} & \dots & a_{2k} & a_{21} \\ a_{32} & a_{33} & \dots & a_{3k} & a_{31} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{k2} & a_{k3} & \dots & a_{kk} & a_{k1} \\ a_{12} & a_{13} & \dots & a_{1k} & a_{11} \end{bmatrix} = [b_{ij}]$$

where $b_{ij} = a_{i+1\,j+1}$, $i+1$, $j+1$ are positive integers modulo k. The following is immediate

LEMMA 1. For $A = [a_{ij}] \in R$, $M^{-1}AM = A$ iff

$$A = \begin{bmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k \\ a_k & a_1 & \dots & a_{k-2} & a_{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_2 & a_3 & \dots & a_k & a_1 \end{bmatrix}$$

for some $a_i \in F[D]$.

For any $A \in R$, A^η denotes $M^{-1}AM$ If $f(D) \in R$ is regular, then the bound of $f(D)$ is the smallest degree monic polynomial $d(D) \in F[D]$ such that $Rd(D) \subseteq Rf(D)$; $f^*(D) \in R$ is such that $f(D)f^*(D) = d(D)I_k = f^*(D)f(D)$, [3]. Further $\Omega_k(f(D)) = f^*(D)\Omega_k(d(D)I_k)$, $R\Omega_k(f(D)) = \Omega_k(d(D)I_k)$ and $\Omega_k(d(D)I_k) = \Omega(d(D))^{k\times 1}$, [3]. For any module N, N^k denotes the direct sum of k copies of N.

3. A σ-INVARIANT $\Omega_k(f(D))$

We start with the following

LEMMA 2. Let $f(D), g(D) \in R$, both be regular Then $\Omega_k(f(D)) = \Omega_k(g(D))$ iff $Rf(D) = Rg(D)$.

PROOF. Let $d(D) =$ bound $(f(D))$, $d'(D) =$ bound $(g(D))$ Let a sequence $S \in \Gamma(F)$ be a generator of the $F[D]$-module $\Omega(d(D))$ By [3, Lemma (2 4)], the mapping

$$\lambda : R/Rd(D) \to \Omega(d(D))^{k \times k} = [\Omega_k(d(D)I_k)]^k$$

such that for any $\overline{[g_{ij}(D)]} \in \overline{R} = R/Rd(D)$, $\lambda\overline{[g_{ij}(D)]} = [g_{ij}(D)S]$ is a left R-isomorphism If $Rf(D) = Rg(D)$, by [3, Lemma (2 4) (iv)], $\Omega_k(f(D)) = \Omega_k(g(D))$ Conversely, let $\Omega_k(f(D)) = \Omega_k(g(D))$ By [3, Theorem 2 5],

$$\Omega_k(d(D)I_k) = R\Omega_k(f(D)) = R\Omega_k(g(D)) = \Omega_k(d'(D)I_k)$$

i e

$$\Omega(d(D))^{k \times 1} = \Omega(d'(D))^{k \times 1}$$

This gives $d(D) = d'(D)$ As $\Omega(d(D))^{k \times k} = \Omega_k(d(D)I_k)^k$, $\lambda(f^*(D)\overline{R}) = [f^*(D)\Omega_k(d(D)I_k)]^k$ $= \Omega_k(f(D)^k$ and $\lambda(g^*(D)\overline{R}) = \Omega_k(g(D))^k$ As $Rd(D) \subseteq f^*(D)R$ and $Rd'(D) \subseteq g^*(D)R$, we get $f^*(D)R = g^*(D)R$ However $Rf(D) = \{h(D) \in R : h(D)f^*(D) \in d(D)R\}$ (see [3, Lemma (2 2)] As $d(D) = d'(D)$, it gives $Rf(D) = Rg(D)$

PROPOSITION 1. For any regular $f(D) \in R$, the following are equivalent

(i) $\Omega(f(D))$ is σ-invariant

(ii) $\Omega(f(D) = \Omega(f^\eta(D))$

(iii) $Rf(D) = Rf^\eta(D)$

PROOF. For any $S = (s_n) \in \Gamma_k(F)$, let $S^\sigma = (\sigma(s_n)) = (Ms_n)$ Obviously $S \in \Omega(f(D))$ iff $S^\sigma \in \Omega_k(Mf(D)M^{-1})$ Thus $\Omega_k(f(D))$ is σ-invariant iff $\Omega_k(f(D)) = \Omega_k(Mf(D)M^{-1})$ By Lemma 3, $\Omega_k(f(D)) = \Omega_k(Mf(D)M^{-1})$ iff $Rf(D) = R(Mf(D)M^{-1})$ iff $RM^{-1}f(D)M = Rf(D)$ iff $\Omega(f^\eta(D)) = \Omega(f(D))$

The above proposition shows that if $Rf(D) = Rg(D)$ for some $g(D) \in R$ satisfying $g^\eta(D) = g(D)$, then $\Omega(f(D))$ is σ-invariant Is the converse true? We investigate this question

LEMMA 3. Let $f(D) \in R$ be regular such that $Rf(D) = Rf^\eta(D)$, let $f(D) = Xf^\eta(D)$ The following hold

(i) $\det(X) = 1$

(ii) There exists $g(D) \in R$ such that $g^\eta(D) = g(D)$ and $Rf(D) = Rg(D)$ iff for some invertible $A \in R$, $A^\eta = AX$

PROOF. (i) is obvious Let $g(D)$ exist, then $g(D) = Af(D)$ for some invertible $A \in R$ Then $g(D) = g^\eta(D)$, gives $AXf^\eta(D) = A^\eta f^\eta(D)$ Hence $A^\eta = AX$. The converse is obvious.

LEMMA 4. Let $f(D)$ and X be as in Lemma 3 Let X^λ be obtained from X by applying the cyclic permutation $\lambda = (1, 2, 3, \ldots, k)$ to the columns of X Then some k-th root of unity, in some field extension of F, is a characteristic value of X^λ.

PROOF. Let $f(D) = [a_{ij}]$, $X = [x_{ij}]$. The equation $f(D) = Xf^\eta(D)$, gives

$$a_{ij} = \sum_{u=1}^{k} x_{iu} a_{u+1, j+1} \, ,$$

where $u + 1$, $j + 1$ are least positive residues modulo k This is a system of k^2 homogeneous linear equations in a_{ij} By arranging a_{ij}'s in the order

$$a_{11}, a_{21}, \ldots, a_{k1}, a_{12}, a_{22}, \ldots, a_{k2}, \ldots$$

we get the coefficient matrix, the $k^2 \times k^2$-matrix

$$C = \begin{bmatrix} I & -X^{\lambda} & 0 & 0 & \dots & 0 & 0 \\ 0 & I & -X^{\lambda} & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & .. & \dots & .. & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & I & -X^{\lambda} \\ -X^{\lambda} & 0 & 0 & 0 & \dots & 0 & I \end{bmatrix}$$

where I is the $k \times k$-identity matrix As I and X^{λ} commute, C as a matrix over $F[X^{\lambda}, I] \subseteq F^{k \times k}[D]$, has determinant $I - (X^{\lambda})^k$ So for some matrix C' over $F[X^{\lambda}, I]$,

$$CC' = \text{diag}_{k \times k}[I - (X^{\lambda})^k, .., I - (X^{\lambda})^k].$$

By taking determinant over $F[D]$, we get $\det(C)\det(C') = [\det(I - (X^{\lambda})^k)]^k$ As C is singular, we get

$$\det(I - (X^{\lambda})^k) = 0.$$

This completes the proof

COROLLARY 1. For $k = 2$, under the hypothesis of Lemma 4, $X = \begin{bmatrix} a & b \\ -b & c \end{bmatrix}$ with $ac + b^2 = 1$

PROOF. Now $X^{\lambda} = \begin{bmatrix} x_{12} & x_{11} \\ x_{22} & x_{21} \end{bmatrix}$ As 1 or -1 is a characteristic value of X^{λ}, and by Lemma 3, $x_{11}x_{22} - x_{12}x_{21} = 1$, the result follows

THEOREM 2. Let F be a Galois field of characteristic $p \neq 2$ If a regular $f(D) \in R = F^{2 \times 2}[D]$ is such that $\Omega_2(f(D))$ is invariant under σ, then $\Omega_2(f(D)) = \Omega_2(g(D))$ for some $g(D) \in R$ satisfying $g^{\eta}(D) = g(D)$

PROOF. By Proposition 1 $Rf(D) = Rf^{\eta}(D)$ Then $f(D) = Xf^{\eta}(D)$, for some $X = \begin{bmatrix} a & b \\ -b & c \end{bmatrix} \in R$ satisfying $ac + b^2 = 1$ In view of Lemma 3 we find an $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in R$ with $0 \neq \det(A) \in F$ such that $A^{\eta} = AX$, i e

$$\begin{bmatrix} a_{22} & a_{21} \\ a_{12} & a_{11} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a & b \\ -b & c \end{bmatrix}$$

Case I. $b = 0$. Then $A = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$ is a solution

Case II $b \neq 0$ By solving the system of linear equations it can be seen that

$$A = \begin{bmatrix} a_{11} & b^{-1}aa_{11} - b^{-1}a_{22} \\ b^{-1}a_{11} - b^{-1}ca_{22} & a_{22} \end{bmatrix} \tag{3 1}$$

with

$$\det(A) = b^{-2}[2a_{11}a_{22} - aa_{11}^2 - ca_{22}^2] \tag{3 2}$$

We now solve for a_{11}, a_{22}, such that $A \in R$ and $\det(A) = 1$ Then (3 2) gives

$$2a_{11}a_{22} - aa_{11}^2 - ca_{22}^2 = b^2. \tag{3 3}$$

In case $c = 0$, (3 3) becomes

$$a_{11}(2a_{22} - aa_{11}) = 1 .$$

By taking $a_{11} \neq 0$ in F, this equation gives $a_{22} \in F[D]$. Similarly if $a = 0$, we can solve for a_{11} and a_{22} Let $a \neq 0 \neq c$ By multiplying (3 3) by c, and by putting $Y = ca_{22}$, we get

$$(Y - a_{11})^2 = b^2(a_{11}^2 - c) . \tag{3 4}$$

This equation shows that a_{11}, a_{22} should be such that $a_{11}^2 - c = d^2$, for some $d \in F[D]$ Then

$$(a_{11} - d)(a_{11} + d) = c .$$

As c divided $1 - b^2 = (1 - b)(1 + b)$, and $1 - b$, $1 + b$ are coprime, write $c = c_1c_2$, with c_1 and c_2 factors of $1 + b$ and $1 - b$ respectively Put

$$a_{11} - d = c_1, \quad a_{11} + d = c_2 .$$

Then

$$a_{11} = \frac{1}{2}(c_1 + c_2), \quad d = \frac{1}{2}(c_2 - c_1) .$$

Then (3 4) yields

$$Y - a_{11} = \pm bd .$$

To be definite, take $Y - a_{11} = bd$ So that

$$ca_{22} = a_{11} + bd = \frac{1}{2}c_1(1 - b) + \frac{1}{2}c_2(1 + b) .$$

Now $1 - b = c_2d_1$, $1 + b = c_1d_2$ for some d_1, $d_2 \in F[D]$ Consequently

$$a_{22} = \frac{1}{2}(d_1 + d_2) .$$

All that remains to prove is that the other entries of A are in $F[D]$ Now (3 3) yields

$$ab^2 = -(aa_{11} - a_{22})^2 + a_{22}^2(1 - ac) = -(aa_{11} - a_{22})^2 + a_{22}b^2 .$$

Consequently b^2 divides $(aa_{11} - a_{22})^2$ This gives $b^{-1}(aa_{11} - a_{22}) \in F[D]$ Similarly $b^{-1}(a_{11} - ca_{22}) \in F[D]$. This proves the theorem.

We now consider the case of char $F = 2$

THEOREM 3. Let F be a Galois field of characteristic 2 Let $f(D) \in R = F^{2\times 2}[D]$ be regular such that $f(D) = Xf^{\eta}(D)$, for some $X = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \in R$ satisfying $ac + b^2 = 1$ Then there exists $g(D) \in R$ satisfying $Rf(D) = Rg(D)$ and $g^{\eta}(D) = g(D)$ iff one of the following holds

(I) $b = 0$

(II) $b \neq 0$, at least one of a and c is non-zero, $a \wedge c = 1$, $a = r^2$ and $c = s^2$ for some r, $s \in F[D]$.

PROOF. Let $Rf(D) = Rg(D)$ with $g^{\eta}(D) = g(D)$ By Lemma 3 we get an invertible A in R such that $A^{\eta} = AX$ Let $b \neq 0$ As in the proof of Theorem 2

$$A = \begin{bmatrix} a_{11} & b^{-1}aa_{11} + b^{-1}a_{22} \\ b^{-1}a_{11} + b^{-1}ca_{22} & a_{22} \end{bmatrix} \tag{3 5}$$

and $\det(A) = b^{-2}(aa_{11}^2 + ca_{22}^2) = \alpha(\neq 0) \in F$. Thus

$$aa_{11}^2 + ca_{22}^2 = b^2\beta^2, \quad \alpha = \beta^2, \quad \beta \in F. \tag{3 6}$$

As $ac + b^2 = 1$, $a \wedge b = b \wedge c = 1$ Then (3 6) yields $a \wedge c = 1$ Further (3 6) yields

$$[aa_{11} + (1+b)a_{22}]^2 = b^2 a\beta^2.$$

This immediately yields $a = r^2$ for some $r \in R$ Similarly $c = s^2$ for some $s \in R$

Conversely if (I) holds, $A = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$ is a solution Let (II) hold. Then $r \wedge s = 1$ So for some $x, y \in R$

$$rx + sy = b.$$

This gives $aa_{11}^2 + ca_{22}^2 = b^2$ with $a_{11} = x$, $a_{22} = y$. This solves for A.

EXAMPLE 1. Let char $F = 2$ Consider any $b_{12}, b_{22} \in F[D]$ such that $b_{12} + b_{22} \neq 0$. Then

$$f(D) = \begin{bmatrix} b_{22}D + (D+1)b_{12} & b_{12} \\ (D+1)b_{22} + Db_{12} & b_{22} \end{bmatrix}$$

has $\det(f(D)) = D(b_{12} + b_{22})^2 \neq 0$ Thus $f(D)$ is regular. Further $f(D) = Xf^{\eta}(D)$ for $X = \begin{bmatrix} D & D+1 \\ D+1 & D \end{bmatrix}$ By Theorem 3 there does not exist any $g(D) \in R$ satisfying $g^{\eta}(D) = g(D)$ and $\Omega_2(f(D)) = \Omega_2(g(D))$ although $\Omega_2(f(D)) = \Omega_2(f^{\eta}(D))$

We now determine the dimension and the generating set of a $\Omega_2(f(D))$, if $f^{\eta}(D) = f(D)$ We start with the following

LEMMA 5. Let $f(D)$, $g(D)$ and $r(D)$ be any three non-zero members of $F[D]$ such that $r(D)$ divides $g(D)$ Let $d(D) = [g(D)/r(D)] \wedge f(D)$. Then $\{S \in \Omega(g(D)) : f(D)S \in \Omega(r(D))\} = \Omega(r(D)d(D))$

PROOF. Let T be a generator of the $F[D]$-module $\Omega(g(D))$. Then for any $s(D) \in F[D]$, $f(D)s(D)T \in \Omega(r(D))$ iff $g(D)$ divides $f(D)s(D)r(D)$ iff $g(D)/r(D)$ divides $f(D)s(D)$ iff for $d(D) = [g(D)/r(D)] \wedge f(D)$, $g(D)/r(D)d(D)$ divides $s(D)$. Consequently $k = \{S \in \Omega(g(D)) : f(D)S \in \Omega(r(D))\}$ is generated by $g(D)/r(D)d(D)T$. so that $K = \Omega(r(D)d(D))$.

We now consider a regular $A \in R$ such that $A^{\eta} = A$. Then $A = \begin{bmatrix} f(D) & g(D) \\ g(D) & f(D) \end{bmatrix}$ for some $f(D), g(D) \in F[D]$. We write $\triangle = f(D)^2 - g(D)^2 = \det(A)$; clearly $\triangle \neq 0$ Further we put $d(D) = f(D) \wedge g(D)$, $d_f(D) = f(D) \wedge \triangle$ and $d_g(D) = g(D) \wedge \triangle$. As $d_f(D)$ divides $f(D)$ and $f(D)^2 - g(D)^2$ clearly $d_f(D)$ divides $d(D)^2$. So that $(d_f(D) \vee d_g(D))$ divides $d(D)^2$ Obviously $d(D)$ divides $d_f(D) \wedge d_g(D)$ Consequently $d(D) = 1$ iff $d_f(D) = 1 = d_g(D)$ Write $f(D) = f_1(D)d(D)$, $g(D) = g_1(D)d(D)$. Then $f_1(D) \wedge g_1(D) = 1$, gives $f_1(D) \wedge (f_1(D)^2 - g_1(D)^2) = 1$ So that

$$\begin{aligned} d_f(D) &= f_1(D)d(D) \wedge d(D)^2(f_1(D)^2 - g_1(D)^2) \\ &= d(D)(f_1(D) \wedge d(D)). \end{aligned}$$

Similarly $d_g(D) = d(D)(g_1(D) \wedge d(D))$ Consequently $d_f(D) \wedge d_g(D) = d(D)$ Further $d_f(D) \vee d_g(D) = [d_f(D)d_g(D)]/d(D)$ We collect these results in the following

LEMMA 6. For $A = \begin{bmatrix} f(D) & g(D) \\ g(D) & f(D) \end{bmatrix}$

(i) $d(D) = f(D) \wedge g(D) = d_f(D) \wedge d_g(D)$ and $d_f(D) \vee d_g(D)$ divides $d(D)^2$

(ii) $d(D) = 1$ iff $d_f(D) = 1 = d_g(D)$

(iii) $d_f(D) \vee d_g(D) = [d_f(D)d_g(D)]/d(D)$

We now prove the theorem that describes generators and the dimension of a $\Omega_2(A)$ with $A'' = A$ Here $A = \begin{bmatrix} f(D) & g(D) \\ g(D) & f(D) \end{bmatrix} = d(D)\begin{bmatrix} f_1(D) & g_1(D) \\ g_1(D) & f_1(D) \end{bmatrix} = d(D)A'$, $d(D) = f(D) \wedge g(D)$ Write $\triangle_1 = \det(A')$ By (2 10), $g_1(D) \wedge \triangle_1 = 1 = f_1(D) \wedge \triangle_1$ So for some μ, μ', $\lambda, \lambda' \in F[D]$

$$f_1(D) = \mu g_1(D) + \lambda\triangle_1 \tag{3 7}$$

$$g_1(D) = \mu' f_1(D) + \lambda'\triangle_1 \tag{3 8}$$

Let

$$d_1(D) = (\mu - \mu') \wedge \triangle_1 . \tag{3 9}$$

We shall use the above expressions and the other previously given notations in the subsequent results

LEMMA 7. Let T_1 be a generator of the $F[D]$-module $\Omega(d_1(D))$ Then for

$$A' = \begin{bmatrix} f_1(D) & g_1(D) \\ g_1(D) & f_1(D) \end{bmatrix}$$

$$\Omega_2(A') = \begin{bmatrix} T_1 \\ -\mu T_1 \end{bmatrix} .$$

PROOF. As $\det(A') = \triangle_1$, $\Omega_2(A') \subseteq \Omega(\triangle_1)^{2\times 1}$ Let T be a generator of the $F[D]$-module $\Omega(\triangle_1)$ Let $\begin{bmatrix} S_1 \\ S_2 \end{bmatrix} \in \Omega_2(A')$ Now $S_1 = s(D)T$ for some $s(D) \in F[D]$ and $f_1(D)S_1 = -g_1(D)S_2$ and $g_1(D)S_1 = -f_1(D)S_2$ By (3 7) $f_1(D)S_1 = f_1(D)(s(D)T) = g_1(D)(\mu s(D)T)$ So that $g_1(D)(S_2 + \mu s(D)T) = 0$ This gives $S_2 + \mu s(D)T \in \Omega(g_1(D)) \cap \Omega(\triangle_1) = 0$, as $g_1(D) \wedge \triangle_1 = 1$ Consequently $S_2 = -\mu s(D)T$ Similarly we also get $S_2 = -\mu' s(D)T$ So that $s(D)(\mu - \mu')T = 0$ Consequently $\triangle_1$ divides $s(D)(\mu - \mu')$ As $d_1(D) = (\mu - \mu') \wedge \triangle_1$, we get $\triangle_1/d_1(D)$ divides $s(D)$ Conversely if $\triangle_1/d_1(D)$ divides $s(D)$, it is immediate that $\begin{bmatrix} s(D)T \\ -\mu s(D)T \end{bmatrix}$ is in $\Omega_2(A')$ Thus $\Omega_2(A')$ is the cyclic $F[D]$-module generated by $\begin{bmatrix} T_1 \\ -\mu T_1 \end{bmatrix}$ where $T_1 = [\triangle_1/d_1(D)]T$ is a generator of $\Omega(d_1(D))$

THEOREM 4. Let $A = \begin{bmatrix} f(D) & g(D) \\ g(D) & f(D) \end{bmatrix} = d(D)\begin{bmatrix} f_1(D) & g_1(D) \\ g_1(D) & f_1(D) \end{bmatrix} \in R$ be regular Then

$$\Omega_2(A) = F[D]\begin{bmatrix} T \\ -\mu T \end{bmatrix} \oplus F[D]\begin{bmatrix} 0 \\ T' \end{bmatrix} .$$

Where T and T' are generators of the $F[D]$-modules $\Omega(d_1(D)d(D))$ and $\Omega(d(D))$ respectively Further $\dim(\Omega_2(A)) = \deg(d_1(D)d(D)) + \deg d(D)$

PROOF. Now $\triangle_1 = \triangle/d(D)^2$ So by (3 9) $d_1(D)d(D)$ divides $\triangle$ Consequently by Lemma 5 $\Omega(d_1(D)d(D)) = \{S \in \Omega(\triangle) : d(D)S \in \Omega(d_1(D))\}$ Let T be a generator of the $F[D]$-module $\Omega(d_1(D)d(D))$, then $T_1 = d(D)T$ is a generator of $\Omega(d_1(D))$ Given $\begin{bmatrix} S_1 \\ S_2 \end{bmatrix} \in \Omega_2(A)$,

$$d(D)\begin{bmatrix} S_1 \\ S_2 \end{bmatrix} \in \Omega_2(A'), \text{ by (2 11)}, \; d(D)\begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = s(D)\begin{bmatrix} T_1 \\ -\mu T_1 \end{bmatrix}, \; s(D) \in F[D] .$$

Thus $d(D)S_1 = s(D)T_1 \in \Omega(d_1(D))$ Consequently $S_1 \in \Omega(d_1(D)d(D))$ Furthermore we get $d(D)S_2 = -s(D)\mu T_1 = -\mu d(D)S_1$ So that $S_2 + \mu S_1 \in \Omega(d(D))$ Hence

$$\begin{bmatrix} S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} S_1 \\ -\mu S_1 \end{bmatrix} + \begin{bmatrix} 0 \\ S' \end{bmatrix}$$

with $S_1 \in \Omega(d_1(D)d(D))$, $S' \in \Omega(d(D))$ So that $\Omega_2(A) \subseteq F[D]\begin{bmatrix} T \\ -\mu T \end{bmatrix} + F[D]\begin{bmatrix} 0 \\ T' \end{bmatrix}$ It is now immediate that

$$\Omega_2(A) = F[D]\begin{bmatrix} T \\ -\mu T \end{bmatrix} \oplus F[D]\begin{bmatrix} 0 \\ T' \end{bmatrix}.$$

The last part is now obvious

EXAMPLE 2. Let F be any Galois field of characteristic 3,

$$A = (D+2)\begin{bmatrix} f(D) & g(D) \\ g(D) & f(D) \end{bmatrix} \text{ with } f(D) = 2D^2 + 2D,\ g(D) = D^2 + D + 1.$$

In the notations of Theorem 4, $d(D) = (D+2)$, $\mu = \mu' = 1, \triangle = (D+2)^2(D^2+D+2)$, $\triangle_1 = D^2 + D + 2$, $d_1(D) = (\mu - \mu') \wedge \triangle_1 = D^2 + D + 2$ So that $d_1(D)d(D) = D^3 + D + 1$ The impulse response sequence T in $\Omega(d_1(D)d(D))$ is of period 8, and its initial cycle is

00102212.

Theorem 4 gives that $\Omega_2(A)$ consists of all sequences of least periods, factors of 8, with first eight terms

$$\begin{bmatrix} c \\ 2c+d \end{bmatrix}, \begin{bmatrix} b \\ 2b+d \end{bmatrix}, \begin{bmatrix} a+2c \\ 2a+c+d \end{bmatrix}, \begin{bmatrix} 2b+2c \\ b+c+d \end{bmatrix}, \begin{bmatrix} 2a+2b+c \\ a+b+2c+d \end{bmatrix},$$
$$\begin{bmatrix} 2a+b+2c \\ a+2b+c+d \end{bmatrix}, \begin{bmatrix} a+2b \\ 2a+b+d \end{bmatrix}, \begin{bmatrix} a+2b \\ 2a+b+d \end{bmatrix}, \begin{bmatrix} 2a \\ a+d \end{bmatrix} \text{ with } a, b, c, d \in F.$$

We end this paper with a brief outline of an application of the σ-invariant sequences to recurring planes A recurring plane over a Galois field F is a matrix, $\overline{A} = [a_{ij}]$ over F, indexed by the set of natural numbers and for which there exist positive integers p, q satisfying $a_{ij} = a_{i+p,j} = a_{i,j+q}$ for all i, j Any such ordered pair (p, q) is called a period of the plane Any consecutive k rows of $\overline{A}$ constitute a matrix $A' = [a_{ij}]$, $s \leq i \leq k + s - 1, j \geq 0$. Each column of A' being a member of $F^{k\times 1}$, we can regard A', a sequence in $\Gamma_k(F)$ Given a regular $f(D) \in F^{k\times k}[D]$, call a recurring plane $\overline{A}$ a row($f(D)$)-plane, if every submatrix of $\overline{A}$ constituted by any k consecutive rows of $\overline{A}$, is a member of $\Omega_k(f(D))$. Given an $f(D)$ such that $\Omega_k(f(D))$ is σ-invariant, each $s \in \Omega_k(f(D))$ gives a row($f(D)$)-plane $\overline{A} = [a_{ij}]$ whose i-th row equals an s-th row of S if $i \equiv s (\text{mod } k)$ The set of these planes can be easily seen to be closed under component-wise addition, shifts of rows, and of columns Their detailed study will be done in some later paper

ACKNOWLEDGMENT. This research was partially supported by the Kuwait University Research Grant No SM075 We thank the referee for his valuable suggestions

REFERENCES

[1] LIDL, R and NIEDERREITER, H, Finite fields, *Encyclopedia of Mathematics and Its Applications,* **20**, Addison Wesley Publishing Co , 1983

[2] SINGH, S , A note on recurring sequences, *Linear Algebra Appl.*, **104** (1988), 97-101.

[3] SINGH, S , Recurrence sequences over vector spaces, *Linear Algebra Appl.*, **131** (1990), 93-106