

where the  $d_i(\lambda)$  are monic of positive degree and  $d_i(\lambda) \mid d_j(\lambda)$  if  $i \leq j$ . By the irreducibility of  $d_s(\lambda) = m(\lambda) = \lambda^3 + \lambda^2 - 1$ , we have

$$d_1(\lambda) = d_2(\lambda) = \cdots = d_s(\lambda) = \lambda^3 + \lambda^2 - 1.$$

Since  $\det(\lambda I - A) = d_1(\lambda) \cdots d_s(\lambda)$ ,

$$3 \cdot s = \deg(\det(\lambda I - A)) = n.$$

Thus we have proved that 3 divides the dimension of  $V$ .

If  $\dim V = 3$ , then  $\lambda I - A$  is equivalent to  $\text{diag}\{1, 1, \lambda^3 + \lambda^2 - 1\}$ . The rational canonical form for  $A$  (or  $T$ ) is  $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ . It follows that all the  $T$ 's are similar when  $\dim V = 3$ .

### 1108

Let  $F_q$  be a finite field with  $q = p^n$  elements, where  $p$  is a prime. Let  $\Pi : F_q \rightarrow F_q$  be the Frobenius automorphism  $\Pi(x) = x^p$ . Prove that  $\Pi$  considered as a linear map over  $F_p$  is diagonalizable if and only if  $n$  divides  $p^n - 1$ . (Here is a misprint. It should be " $n$  divides  $p - 1$ ".)

(Harvard)

#### Solution.

It is wellknown that  $F_p \subseteq F_q$  is a Galois extension with

$$\text{Gal}(F_q/F_p) = \{1, \Pi, \Pi^2, \dots, \Pi^{n-1}\}.$$

By the Normal Base Theorem, there exists a  $u \in F_q$  such that  $\{u, \Pi(u), \Pi^2(u), \dots, \Pi^{n-1}(u)\}$  is a base for  $F_q$  over  $F_p$ . When  $\Pi$  is considered as a linear map of  $F_q$  over  $F_p$ , the matrix of  $\Pi$  relative to the base  $\{u, \Pi(u), \Pi^2(u), \dots, \Pi^{n-1}(u)\}$  is

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

The normal form for  $\lambda E - M$  is  $\text{diag}\{1, \dots, 1, \lambda^n - 1\}$  and the minimal polynomial  $m(\lambda)$  of  $M$  is  $\lambda^n - 1 = \det(\lambda E - M)$ .

Suppose that  $\Pi$  is diagonalizable as a linear map over  $F_p$ . Then  $m(\lambda) = \lambda^n - 1$  has no multiple root, and all the roots of  $\lambda^n - 1$  are in  $F_p$ . On the other

hand, all the root of  $\lambda^n - 1$  forms a subgroup of  $F_p^* = F_p \setminus \{0\}$ . Thus  $n$  divides  $p - 1$ .

Conversely, if  $n$  divides  $p - 1$ ,  $\lambda^n - 1$  has no multiple root and

$$\lambda^n - 1 = (\lambda - 1) \cdot (\lambda - a^d)(\lambda - a^{2d}) \cdots (\lambda - a^{(n-1)d})$$

where  $d = \frac{p-1}{n}$  and  $a$  is the generator of the group  $F_p^*$ . Hence  $M$  is similar to  $\text{diag}\{1, a^d, \dots, a^{(n-1)d}\}$  in  $M_n(F_p)$ . So  $\Pi$  is diagonalizable as a linear map over  $F_p$ .

## 1109

Let  $A(t)$  be a non-singular matrix whose elements are differentiable functions of real variable  $t$ . Let  $A'(t)$  denote the matrix formed by the derivatives of the elements. Show that the derivative of the determinant  $\det A$  satisfies

$$\frac{d}{dt}(\det A) = \det A \cdot \text{trace}(A' \cdot A^{-1}).$$

(Harvard)

**Solution.**

Let

$$A(t) = \begin{pmatrix} a_{11}(t) & a_{12}(t) & \cdots & a_{1n}(t) \\ a_{21}(t) & a_{22}(t) & \cdots & a_{2n}(t) \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}(t) & a_{n2}(t) & \cdots & a_{nn}(t) \end{pmatrix}.$$

Then

$$A'(t) = \begin{pmatrix} a'_{11}(t) & a'_{12}(t) & \cdots & a'_{1n}(t) \\ a'_{21}(t) & a'_{22}(t) & \cdots & a'_{2n}(t) \\ \cdots & \cdots & \cdots & \cdots \\ a'_{n1}(t) & a'_{n2}(t) & \cdots & a'_{nn}(t) \end{pmatrix}$$

and

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

where  $A_{ij}$  is the algebraic cofactor of  $a_{ij}(t)$ . Hence

$$\begin{aligned} \det A \cdot \text{trace}(A' A^{-1}) &= \sum_{j=1}^n a'_{1j}(t) A_{1j} + \sum_{j=1}^n a'_{2j}(t) A_{2j} + \cdots + \sum_{j=1}^n a'_{nj}(t) A_{nj} \\ &= \sum_i \sum_j a'_{ij}(t) A_{ij} = \sum_j \left( \sum_i a'_{ij}(t) A_{ij} \right). \end{aligned}$$