

**Solution.**

By re-ordering the elements  $v_1, v_2, \dots, v_n$ , we assume that

$$\sigma = (v_1 \cdots v_{i_1})(v_{i_1+1} \cdots v_{i_2}) \cdots (v_{i_{s+1}} \cdots v_n), \quad (1 \leq i_1 < i_2 < \cdots < i_s < n),$$

when  $\sigma$  is expressed as the product of disjoint cycles (This decomposition may have 1-cycles). Let  $W_j$  be the subspace of  $V$  generated by  $\{v_{i_{j-1}+1}, \dots, v_{i_j}\}$  for  $j = 1, 2, \dots, s+1$  ( $i_0 = 0, i_{s+1} = n$ ). Then the  $W_j$  are invariant subspaces of  $A$  and  $V = W_1 \oplus W_2 \oplus \cdots \oplus W_{s+1}$ . Let  $M_j$  be the matrix of  $A|_{W_j} : W_j \rightarrow W_j$  relative to the base  $\{v_{i_{j-1}+1}, \dots, v_{i_j}\}$  of  $W_j$  over  $\mathcal{C}$ . Then  $M = \text{diag}\{M_1, \dots, M_{s+1}\}$  is the matrix of  $A$  relative to the base  $\{v_1, v_2, \dots, v_n\}$ . So it suffices to prove that every  $M_j$  is diagonalizable.

Hence, without loss of generality, we may assume that  $\sigma$  is the  $n$ -cycle  $(v_1, v_2, \dots, v_n)$ . The matrix of  $A$  relative to the base  $\{v_1, v_2, \dots, v_n\}$  is

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

It is easy to see that the minimal polynomial of  $M$  is  $\lambda^n - 1$ , and thus  $M$  is diagonalizable.

This completes the proof that  $A$  is diagonalizable.

## 1107

Let  $V$  be a finite dimensional vector space over the field of rational numbers. Suppose  $T$  is a non-singular linear transformation of  $V$  such that  $T^{-1} = T^2 + T$ . Prove that 3 divides the dimension of  $V$ , and prove that if  $\dim V = 3$ , then all such  $T$ 's are similar.

(Harvard)

**Solution.**

Since  $T^{-1} = T^2 + T$ ,  $T$  is annihilated by the polynomial  $\lambda^3 + \lambda^2 - 1$ . Obviously,  $\lambda^3 + \lambda^2 - 1$  is irreducible over the field  $Q$  of rational numbers. Thus  $\lambda^3 + \lambda^2 - 1$  is the minimal polynomial  $m(\lambda)$  of  $T$ .

Now let  $n$  be the dimension of  $V$  over  $Q$ ,  $A$  be the matrix of  $T$  relative to some base of  $V$ ,  $\text{diag}\{\overbrace{1, \dots, 1}^{n-s}, d_1(\lambda), \dots, d_s(\lambda)\}$  be the normal form for  $\lambda I - A$

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