page 16 -

2. List of all possible monic polynomials of degree 2:

a) x^2 - splits to $x\,x$ - not irreducible

b) $x^2+1 = (x+1)^2 = x^2 + 2x + 1$ - not irreducible

c) $x^2+x = x(x+1)$ not irreducible

d) x^2+x+1. Irreducible. If $x^2+x+1 = (x+a)(x+b)$ it would be a polynomial of the form a, b, c - which is not true.

Two extension of $\mathbb{Z}_2$ are pol. $p(x) = a + bx$, $a, b \in \mathbb{Z}_2$ corresponding to $\mathbb{Z}_2^2 = (a,b)^T$. Product:

$$(a+xb)(c+xd) = ac + x(ad+bc) + bdx^2 =$$

$$(ac-bd) + (ad+bc-bd)x + bd(x^2+x+1) =$$

$$ac+bd, \quad ad+bc+bd,$$

$(-bd) = bd$ So $(a,c)^T(b,d)^T = (ac+bd,\ ad+bc+bd)$

3. Any finite extension of $\mathbb{Z}_p$ by an irreducible polynomial $q(x) = x^d + q_1x^{d-1} + \cdots + q_d$ is of the form $a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ where $a_i \in \mathbb{Z}_p$. So all possible polynomials of the form are isomorphic to $\mathbb{Z}_p^d$ which has $\underbrace{p \cdot p \cdots p}_{d} = p^d$ elements.

4. a. characteristic pol. of $A \in \mathbb{F}^{n\times n}$ is

$$\det(zI_n - A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (z\delta_{i\sigma(i)} - a_{i\sigma(i)})$$

where $[\delta_{ij}]_{i,j=1}^{n}$ are the entries of the identity matrix I_n.

in the product $(*)$ $(z\delta_{1\sigma(1)} - a_{1\sigma(1)}) \cdots (z\delta_{n\sigma(n)} - a_{n\sigma(n)})$ to get the ~~coefficient~~ term z^n we need to have that each factor contains z. So $\delta_{i\sigma(i)} = 1 \Rightarrow \sigma(i) = i$, $i = 1, \ldots, n$.

Hence z^n comes only from the factor

$$(z - a_{11})(z - a_{22}) \cdots (z - a_{nn}) = z^n \cdots \quad \text{monic.}$$

b. To get z^{n-k} in the term $(*)$ one has $n-k$ term with z

So σ fixes all elements in some subset $\beta \subset [n]$

$\sigma(j)>j$ for $j\in\beta$. let $\alpha=[n]/\beta$ so we need to take $\prod_{i\in\alpha}(-1)a_{i\sigma(i)}$. ~~When~~ Note that σ can be viewed as

$\sigma: \alpha\to\alpha$ (bijection) Hence

$$\sum sign(\sigma)\prod_{i\in\alpha}(-1)a_{i\sigma(i)} = (-1)^k\det(A[\alpha,\alpha])$$

σ identity on β

Now we need to take $\sum\det(A[\alpha,\alpha])$ on all α subsets of $[n]$ of cardinality k.

---

5. $A\underline{X}=\lambda\underline{X} \Rightarrow (\lambda I-A)\underline{X}=\underline{0}$ $\underline{X}\neq\underline{0}$. This is possible iff $\lambda I-A$ is singular $\det(\lambda I-A)=0$

---

6. $\begin{bmatrix}1&1\\1&0\end{bmatrix}$ $\det\begin{bmatrix}\lambda-1&-1\\-1&\lambda\end{bmatrix}=\lambda(\lambda-1)-1=\lambda^2-\lambda-1=$ $\lambda^2+\lambda+1$

since $-1=1$ in $\mathbb{Z}_2$. This is an irreducible pol. in $\mathbb{Z}_2$ see problem 2. So $\det(0-A)=1$ $\det(I-A)=1$ no eigenvalues in $\mathbb{Z}_2$.

---

7. $\mathbb{C}$ is an extension of $\mathbb{R}$ by considering $p(x)=x^2+1$ so any element in $\mathbb{C}$ is $a+b\underline{i}$ where $i^2=-1$.

$$z^p-1=(z-1)(z^{p-1}+z^{p-2}+\cdots+1)=(z-1)\,\varphi(z)$$

The roots of $z^{p-1}+\cdots+1=0$ are all complex numbers

$$e^{\frac{2\pi \underline{i} k}{p}}=\cos\frac{2\pi}{p}k+\left(\sin\frac{2\pi k}{p}\right)\underline{i}=\zeta^k,\quad k=1,\ldots,p-1$$

where $\zeta=\cos\frac{2\pi}{p}+\left(\sin\frac{2\pi}{p}\right)\underline{i}$

According Additional HW problem, $\det V(1,\zeta,\zeta^2,\ldots,\zeta^{p-1})$ is $\neq 0$.

So $1,\zeta,\ldots,\zeta^{p-1}$ are linearly independent over $\mathbb{Q}$.

If $\varphi(z)=\varphi_1\cdots\varphi_j$ where φ_i irreducible, and of course of degree ≥ 2 the extension $(\mathbb{Z}_p)\varphi_1$ will contain all the roots of z^p-1. ~~So since~~ Assume $\varphi_1(\zeta)=0$.

So $1,\zeta,\ldots,\zeta^{p-1}$ has more elements than $\deg\varphi_1$. Hence linearly dependent over $\mathbb{Q}$. Contradiction.

page 18

1. Choose a basis in $\underline{V}$. Then $\underline{x} = \sum_{i=1}^{n} x_i \underline{v}_i \rightarrow [x_1, \dots, x_n]^T$ $\quad = [\underline{v}_1, \dots, \underline{v}_n]$

2. $f \in V^*$, $x \in V$. Then $\varphi : V \to V^{**}$
$\varphi(x)(f) = f(x)$. This is isomorphism.

3. ~~Sta~~ $T[\underline{v}_1, \dots, \underline{v}_n] = [\underline{u}_1, \dots, \underline{u}_n]\underline{X}$, $X \in F^{n \times n}$
if X invertible $[\underline{u}_1, \dots, \underline{u}_n] = [\underline{v}_1, \dots, \underline{v}_n] X^{-1}$ isomorphis.
if T isomor $T^{-1}[\underline{u}_1, \dots, \underline{u}_n] = [\underline{v}_1, \dots, \underline{v}_n] Y$.
So $XY = YX = I_n \Rightarrow Y = X^{-1}$.

4. $\dim \underline{V} = \dim \underline{U}$.

5. $A \sim A \Rightarrow A = I_n^{-1} A I_n$
$A \sim B \Leftrightarrow B = Q^{-1} A Q \Rightarrow A = Q B Q^{-1} = (Q^{-1})^{-1} B Q^{-1} \Rightarrow B \sim A$.
$B \sim C \Rightarrow C = P^{-1} B P \Rightarrow C = P^{-1}(Q^{-1} A Q) P = (QP)^{-1} A (QP)$
$\Rightarrow A \sim C$.

6. $T \, [v_1, \dots, v_n] = [v_1, \dots, v_n] A$
$[v_1, \dots, v_n] = [u_1, \dots, u_n] X \Rightarrow T[\underline{u}_1, \dots, \underline{u}_n] = T[v_1 \dots v_n] X^{-1} =$
$[v_1, \dots, v_n] A X^{-1} = [u_1 \dots u_n] X A X^{-1}$
and vice versa. If $B = X A X^{-1}$ then take a new basis $[\underline{u}_1, \dots, \underline{u}_n] = [v_1, \dots, v_n] X^{-1}$.

---

7. a. $\det(\lambda I - B) = \det(\lambda I - Q^{-1} A Q) = \det[Q^{-1}(\lambda I - A) Q] =$
$= \det(Q^{-1}) \det(\lambda I - A) \det(Q) = (\det(Q))^{-1} \det(\lambda I - A) \det Q =$
$\det(\lambda I - B)$.

b. let $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
$\det(\lambda I - A) = \lambda^2$ $\quad \det(\lambda I - B) = \lambda^2$ $\quad Q^{-1} A Q = O \neq B$.
So A and B are not similar.

8. Thm. If $\lambda_1 \cdots \lambda_m$ are m distinct eigenvalues of $A \in \mathbb{F}^{n \times n}$ then the corresponding eigenvectors of A $\underline{x}_1, \cdots, \underline{x}_m$ are linearly independent. See page 198-199 in my Math 320 notes.

So if A has n distinct eigenvalues, let $X = [\underline{x}_1 \ \underline{x}_2 \cdots \underline{x}_n] \in GL(n, \mathbb{F})$ (invertible matrix).

let $\Delta = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$ diagonal matrix

Then $AX = X\Delta \iff X^{-1}AX = \Delta$.

Thus A is similar to a diagonal matrix with eigenvalues $\lambda_1 \cdots \lambda_n$.

Similarly B is similar to Δ. Hence $A \sim B$.