Title

D. Zack Garza

Friday 7th August, 2020

Contents

1 Spring 2019

1.1 1

> A is diagonalizable iff $\underset{A}{\min}(x)$ is separable. See further discussion here.

Claim: If $A \in \mathrm{GL}(m, \mathbb{F})$ is invertible and $A^n/\mathbb{F}$ is diagonalizable, then $A/\mathbb{F}$ is diagonalizable.

Let $A \in \mathrm{GL}(m, \mathbb{F})$. Since A^n is diagonalizable, $\min_{A^n}(x) \in \mathbb{F}[x]$ is separable and thus factors as a product of m **distinct** linear factors:

$$\min_{A^n}(x) = \prod_{i=1}^{m} (x - \lambda_i), \quad \min_{A^n}(A^n) = 0$$

where $\{\lambda_i\}_{i=1}^m \subset \mathbb{F}$ are the **distinct** eigenvalues of A^n.

Moreover $A \in \mathrm{GL}(m, \mathbb{F}) \implies A^n \in \mathrm{GL}(m, \mathbb{F})$: A is invertible $\iff \det(A) = d \in \mathbb{F}^\times$, and so $\det(A^n) = \det(A)^n = d^n \in \mathbb{F}^\times$ using the fact that the determinant is a ring morphism $\det : \mathrm{Mat}(m \times m) \longrightarrow \mathbb{F}$ and $\mathbb{F}^\times$ is closed under multiplication.

So A^n is invertible, and thus has trivial kernel, and thus zero is not an eigenvalue, so $\lambda_i \neq 0$ for any i.

Since the λ_i are distinct and nonzero, this implies x^k is not a factor of $\mu_{A^n}(x)$ for any $k \geq 0$. Thus the m terms in the product correspond to precisely m **distinct linear** factors.

We can now construct a polynomial that annihilates A, namely

$$q_A(x) \coloneqq \min_{A^n}(x^n) = \prod_{i=1}^{m} (x^n - \lambda_i) \in \mathbb{F}[x],$$

where we can note that $q_A(A) = \min_{A^n}(A^n) = 0$, and so $\min_{A}(x) \mid q_A(x)$ by minimality.

We now claim that $q_A(x)$ has exactly $n \cdot m$ distinct linear factors in $\overline{\mathbb{F}}[x]$, which reduces to showing that no pair $x^n - \lambda_i, x^n - \lambda_j$ share a root. and that $x^n - \lambda_i$ does not have multiple roots.

- For the first claim, we can factor

$$x^n - \lambda_i = \prod_{k=1}^{n} (x - \lambda_i^{\frac{1}{n}} e^{\frac{2\pi i k}{n}}) \coloneqq \prod_{k=1}^{n} (x - \lambda^{\frac{1}{n}} \zeta_n^k),$$

  where we now use the fact that $i \neq j \implies \lambda_i^{\frac{1}{n}} \neq \lambda_j^{\frac{1}{n}}$. Thus no term in the above product appears as a factor in $x^n - \lambda_j$ for $j \neq i$.

- For the second claim, we can check that $\frac{\partial}{\partial x}(x^n - \lambda_i) = n x^{n-1} \neq 0 \in \mathbb{F}$, and $\gcd(x^n - \lambda_i, n x^{n-1}) = 1$ since the latter term has only the roots $x = 0$ with multiplicity $n - 1$, whereas $\lambda_i \neq 0 \implies$ zero is not a root of $x^n - \lambda_i$.

But now since $q_A(x)$ has exactly distinct linear factors in $\overline{\mathbb{F}}[x]$ and $\min_{A}(x) \mid q_A(x)$, $\min_{A}(x) \in \mathbb{F}[x]$ can only have distinct linear factors, and A is thus diagonalizable over $\mathbb{F}$.

■

1.2 2

1.2.1 (a)

Go to a field extension. Orders of multiplicative groups for finite fields are known.

We can consider the quotient $K = \dfrac{\mathbb{F}_p[x]}{\langle \pi(x) \rangle}$, which since $\pi(x)$ is irreducible is an extension of $\mathbb{F}_p$ of degree d and thus a field of size p^d with a natural quotient map of rings $\rho : \mathbb{F}_p[x] \longrightarrow K$.

Since $K^\times$ is a group of size $p^d - 1$, we know that for any $y \in K^\times$, we have by Lagrange's theorem that the order of y divides $p^d - 1$ and so $y^{p^d} = y$.

So every element in K is a root of $q(x) = x^{p^d} - x$.

Since ρ is a ring morphism, we have

$$\begin{aligned}
\rho(q(x)) = \rho(x^{p^d} - x) = \rho(x)^{p^d} - \rho(x) = 0 \in K \\
&\iff q(x) \in \ker \rho \\
&\iff q(x) \in \langle \pi(x) \rangle \\
&\iff \pi(x) \,\Big|\, q(x) = x^{p^d} - x \quad \text{"to contain is to divide".}
\end{aligned}$$

■

1.2.2 (b)

Some potentially useful facts:

- $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.
- $x^{p^d} - x \,\Big|\, x^{p^n} - x \iff d \,\Big|\, n$
- $\mathbb{GF}(p^d) \leq \mathbb{GF}(p^n) \iff d \,\Big|\, n$
- $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n.

Claim: $\pi(x)$ divides $x^{p^n} - x \iff \deg \pi$ divides n.

$\implies$: Let $L \cong \mathbb{GF}(p^n)$ be the splitting field of $\varphi_n(x) \coloneqq x^{p^n} - x$; then since $\pi \,\Big|\, \varphi_n$ by assumption, π splits in L. Let $\alpha \in L$ be any root of π; then there is a tower of extensions $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$.

Then $\mathbb{F}_p \leq \mathbb{F}_p(\alpha) \leq L$, and so

$$\begin{aligned}
n &= [L : \mathbb{F}_p] \\
&= [L : \mathbb{F}_p(\alpha)] \; [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\
&= \ell d,
\end{aligned}$$

for some $\ell \in \mathbb{Z}^{\geq 1}$, so d divides n.

$\impliedby$: If $d \,\Big|\, n$, use the fact (claim) that $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic f_i of degree d dividing n. So $f = f_i$ for some i.

$\blacksquare$

1.3 3

- Sylow theorems:
- $n_p \cong 1 \mod p$
- $n_p \mid m$.

It turns out that $n_3 = 1$ and $n_5 = 1$, so $G \cong S_3 \times S_5$ since both subgroups are normal.

There is only one possibility for S_5, namely $S_5 \cong \mathbb{Z}/(5)$.

There are two possibilities for S_3, namely $S_3 \cong \mathbb{Z}/(3^2)$ and $\mathbb{Z}/(3)^2$.

Thus

- $G \cong \mathbb{Z}/(9) \times \mathbb{Z}/(5)$, or
- $G \cong \mathbb{Z}/(3)^2 \times \mathbb{Z}/(5)$.

$\blacksquare$

1.4 4

Concepts Used:

- Notation: X/G is the set of G-orbits
- Notation: $X^g = \left\{x \in x \mid g \cdot x = x\right\}$
- Burnside's formula: $|G||X/G| = \sum |X^g|$.

1.4.1 a

Strategy: Burnside.

- Define a sample space $\Omega = G \times G$, so $|\Omega| = |G|^2$.
- Identify the event we want to analyze: $A \coloneqq \left\{(g,h) \in G \times G \mid [g,h] = 1\right\}$.
  - Define and note:

$$A_g \coloneqq \left\{(g,h) \mid h \in H, [g,h] = 1\right\} \implies A = \coprod_{g \in G} A_g.$$

- Set n be the number of conjugacy classes, note we want to show $P(A) = n/|G|$.
- Let G act on itself by conjugation, which partitions G into conjugacy classes.
  - What are the orbits?

$$\mathcal{O}_g = \left\{hgh^{-1} \mid h \in G\right\},$$

    which is the conjugacy class of g.

- What are the fixed points?

$$X^g = \left\{ h \in G \,\middle|\, hgh^{-1} = g \right\},$$

which are the elements of G that commute with g, which is precisely A_g.

- Note $|X/G| = n$, the number of conjugacy classes.
- Note that

$$|A| = \left| \coprod_{g \in G} A_g \right| = \sum_{g \in G} |A_g| = \sum_{g \in G} |X^g|.$$

- Apply Burnside

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

- Rearrange and use definition:

$$n|G| = |X/G||G| = \sum_{g \in G} |X^g|$$

- Compute probability:

$$P(A) = \frac{|A|}{|\Omega|} = \frac{\sum_{g \in G} |X^g|}{|G|^2} = \frac{|X/G||G|}{|G|^2} = \frac{n|G|}{|G|^2} = \frac{n}{|G|}.$$

■

1.4.2 b

Class equation:

$$|G| = Z(G) + \sum_{\substack{\text{One } x \text{ from each} \\ \text{conjugacy class}}} [G : Z(x)]$$

where $Z(x) = \left\{ g \in G \,\middle|\, [g, x] = 1 \right\}$.

1.4.3 c

Todo: revisit.

As shown in part 1,

$$\mathcal{O}_x = \left\{ g \curvearrowright x \,\middle|\, g \in G \right\} = \left\{ h \in G \,\middle|\, ghg^{-1} = h \right\} = C_G(g),$$

and by the class equation

$$|G| = |Z(G)| + \sum_{\substack{\text{One } x \text{ from each} \\ \text{conjugacy class}}} [G : Z(x)]$$

Now note

- Each element of $Z(G)$ is in its own conjugacy class, contributing $|Z(G)|$ classes to n.
- Every other class of elements in $G \setminus Z(G)$ contains at least 2 elements
  - Claim: each such class contributes **at least** $\frac{1}{2}|G \setminus Z(G)|$.

Thus

$$\begin{aligned} n &\leq |Z(G)| + \frac{1}{2}|G \setminus Z(G)| \\ &= |Z(G)| + \frac{1}{2}|G| - \frac{1}{2}|Z(G)| \\ &= \frac{1}{2}|G| + \frac{1}{2}|Z(G)| \end{aligned}$$

$$\begin{aligned} \implies \frac{n}{|G|} &\leq \frac{1}{2}\frac{|G|}{|G|} + \frac{1}{2}\frac{|Z(G)|}{|G|} \\ &= \frac{1}{2} + \frac{1}{2}\frac{1}{[G : Z(G)]}. \end{aligned}$$

1.5 5

1.5.1 a

- Suppose toward a contradiction $\mathrm{Tor}(M)$ has rank $n \geq 1$.
- Then $\mathrm{Tor}(M)$ has a linearly independent generating set $B = \{\mathbf{r}_1, \cdots, \mathbf{r}_n\}$, so in particular

$$\sum_{i=1}^{n} s_i \mathbf{r}_i = 0 \implies s_i = 0_R \,\forall i.$$

- Let $\mathbf{r}$ be any of of these generating elements.
- Since $\mathbf{r} \in \mathrm{Tor}(M)$, there exists an $s \in R \setminus 0_R$ such that $s\mathbf{r} = 0_M$.
- Then $s\mathbf{r} = 0$ with $s \neq 0$, so $\{\mathbf{r}\} \subseteq B$ is *not* a linearly independent set, a contradiction.

■

1.5.2 b

- Let $n = \operatorname{rank} M$, and let $\mathcal{B} = \{\mathbf{r}_i\}_{i=1}^{n} \subseteq R$ be a generating set.
- Let $\tilde{M} \coloneqq M/\mathrm{Tor}(M)$ and $\pi : M \longrightarrow M'$ be the canonical quotient map.
- **Claim:** $\tilde{\mathcal{B}} \coloneqq \pi(\mathcal{B}) = \{\mathbf{r}_i + \mathrm{Tor}(M)\}$ is a basis for $\tilde{M}$.
  - **Linearly Independent:**

* Suppose that

$$\sum_{i=1}^{n} s_i(\mathbf{r}_i + \operatorname{Tor}(M)) = \mathbf{0}_{\tilde{M}}.$$

* Then using the definition of coset addition/multiplication, we can write this as

$$\sum_{i=1}^{n} (s_i\mathbf{r}_i + \operatorname{Tor}(M)) = \left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) + \operatorname{Tor}(M) = 0_{\tilde{M}}.$$

* Since $\tilde{\mathbf{x}} = 0 \in \tilde{M} \iff \tilde{\mathbf{x}} = \mathbf{x} + \operatorname{Tor}(M)$ where $\mathbf{x} \in \operatorname{Tor}(M)$, this forces $\sum s_i\mathbf{r}_i \in \operatorname{Tor}(M)$.
* Then there exists a scalar $\alpha \in R^\bullet$ such that $\alpha \sum s_i\mathbf{r}_i = 0_M$.
* But since R is an integral domain and $\alpha \neq 0$, we must have $s_i = 0$ for all i.

– **Spanning:**

* Write $\pi(\mathcal{B}) = \{\mathbf{r}_i + \operatorname{Tor}(M)\}_{i=1}^{n}$ as a set of cosets.
* Letting $\mathbf{x} \in M'$ be arbitrary, we can write $\mathbf{x} = \mathbf{m} + \operatorname{Tor}(M)$ for some $\mathbf{m} \in M$ where $\pi(\mathbf{m}) = \mathbf{x}$ by surjectivity of π.
* Since $\mathcal{B}$ is a basis for M, we have $\mathbf{m} = \sum_{i=1}^{n} s_i\mathbf{r}_i$, and so

$$\begin{aligned}
\mathbf{x} &= \pi(\mathbf{m}) \\
&= \pi\left(\sum_{i=1}^{n} s_i\mathbf{r}_i\right) \\
&= \sum_{i=1}^{n} s_i\pi(\mathbf{r}_i) \\
&= \sum_{i=1}^{n} s_i(\mathbf{r}_i + \operatorname{Tor}(M)),
\end{aligned}$$

which expresses $\mathbf{x}$ as a linear combination of elements in $\mathcal{B}'$.

1.5.3 c

M **is not free: Claim**: If $I \trianglelefteq R$ is a free R-module, then I is a principal ideal.

Proof: Let $I = \langle B \rangle$ for some basis – if B contains more than 1 element, say m_1 and m_2, then $m_2m_1 - m_1m_2 = 0$ is a linear dependence, so B has only one element m.

But then $I = \langle m \rangle = R_m$ is cyclic as an R- module and thus principal as an ideal of R. The result follows by the contrapositive.

M **is rank 1**: For any module, we can take an element $M \neq 0_M$ and consider its cyclic module Rm.

Thus the rank of M is at least 1, since $\{m\}$ is a subset of a spanning set. It can not be linearly dependent, since R is an integral domain and $M \subseteq R$, so $\alpha m = 0 \implies \alpha = 0$.

However, the rank is at most 1 since R is commutative. If we take two elements $\mathbf{m}, \mathbf{n} \in M$, then since $m, n \in R$ as well, we have $nm = mn$ and so

$$(n)\mathbf{m} + (-m)\mathbf{n} = 0_R = 0_M$$

is a linear dependence. 2 M **is torsion-free**:

Let $x \in \mathrm{Tor} M$, then there exists some $r \neq 0 \in R$ such that $rx = 0$. But $x \in R$ and R is an integral domain, so $x = 0$, and thus $\mathrm{Tor}(M) = \{0_R\}$.

■

1.6 6

1.6.1 a

Define the set of proper ideals

$$S = \left\{ J \;\middle|\; I \subseteq J < R \right\},$$

which is a poset under set inclusion.

Given a chain $J_1 \subseteq \cdots$, there is an upper bound $J \coloneqq \bigcup J_i$, so Zorn's lemma applies.

1.6.2 b

$\implies$:

We will show that $x \in J(R) \implies 1 + x \in R^\times$, from which the result follows by letting $x = rx$.

Let $x \in J(R)$, so it is in every maximal ideal, and suppose toward a contradiction that $1 + x$ is **not** a unit.

Then consider $I = \langle 1 + x \rangle \trianglelefteq R$. Since $1 + x$ is not a unit, we can't write $s(1 + x) = 1$ for any $s \in R$, and so $1 \notin I$ and $I \neq R$

So $I < R$ is proper and thus contained in some maximal proper ideal $\mathfrak{m} < R$ by part (1), and so we have $1 + x \in \mathfrak{m}$. Since $x \in J(R)$, $x \in \mathfrak{m}$ as well.

But then $(1 + x) - x = 1 \in \mathfrak{m}$ which forces $\mathfrak{m} = R$.

$\impliedby$

Fix $x \in R$, and suppose $1 + rx$ is a unit for all $r \in R$.

Suppose towards a contradiction that there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$ and thus $x \notin J(R)$.

Consider

$$M' \coloneqq \left\{ rx + m \;\middle|\; r \in R,\ m \in M \right\}.$$

Since $\mathfrak{m}$ was maximal, $\mathfrak{m} \subsetneq M'$ and so $M' = R$.

So every element in R can be written as $rx + m$ for some $r \in R, m \in M$. But $1 \in R$, so we have

$$1 = rx + m.$$

So let $s = -r$ and write $1 = sx - m$, and so $m = 1 + sx$.

Since $s \in R$ by assumption $1 + sx$ is a unit and thus $m \in \mathfrak{m}$ is a unit, a contradiction.

So $x \in \mathfrak{m}$ for every $\mathfrak{m}$ and thus $x \in J(R)$.

1.6.3 c

- $\mathfrak{N}(R) = \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$.
- $J(R) = \text{Spec}_{\text{max}}(R) = \displaystyle\bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$.

We want to show $J(R) = \mathfrak{N}(R)$.

$\mathfrak{N}(R) \subseteq J(R)$:

We'll use the fact $x \in \mathfrak{N}(R) \implies x^n = 0 \implies 1 + rx$ is a unit $\iff x \in J(R)$ by (b):

$$\sum_{k=1}^{n-1} (-x)^k = \frac{1 - (-x)^n}{1 - (-x)} = (1 + x)^{-1}.$$

$J(R) \subseteq \mathfrak{N}(R)$:

Let $x \in J(R) \setminus \mathfrak{N}(R)$.

Since R is finite, $x^m = x$ for some $m > 0$. Without loss of generality, we can suppose $x^2 = x$ by replacing x^m with x^{2m}.

If $1 - x$ is not a unit, then $\langle 1 - x \rangle$ is a nontrivial proper ideal, which by (a) is contained in some maximal ideal $\mathfrak{m}$. But then $x \in \mathfrak{m}$ and $1 - x \in \mathfrak{m} \implies x + (1 - x) = 1 \in \mathfrak{m}$, a contradiction.

So $1 - x$ is a unit, so let $u = (1 - x)^{-1}$.

Then

$$\begin{aligned}
(1 - x)x = x - x^2 = x - x = 0 \\
&\implies u(1 - x)x = x = 0 \\
&\implies x = 0.
\end{aligned}$$

1.7 7

Work with matrix of all ones instead. Eyeball eigenvectors. Coefficients in minimal polynomial: size of largest Jordan block Dimension of eigenspace: number of Jordan blocks

1.7.1 a

Let A be the matrix in the question, and B be the matrix containing 1's in every entry.

- Noting that $B = A + I$, we have

$$\begin{aligned} &B\mathbf{x} = \lambda\mathbf{x} \\ \iff &(A+I)\mathbf{x} = \lambda\mathbf{x} \\ \iff &A\mathbf{x} = (\lambda - 1)\mathbf{x}, \end{aligned}$$

  so we will find the eigenvalues of B and subtract one from each.

- Note that $B\mathbf{v} = \left[\sum v_i, \sum v_i, \cdots, \sum v_i\right]$, i.e. it has the effect of summing all of the entries of $\mathbf{v}$ and placing that sum in each component.

- We proceed by finding p eigenvectors and eigenvalues, since the JCF and minimal polynomials will involve eigenvalues and the transformation matrix will involve (generalized) eigenvectors.

- Claim: each vector of the form $\mathbf{p}_i \coloneqq \mathbf{e}_1 - \mathbf{e}_{i+1} = [1, 0, 0, \cdots, 0 - 1, 0, \cdots, 0]$ where $i \neq j$ is also an eigenvector with eigenvalues $\lambda_0 = 0$, and this gives $p - 1$ linearly independent vectors spanning the eigenspace E_{λ_0}

  - Compute

$$B\mathbf{p}_i = [1 + 0 + \cdots + 0 + (-1) + 0 + \cdots + 0] = [0, 0, \cdots, 0]$$

  - So every $\mathbf{p}_i \in \ker(B)$, so they are eigenvectors with eigenvalue 0.
  - Since the first component is fixed and we have $p - 1$ choices for where to place a -1, this yields $p - 1$ possibilities for $\mathbf{p}_i$
  - These are linearly independent since the $(p-1) \times (p-1)$ matrix $\left[\mathbf{p}_1^t, \cdots, \mathbf{p}_{p-1}^t\right]$ satisfies

$$\det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} = (1) \cdot \det \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix} = (-1)^{p-2} \neq 0.$$

  where the first equality follows from expanding along the first row and noting this is the first minor, and every other minor contains a row of zeros.

- Claim: $\mathbf{v}_1 = [1, 1, \cdots, 1]$ is an eigenvector with eigenvalue $\lambda_1 = p$.

  - Compute

$$B\mathbf{v} = \left[\sum_{i=1}^{p} 1, \sum_{i=1}^{p} 1, \cdots, \sum_{i=1}^{p} 1\right] = [p, p, \cdots, p] = p[1, 1, \cdots, 1] = p\mathbf{v}_1,$$

    thus $\lambda_1 = p$
  - $\dim E_{\lambda_1} = 1$ since the eigenspaces are orthogonal and $E_{\lambda_0} \oplus E_{\lambda_1} \leq F^p$ is a subspace, so $p > \dim(E_{\lambda_0}) + \dim E_{\lambda_1} = p - 1 + \dim E_{\lambda_1}$ and it isn't zero dimensional.

- Using that the eigenvalues of A are $1+\lambda_i$ for λ_i the above eigenvalues for B,

$$\begin{aligned} \text{Spec }(B) &:= \{(\lambda_i, m_i)\} = \{(p,1),(0,p-1)\} \implies \chi_B(x) = (x-p)x^{p-1} \\ &\implies \text{Spec }(A) = \{(p-1,1),(-1,p-1)\} \implies \chi_A(x) = (x-p+1)(x+1)^{p-1} \end{aligned}$$

Note: we can always read off the *characteristic* polynomial from the spectrum.

- The dimensions of eigenspaces are preserved, thus

$$JCF_{\mathbb{Q}}(A) = J_{p-1}^1 \oplus (p-1)J_{-1}^1 = \left[\begin{array}{c|c|c|c|c|c} p-1 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

- The matrix P such that $A = PJP^{-1}$ will have columns the bases of the generalized eigenspaces.
- In this case, the generalized eigenspaces are the usual eigenspaces, so

$$P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

1.7.2 b

For $F = \mathbb{F}_p$, all eigenvalues/vectors still lie in $\mathbb{F}_p$, but now $-1 = p-1$, making $(x-(p-1))(x+1)^{p-1} = (x+1)(x+1)^{p-1}$, so $\chi_{A,\mathbb{F}_p}(x) = (x+1)^p$, and the Jordan blocks may merge.

- A computation shows that $(A+I)^2 = pA = 0 \in M_p(\mathbb{F}_p)$ and $(A+I) \neq 0$, so $\min_{A,\mathbb{F}_p}(x) = (x+1)^2$.
  - Thus the largest Jordan block corresponding to $\lambda = -1$ is of size 2
- Can check that $\det(A) = \pm 1 \in \mathbb{F}_p^\times$, so the vectors $\mathbf{e}_1 - \mathbf{e}_i$ are still linearly independent and thus $\dim E_{-1} = p-1$
  - So there are $p-1$ Jordan blocks for $\lambda = 0$.

Summary:

$$\begin{aligned} &\min_{A,\mathbb{F}_p}(x) = (x+1)^2 \\ &\chi_{A,\mathbb{F}_p}(x) \equiv (x+1)^p \\ &\dim E_{-1} = p-1. \end{aligned}$$

Thus

$$JCF_{\mathbb{F}_p}(A) = J_{-1}^2 \oplus (p-2)J_{-1}^1 = \left[\begin{array}{cc|c|c|c|c} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \ddots & \ddots & 0 \\ \hline 0 & 0 & 0 & \cdots & -1 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 \end{array}\right].$$

To obtain a basis for $E_{\lambda=0}$, first note that the matrix $P = [\mathbf{v}_1, \mathbf{p}_1, \cdots, \mathbf{p}_{p-1}]$ from part (a) is singular over $\mathbb{F}_p$, since

$$\begin{aligned} \mathbf{v}_1 + \mathbf{p}_1 + \mathbf{p}_2 + \cdots + \mathbf{p}_{p-2} &= [p-1, 0, 0, \cdots, 0, 1] \\ &= [-1, 0, 0, \cdots, 0, 1] \\ &= -\mathbf{p}_{p-1}. \end{aligned}$$

We still have a linearly independent set given by the first $p-1$ columns of P, so we can extend this to a basis by finding one linearly independent generalized eigenvector.

Solving $(A - I\lambda)\mathbf{x} = \mathbf{v}_1$ is our only option (the others won't yield solutions). This amounts to solving $B\mathbf{x} = \mathbf{v}_1$, which imposes the condition $\sum x_i = 1$, so we can choose $\mathbf{x} = [1, 0, \cdots, 0]$.

Thus

$$P = [\mathbf{v}_1, \mathbf{x}, \mathbf{p}_1, \cdots, \mathbf{p}_{p-2}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

1.8 8

Concepts used:

- $\zeta_n := e^{\frac{2\pi i}{n}}$, and ζ_n^k is a primitive nth root of unity $\iff \gcd(n,k) = 1$
  - In general, ζ_n^k is a primitive $\dfrac{n}{\gcd(n,k)}$th root of unity.
- $\deg \Phi_n(x) = \varphi(n)$
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ (proof: for a nontrivial gcd, the possibilities are $p, 2p, 3p, 4p, \cdots, p^{k-2}p, p^{k-1}p$.)
- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$

Let $K = \mathbb{Q}(\zeta)$

1.8.1 a

- $\zeta := e^{2\pi i/8}$ is a primitive 8th root of unity
- The minimal polynomial of an nth root of unity is the nth cyclotomic polynomial Φ_n

- The degree of the field extension is the degree of Φ_8, which is

$$\varphi(8) = \varphi(2^3) = 2^{3-1} \cdot (2-1) = 4.$$

- So $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

1.8.2 b

- $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}/(8)^\times \cong \mathbb{Z}/(4)$ by general theory
- $\mathbb{Z}/(4)$ has exactly one subgroup of index 2.
- Thus there is exactly **one** intermediate field of degree 2 (a quadratic extension).

1.8.3 c

- Let $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$.
- Note $\mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2})$
  - $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta)$
    - $\zeta_8^2 = i$, and $\zeta_8 = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$ so $\zeta_8 + \zeta_8^{-1} = 2/\sqrt{2} = \sqrt{2}$.
  - $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(i, \sqrt{2})$:
    - $\zeta = e^{2\pi i/8} = \sin(\pi/4) + i\cos(\pi/4) = \dfrac{\sqrt{2}}{2}(1+i)$.
- Thus $L = \mathbb{Q}(i, \sqrt{2})(\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$.
  - Uses the fact that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ since $\sqrt[4]{2}^2 = \sqrt{2}$
- Conclude

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})]\ [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$$

  using the fact that the minimal polynomial of i over any subfield of $\mathbb{R}$ is always x^2+1, so $\min_{\mathbb{Q}(\sqrt[4]{2})}(i) = x^2 + 1$ which is degree 2.