January 2020, Q1

a.) Find all possible JCFs of a 4 x 4 matrix whose minimal polynomial consists of two (possibly repeated) invariant factors.

The characteristic polynomial is equal to the product of the invariant factors; the minimal polynomial is the largest invariant factor; and each invariant factor divides the minimal polynomial. This implies that the only possibilities are

(i.) m(x) = (x - a)(x - b)
(ii.) m(x) = (x - a)^2 (x - b)
(iii.) m(x) = (x - a)(x - b)^2 or
(iv.) m(x) = (x - a)^2 (x - b)^2.

$$\chi(x) = (x-a)^3(x-b),\quad (x-a)^2(x-b)^2,\quad (x-a)(x-b)^3$$

The invariant factors are all products of the linear polynomials x - a and x - b, so the elementary divisors must be some number of x - a and some number of x - b. So, the Jordan Canonical Form is a diagonal matrix with some number of a and b on the diagonal.

January 2020, Q3

Prove that the rank of an n x m nonzero matrix is equal to the largest positive integer t such that there exists a t x t submatrix of A whose determinant is nonzero.

(Aaron) Proceed by induction on n. In the inductive step, use elementary row and column operations to obtain a pivot in the first row and column; then, use the inductive hypothesis.

August 2018, Q4

Find the number of 2 x 2 matrices A over Z/pZ such that A^2 = I.

$\mu_A(x) \mid (x^2-1)$ = (x - 1)(x + 1) (if p is odd), hence A is diagonalizable with eigenvalues 1 or -1, hence A is similar to I, -I, or diag{1, -1}. But any matrix that is similar to I or -I must be itself be I or -I, so we need only consider the case that A is similar to $\underbrace{\text{diag}\{1, -1\}}_{D}$.

A is similar to D if and only if A is conjugate to D if and only if A belongs to the orbit of D with respect to conjugacy.

$$|\mathcal{O}(D)| = |GL(2,\mathbb{Z}_p)| / |Stab(D)| = (p^2-1)(p^2-p) / |Stab(D)|$$

Stab(D) = {P | PDP^{-1} = D} = {P | PD = DP} = {P | P commutes with D}

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}$$

These are equal if and only if b = 0 and c = 0.

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$$

Stab(D) = {diag{a, d} | a, d are nonzero and belong to Z/pZ}
|Stab(D)| = (p - 1)(p - 1) = (p - 1)^2

|O(D)| = (p^2 - 1)(p^2 - p)/(p - 1)^2 = p(p + 1) $+1$ $+1$

$\underline{p=2}$: $\mu_A(x) \mid (x-1)^2$

$\mu_A(x) = x-1$ or $\mu_A(x) = (x-1)^2$

$+1$

$A \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = J$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

These are equal if and only if c = 0 and a = d.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

$$= \left\{ \begin{pmatrix} a & a+b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_2 \setminus \{0\} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$|\mathcal{O}(J)| = (2^2-1)(2^2-2)/2 = 3+1$$

January 2017, Q1(iii.)

Find a prime number p, an integer n, and a non-abelian group of order p^n whose center contains more than one normal subgroup of order p.

Observation: n must be at least 4. Indeed, if n = 3, then by Lagrange's Theorem, |Z(G)| is either 1, p, or p^2. If |Z(G)| = 1 or p, then G contains at most one normal subgroup of order p.

If $|Z(G)| = p^2$, then $|G/Z(G)| = p$, hence $G/Z(G)$ is cyclic so that G is abelian — a contradiction.

Let's construct a non-abelian group of order 2^4 whose center contains more than one normal subgroup of order 2. (By what we just said, this is the smallest possible order of such a group.)

Ex.: $\mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_4 = (\mathbb{Z}_4 \times \mathbb{Z}_4, \cdot)$

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 + \varphi(h_1)(g_2), h_1 + h_2)$$

$$\varphi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_4)$$

Fact: Aut(Z/nZ) are precisely multiplication by an integer k such that gcd(n, k) = 1.

In particular, we have that Aut(Z/4Z) = {1, 3}.

$$1 \swarrow \; id \qquad 3 \searrow \; \sigma(a) = 3a$$

Fact (Proposition 21 from my note "Permutation Groups and the Semidirect Product"):
For any semidirect product G \rtimes_f H, we have that

[Z(G) \cap Fix(f(H))] \times [Z(H) \cap ker(f)] \subseteq Z(G \rtimes H),

where f is a group homomorphism f : H \to Aut(G).

$G = \mathbb{Z}_4$

$H = \mathbb{Z}_4$

$$Z(\mathbb{Z}_4) = \mathbb{Z}_4 = Z(\mathbb{Z}_4)$$

$$\varphi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_4)$$
$$k \mapsto \sigma^k$$

$$Fix(\varphi(\mathbb{Z}_4)) = Fix(Aut(\mathbb{Z}_4)) = \{0,2\}$$

$$\ker \varphi = \{0,2\}$$

$$\{0,2\} \times \{0,2\} \subseteq \mathbb{Z}_4 \rtimes_\varphi \mathbb{Z}_4 = D$$

$\{(0,0),(0,2)\} \trianglelefteq D$, $\{(0,0),(2,2)\} \trianglelefteq D$