January 1998
Algebra Qualifying Exams
Solutions

1A) Let F be a field, let A be an $n \times n$ matrix over F, and let $w \in F^m$ be a column vector. Show that exactly one of the following holds:

(i) $Av = w$ for some $v \in F^n$.

(ii) There is a u in F^m such that $u^T A = 0$ and $u^T w = 1$ (where u^T is the row vector obtained by transposing u).

Answer: Suppose (i) is true. Then $Av = w \implies u^T (Av) = u^T w \implies \left(u^T A\right) v = u^T w$ but this is a contradiction as $\left(u^T A\right) = 0$ and $0v = 0$ but $u^T w = 1$.

Suppose (ii) is true. If (i) is true then (ii) is false so this contradiction forces (i) to be false.

Lastly, suppose both are false. $Av = w$ is solvable if and only if $w^T u = 0$ whenever $A^T u = 0$ so one of them must be true.

1B) Let A be the matrix $\begin{pmatrix} 4 & 5 & 3 \\ -5 & -10 & -10 \\ 3 & 6 & 6 \end{pmatrix}$. Compute its characteristic polynomial, minimal polynomial, Jordan canonical form, and rational canonical form.

Answer: The characteristic polynomial is $\det(A - xI) = -x^3$. The minimal polynomial must divide the characteristic by the Cayley-Hamilton theorem and thus can be either x, x^2, or x^3. It is clearly not x. $A^2 \neq 0$ and so is not x^2. Thus the minimal polynomial is x^3. In this case the RCF and JCF are the same and we have

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

2A) Let G be a group that acts on a 10-element set S. Suppose that $g \in G$ has order 35. Show that for some positive natural number $n < 35$, the element g^n fixes all points of S.

Answer: Let $\sigma \in S_{10}$ such that $|\sigma| = m$. σ can be written as a product of disjoint cycles with $\sigma = \rho_1 \cdots \rho_m$, with $|\sigma| = \text{lcm}(|\rho_1|, ..., |\rho_m|)$ with the max $\sigma = 2 \cdot 3 \cdot 5 = 30$. Notice that there does not exist $\sigma \in S_{10}$ such that $\sigma = 35 = 5 \cdot 7$ as $5 + 7 = 12$. Let $\sigma : G \to S_{10}$ by $\varphi(g) = \varphi g$. Show there is an $n \in \mathbb{N}$ with $n < 35$ such that $\varphi(g^n) = id$.

$\varphi(g^n)(x) = \varphi g^n(x) = (\sigma g(x))^n = x$ for all $x \in S$. Note that the order of the image is $1, 5, 7$, or 35 but cannot be 35 as we already explained.

2B) Let p and q be primes with $p < q$. Show that if there is a non-abelian group of order pq, then $q \equiv 1 \bmod p$.

Answer: Proof by contrapositive. Assume that $q \neq 1 \bmod p$ and show that G with $|G| = pq$ is abelian. By Sylow theorems we know that the number of p-Sylow subgroups $n_p \equiv 1 \bmod p$ and so there are $1 + np$ of them for some $n \in \mathbb{N}$. But as p and q are prime and $q \neq 1 \bmod p$, there must be a unique p-Sylow subgroup as $1 + np | pq$. So call this subgroup P. Also there is a unique Sylow q-Subgroup by the same argument. Call this subgroup Q. As both have prime order we know they are cyclic. So say $P = (x)$ and $Q = (y)$. We also know from a corollary to Sylow's theorems that a Sylow subgroup is unique iff it is normal as all Sylow subgroups are conjugate. We know that $P \cap Q = 1$ and that $x^{-1} y^{-1} x y \in P \cap Q$ as both are normal and so $xy = yx$. Also $|PQ| = |P| |Q| / |P \cap Q| = pq/1 = pq$. So $G = PQ = (xy)$ and thus G is a cyclic group and thus Abelian.

3A) Let R be a PID. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an increasing sequence of ideals in R. Prove that the sequence is eventually constant, i.e. for some n, $I_n = I_{n+1} = I_{n+2} = \cdots$.

Answer: Consider the ideal $J = \cup_k I_k$. As R is a PID we know that $J = (x)$ for some $x \in R$. And thus as $x \in I_m$ for some m we know that for all $n > m$ we have that $I_n = I_m$.

3B) Determine whether or not the rings $\mathbb{Q}[x] / (p) \oplus \mathbb{Q}[x] / (q)$ and $\mathbb{Q}[x] / (pq)$ are isomorphic where $p = x^4 + 4$ and $q = x^4 + 2^3 - 4x - 4$.

Answer: We note that $x^4 + 4 = \left(x^2 + 2x + 2\right)\left(x^2 - 2x + 2\right)$. Each of these factors is irreducible as they have non rational roots. Now note that $\left(x^2 + 2x + 2\right)\left(x^2 - 2\right) = x^4 + 2x^3 - 4x - 4$. Thus $\langle p \rangle \cap \langle q \rangle = \left\langle \left(x^2 - 2\right)\left(x^2 - 2x + 2\right)\left(x^2 + 2x + 2\right) \right\rangle \neq \langle pq \rangle$. Thus the quotients cannot be isomorphic.

4A) Let p be a prime, and let F be the field with p elements. Suppose that $f \in F[x]$ is a polynomial of degree 4 such that f and $x^{p^2} - x$ are relatively prime. Show that f is irreducible.
Answer: From Grove we know that $x^{p^n} - x = \prod$ (irreducible polynomials degree $d|n$). Or from Theorem 3.11 we know that $[F_{p^n} : F_p] = n$ and $G(F_{p^n} : F_p) \cong \mathbb{Z}_n$ and F_{p^n} is a splitting field of $x^{p^n} - x$ over F_p. Now as $n = 2$ we know that $x^{p^2} - x$ factors into irreducible linear and quadratic factors. Take $\alpha \in F_p^*$ with $\left|F_p^*\right| = p-1$. Then $(\alpha)^{p^2} = ((\alpha)^p)^p - \alpha = \alpha^p - \alpha = \alpha - a = 0$. So every linear polynomial in $F_p[x]$ is a factor of $x^{p^n} - x$ so F has no linear factors as f is relatively prime to $x^{p^n} - x$. Now assume that f has quadratic factors, i.e. $f = gh$ where $\deg(g) = \deg(h) = 2$ and g and h are irreducible. However as $\deg x^{p^2} - x$ is degree p^2 and we have p linear terms and so there are $p^2 - p$ degrees worth of irreducible degree 2 polynomials. Thus we have all possible degree 2 irreducible polynomials over F_p. Thus as f and $x^{p^2} - x$ are relatively prime, we know that it has no quadratic terms.

4B) Let K be a finite extension of $\mathbb{Q}$ containing primitive n-th roots of unity, and let $\bar{K}$ be an algebraic closure of K. If $b^n = a \in K$ for some $b \in \bar{K} \backslash K$, then show that the extension $K(b)$ over K is Galois with cyclic Galois group. Give a generator of this Galois group explicitly.
Answer: We know that $x^n - a \in K[x]$ has a root in $\bar{K} \backslash K$, i.e. $b^n = a$. The full set of roots is given by $b, b\omega, ..., b\omega^{n-1}$ where ω is a primitive nth root of unity. All of these are in $K(b)$ so $K(b)$ is a splitting field for $x^n - a$ over K. Therefore Galois over K. Let $\varphi \in G(K(b) : K)$. We know that φ is determined by its action on b. So $\varphi(b) = \omega^k b$ for some $k \in (0, 1, ..., n-1)$. This gives an isomorphism with $\mathbb{Z}_n$ since $\varphi_k \varphi_l(b) = \omega^{k+l} b = \omega^m b$ where $m = k + l \bmod n$. Therefore $G(K(b) : K) \cong \mathbb{Z}_n$. Let $k \in \mathbb{Z}_n$ such that $(k, n) = 1$ then $(k) = \mathbb{Z}_n$ and therefore $(\varphi_k) = G(K(b) : K)$.

5A) Let A be an $n \times n$ rational matrix. Suppose that $d \neq 0$ is a natural number such that the entries of the matrices $\left\{A^K : K \geq 0\right\}$ are integral multiples of $1/d$. Show that for some invertible matrix C, the matrix $C^{-1}AC$ has integer entries. Hint: Consider the $\mathbb{Z}$-module generated by $\left\{A^k v : k \geq 0,\, v \in \mathbb{Z}^n\right\}$.
Answer: Did not have time!

5B) Let M be $\mathbb{C}^3$ with elements considered as column vectors. We make M into a $\mathbb{C}[x]$ module by having x act by left multiplication by the matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{pmatrix}$$

and by having elements of $\mathbb{C}$ act by scalar multiplication. Find the rank and torsion of this module and give its decomposition as a direct sum of cyclic modules.
Answer: The matrix that is given is in JCF. Thus it has only only invariant factor of $(x-1)^2(x-i)$. Thus we know that $M \cong \mathbb{C}[x] / \left\langle (x-1)^2 (x-i) \right\rangle$ which has rank 0 and ?????????