August 1999
Algebra Qualifying Exam
Sample Solutions

1A) An $n \times n$ matrix A over a field F is called anti-idempotent if $A^2 = -A$. Suppose A is anti-idempotent.

(a) What are the possible minimal polynomials for A?

(b) Show that A is diagonalizable over F.

(c) Show that two idempotent matrices over F are similar if and only if they have the same rank.

Answer: (a) As $A^2 = -A \implies A^2 + A = 0$ we know that $x^2 + x = x(x+1) = 0$ so the possible minimal polynomials are $x^2 + x$, $x + 1$, or x.

(b) The minimal polynomial has only distinct linear factors and a matrix is diagonalizable if and only if the minimal polynomial has distinct linear factors.

(c) The same rank implies that they have the same row and column space, so as the only eigenvalues are -1 and 0, they have the same JCF and so are similar.

1B) Let α be $\sqrt{2} + \sqrt{-1}$ in $\mathbb{Q}\left(\sqrt{2}, \sqrt{-1}\right) = L$. Choose a $\mathbb{Q}$-basis B for the $\mathbb{Q}$-vector space L. Furthermore, determine the matrix M_B of the linear transformations $\alpha^* : L \to L$ given by $x \to x \cdot \alpha$ and the rational canonical form of M_B.

Answer: Basis: $\left\{1, i, \sqrt{2}, \sqrt{2}i\right\}$. For the matrix M_B, just look at the images of the basis elements: $1 \to \sqrt{2} + i$, $i \to -1 + \sqrt{2}i$, $\sqrt{2} \to 2 + i\sqrt{2}$, $\sqrt{2}i \to 2i - \sqrt{2}$

$$M_B = \begin{bmatrix} 0 & -1 & 2 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

RCF: The Smith Normal Form of $A - xI$ is:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & x^4 - 2x^2 + 9 \end{bmatrix}$$

The characteristic polynomial of A is $\det(A - \lambda I) = x^4 - 2x^2 + 9$. As A has distinct factors, it must have characteristic polynomial equal to minimal polynomial as all invariant factors divide the next one. Thus the RCF is

$$\begin{bmatrix} 0 & 0 & 0 & -9 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

2A)There is a simple group of order 168. Determine, with reasons, how many elements of order 7 it has.

Answer: As $168 = 2^3 \cdot 3 \cdot 7$, we know by the Sylow theorems that there are $n_7 = 1 \bmod 7$ Sylow 7-subgroups. So there are either $1, 8, 15, 22, 29, 36, ...$ of them. But we know that our only choices are 1 or 8 as n_7 must divide the order of G. A corollary to the Sylow theorems says that a Sylow subgroup is normal if and only if it is unique. As our group is simple, there must be 8 Sylow 7-subgroups and therefore $8\,(7-1) = 8 \cdot 6 = 48$ elements of order 7.

2B) Let G be a finite nilpotent group. Show that for any divisor n of the order of G there exists a subgroup whose order is n. Hint: Consider the case that G is a p-group, p a prime first. Note that the center of G is nontrivial.
Answer: First I will prove the following claim: A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.

Proof: We first show that if H is a proper subgroup of a nilpotent group that $N(H) \neq H$ (the normalizer of H is not H). Let n be maximal such that $Z_n \subsetneqq H$ (contained in but not equal to H). Choose $x \in Z_{n+1} \notin H$. Let $h \in H$. Then

$$x^{-1}hx = h\left(h^{-1}x^{-1}hx\right) \in HZ_n = H,$$

so $x \in N(H)$. Now let P be a Sylow P-subgroup. Suppose P is not normal, that is $N(P) \neq G$. Then P is a proper subgroup of G, so by assertion $N(P) \neq P$. Using the same fact again for proper subgroup $N(P)$ we have $N(N(P)) \neq N(P)$, a contradiction (See Grove p.30 Prop 7.4).

($H \supset N \supset NP$, let $x \in N(H)$. P and $x^{-1}Px$ are Sylow P-subgroups in H. So $\exists y \in H$ s.t. $P = y^{-1}x^{-1}Pxy$. So $xy \in N(P) \subset A$, so $x \in H$.)
This proves every Sylow P-subgroup is normal. The converse is proved by noting that every Sylow subgroup is a p-group and therefore nilpotent (Grove p.29). (G/Z_1 is also a p-group, ...) And the direct product of nilpotent groups is nilpotent. (Let H and K be nilpotent groups. $Z_m(H \times K) = Z_m(H) \times Z_m(K)$ for any m. Hence $Z_m(H \times K) = H \times K$ for some m. Therefore $H \times K$ is nilpotent and the general result follows from induction.) Or we could have just quoted Grove Theorem 7.8: A finite group G is nilpotent iff it is the direct product of its Sylow subgroups.
Lastly, assume that $|G| = n = p_1^{e_1} \cdots p_r^{e_r}$. Then $G = S_{p_1} \oplus \cdots \oplus S_{p_r}$ and $|S_{p_i}| = p_i^{e_i}$. Let $d = p_1^{f_1} \cdots p_r^{f_r}$. By the first Sylow theorem, each S_{p_i} contains a subgroup S'_{p_i} of order $p_i^{f_i}$. Grove p.20 using ex 2.4 and Sylow 1). Then $H = S'_{p_1} \oplus \cdots \oplus S'_{p_r}$ is a subgroup of order d.

3A) Suppose the abelian group A has presentation

$$A = \langle a, b, c, d : 3a = 7d, b = 3d, 2a = b - 5d \rangle$$

Determine the structure of A as a direct sum of cyclic groups.
Answer: Another SNF calculation as if A is a finitely generated abelian group then there exists a non-negative integer m and integers $n_1, ..., n_k$ all larger than 1 with $n|n_{i-1}$ for $2 \leq$

$i \leq k$ such that $A \cong \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$:

$$\begin{bmatrix} 3 & 0 & 0 & -7 \\ 0 & 1 & 0 & -3 \\ 2 & -1 & 0 & 5 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 3 & -7 & 0 \\ 1 & 0 & -3 & 0 \\ -1 & 2 & 5 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & -3 & 0 \\ 0 & 3 & -7 & 0 \\ -1 & 2 & 5 & 0 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} 1 & 0 & -3 & 0 \\ 0 & 3 & -7 & 0 \\ 0 & 2 & 2 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & -7 & 0 \\ 0 & 2 & 2 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 3 & -7 & 0 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 1 & -9 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 1 & -10 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -10 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -10 & 0 \\ 0 & 0 & 20 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 20 & 0 \end{bmatrix}$$

So our group has 1 free generator and thus $G \cong \mathbb{Z}_{20} \oplus \mathbb{Z}$.

3B) Let R be a PID, let M be a free R-module of finite rank and let f be an R-endomorphism of M. Show that f is injective if and only if $M/\operatorname{Im}(f)$ is an R-torsion module.
Answer:

4A) Recall that two elements r and s of a ring R are algebraically independent over a subring S of R is the only poynomial $f(x,y) \in S[x,y]$ for which $f(r,s) = 0$ is the zero polynomial. If p and q are distinct (positive) primes in $\mathbb{Z}$, show that $\sqrt{p}$ and $\sqrt{q}$ are algebraically independent over $\mathbb{Z}$. **Note:** This is not true, find a counterexample.
Answer: If we take the polynomial $f(x,y) = px^2 - qy^2$ and take $x = \sqrt{q}$ and $y = \sqrt{p}$ then we have that $p\sqrt{q}^2 - q\sqrt{p}^2 = pq - qp = pq - pq = 0$.

4B) Let $f(x) = x^3 + 5x - 1 \in \mathbb{Q}[x]$.
(a) Show that f is an irreducible polynomial over $\mathbb{Q}$.
(b) Since f is irreducible $L = \mathbb{Q}[x]/(f)$ is a field. Determine the multiplicative inverse of $2x - 2 + (f)$ in L explicitly.
Answer: (a) As f is a degree 3 polynomial, it is irreducible iff it has a linear factor, i.e. a root in $\mathbb{Q}$. If we reduce coefficients mod 2, we get $\bar{f} = x^3 + x + 1$ and $\bar{f}(\bar{1}) = \bar{1}$ and $\bar{f}(\bar{0}) = \bar{1}$ so we know that f does not have any roots. We also could have noted that f is monic over $\mathbb{Q}$ and it contains a root in $\mathbb{Q}$ if and only if it contains a root in $\mathbb{Z}$ and the only choices would be 1 or -1 and $f(1) = 5$ and $f(-1) = -7$.
(b) As $\mathbb{Q}[x]$ is a PID we have unique factorization taking $p(x), q(x) \in \mathbb{Q}[x]$ such that $p(x)(x^3 + 5x - 1) + q(x)(2x - 2) = 1$. Use the Euclidean algorithm and we get inverse:

$$x^2 + x + 6 + (f)$$

5A) Let $F = C$, let $K = C(t)$, the field of rational operatornametions is an indeterminate t, and let G *be* the Galois group $G(K:F)$. Suppose φ and θ in G are determined by $\varphi(t) = \zeta t$ and $\theta(t) = 1/t$, where ζ is a primitive n^{th} root of unity in C, $n \geq 4$, and set $H = \langle \varphi, \theta \rangle \leq G$. Show that H is isomorphic with the dihedral group of order $2n$.
Answer:

5B) Let $\mathbb{F}_n$ denote the field with n elements.

(a) Construct explicitly the field with 64 elements by taking a degree 3 irreducible polynomial in $\mathbb{F}_4$.

(b) Determine the order and structure of the Galois group G of this extension.

(c) How many primitive elements over $\mathbb{F}_4$ does $\mathbb{F}_{64}$ contain? Justify.

Answer: (a) We first need a degree 3 irreducible polynomial over $\mathbb{F}_4[x]$. We take $\mathbb{F}_4$ as the set $\{0, 1, t, t+1\}$ with $t^2 + t + 1 = 0$. Consider the polynomial $f(x) = x^3 + x + 1$. We know that $f(1) = 1 = f(0)$. $f(t) = t^3+t+1 = t(t^2)+t+1 = t(t+1)+t+1 = t^2+1 = t+1+1 = t$. Also $f(t+1) = (t+1)^3 + t + 1 + 1 = (t^2+1)(t+1) + t = t(t+1) + t = t^2 = t+1$. Thus we take

$$\mathbb{F}_{2^6} = \mathbb{F}_{64} = \mathbb{F}_4[x] / \langle x^3 + x + 1 \rangle$$

(b) Suppose F is a finite field with q elements having prime field F_p. Then $q = p^n$ where $n = [F : F_p]$ and F is a splitting field over F_p for the polynomial $f(x) = x^q - x$. Conversely, if $0 < n \in \mathbb{N}$ and p is prime, then there is a field F with $q = p^n$ elements. The Galois group $G(F : F_p)$ is cyclic of order n, with the Frobenius map φ_p as a generator. By the Fundamental Theorem of Galois Theory and the fact that $[F_{64} : F_4] = 3$ we must have that $G \cong \mathbb{Z}_3$.

(c) There are 60 primitive elements as there are no subfields between F_4 and F_{64} and so for $\gamma \in F_{64}$, $F_4 \leq F_4(\gamma) \leq F_{64}$ and the only 4 elements for which $F_4(\gamma) \neq F_{64}$ are the elements of F_4 as there are no other possible subfields.