August 1994
Algebra Qualifying Exam
SOLUTIONS

1A) Suppose that A is an $n \times n$ complex matrix and $A^k = I$ for some $k \in \mathbb{Z}^+$. Prove that A can be diagonalized.
Answer: As A is over $\mathbb{C}$ we are guaranteed a Jordan Canonical Form (JCF) which is unique up to conjugation over $\mathbb{C}$. Therefore $J = P^{-1}AP$ and thus $PJP^{-1} = A$. So $\left(PJP^{-1}\right)^k = A^k = I$ implies that $PJ^kP^{-1} = I$ and so $J^k = I$. The only way that $J^k = I$ is if J is diagonal.

1B) True or false; for each give either a brief reason or a counterexample.
(a) If a matrix A is both Hermitian and unitary then $A = \pm I$.
(b) If V is a finite dimensional vector space and $T : V \to V$ is a linear transformation then $V = \operatorname{Im}(T) \oplus \ker(T)$.
(c) Eigenvalues of orthogonal matrices are real numbers.
Answer: (a) False, look at $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. They are Hermitian as $\bar{A}^T = A$ and unitary as $\bar{A}^T = A^{-1}$ (or $\bar{A}^T A = I$).
(b) False, take V as the polynomials of degree $\leq n$ and T the differential operator. So $\operatorname{Im}(T)$ is polynomials degree $\leq n-1$ and $\ker T$ is the constant operatornametions and So $\operatorname{Im}(T) \cap Ker(T) \neq \emptyset$. The only thing that holds is $DimV = Dim \operatorname{Im} + Dim \ker$.
(c) False, recall that orthogonal implies that $AA^T = I$. So take

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

but the characteristic equation of the first matrix is $x^2 + 1$ and so has eigenvalues $\pm i$.

2A) How many essentially distinct ways can A_4 act transitively on a set with 3 elements?
Answer: We first note that for any group G and a nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G to S_A. So we need to look at

$$\varphi : A_4 \to S_3.$$

Note that the only transitive subgroups of S_3 are S_3 and A_3. To find all homomorphisms we must see how many possible kernels there are which is the same as finding all possible normal subgroups: The only possible normal subgroups at 1, A_4, and the Klein 4 group V_4 ($\mathbb{Z}_2 \times \mathbb{Z}_2$). The fundamental homomorphism theorem says that $A_4 / \ker\varphi \cong \operatorname{Im}\varphi$ and so

$$\begin{aligned} A_4/1 &= A_4 \text{ and this image is too large} \\ A_4/A_4 &= 1 \text{ and this is not a transitive action} \\ A_4/V_4 &\cong Z_3 \text{ which is a transitive action.} \end{aligned}$$

So there is only one essentially distinct way.

2B) Suppose G is a group, $H \leq G$ and $x^2 \in H$ for all $x \in G$. Show that $H \lhd G$ and G/H is abelian.
Answer: If a subgroup contains the commutator subgroup then it is normal so we need to show that $G' \subset H$. Let $x^{-1}y^{-1}xy \in G'$. As

$$\begin{aligned} x^{-1}y^{-1}xy &= x^{-1}y^{-1}x^{-1}y^{-1}yxxyxxx^{-1}x^{-1} \\ &= \left(x^{-1}y^{-1}\right)^2 (yxx)^2 \left(x^{-1}\right)^2 \in H \end{aligned}$$

so $G' \subseteq H$ and so $H \lhd G$. As $\left(a^{-1}b^{-1}ab\right)H = H$, $(aH)(bH) = (bH)(aH)$.

3A) Show that every nonzero prime ideal in the ring $\mathbb{Z}[i]$ of Gaussian integers is maximal.
Answer: As $\mathbb{Z}[i]$ is a Euclidean domain (take $d = a^2 + b^2$ for the norm of $a + bi \in \mathbb{Z}[i]$) and ED $\Longrightarrow$ PID, we know that $\mathbb{Z}[i]$ is a PID. So show that in a PID every nonzero prime ideal is maximal. Suppose $P \neq R$ is

a prime ideal in R. $P = \langle p \rangle$ for some prime element $p \in P$ as $\mathbb{Z}[i]$ is a PID. Suppose I is an ideal such that $P \subsetneq I$. Show $I = R$. So there is an $a \in I$ such that $a \notin P$. So $\gcd(a, p) = 1$ and thus there are $s, t \in \mathbb{Z}[i]$ such that $1 = as + pt$. As $as \in I$ thus $1 \in I$ and $I = R$. So P is maximal.

3B) Suppose that R is a noncommutative semisimple ring and that $|R| = 81$. Describe the center of R as completely as possible.
Answer: As R is finite it is Artinian. By the Weddeburn Artin structure theorem we know that R is isomorphic to a direct sum of full matrix algebras over a division ring. If we have a finite division ring then it is a field by another theorem of Weddeburn. As $81 = 3^4$ the only possibility is a 2×2 matrix over $\mathbb{F}_3$. Now assume that $A \in Z(R)$, the center of R, then for any $B \in R$ we have $AB = BA$ and thus

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} &= \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Longrightarrow \\ \begin{bmatrix} ae + bg & af + bh \\ ec + dg & cf + dh \end{bmatrix} &= \begin{bmatrix} ae + fc & eb + fd \\ ga + hc & gb + hd \end{bmatrix} \end{aligned}$$

and so $bg = cf$ and as g and f are arbitrary, $b = c = 0$. So $af = fd$ and so $a = d$. So the center are just the scalar multiples of the identity matrix I and thus $|Z(R)| = 3$.

4A) If $f(x) = x^6 + x^4 - 3x^2 - 3 \in \mathbb{Q}[x]$, find a splitting field $K \subseteq \mathbb{C}$ for $f(x)$, and determine the Galois group of $f(x)$.
Answer: We first note that f is reducible. $f = \left(x^2+1\right)\left(x^4-3\right)$ which has roots $\pm i, \pm\sqrt[4]{3}, \pm\sqrt[4]{3}i$ and thus splitting field $\mathbb{Q}\left(\sqrt[4]{3}, i\right) = K$. We know that

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt[4]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{3}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8$$

We also know that $x^2 + 1$ splits over the splitting field for $x^4 - 3$ and thus we only consider that $G \leq S_4$. So G is D_4 as G is not abelian and D_4 is the only nonabelian group of order 8 of G. There are 3 of these and they are all conjugate as they are the Sylow 3-subgroups of S_4. Another (horrible) approach is to compute the resolvent cubic of $x^4 - 3$.

4B) Suppose that $f(x) \in \mathbb{Q}[x]$, $g(x) = f\left(x^2\right)$, $K \subseteq \mathbb{C}$ is a splitting field for $g(x)$ and $[K : \mathbb{Q}]$ is odd. Show that $f(x)$ and $g(x)$ have the same Galois group.
Answer: Say L is the splitting field of $f(x)$ with roots α_i. Then we know that the roots of $g(x)$ are $\pm\sqrt{\alpha_i}$. Thus is $[L : \mathbb{Q}] = n = 2m + 1$ then we know that $[K : \mathbb{Q}] = 2^k \cdot n$ for some k as each extension field for the roots $\sqrt{\alpha_i}$ is either 1 or 2. But as $[K : \mathbb{Q}]$ is odd we know that $k = 0$ and f and g have the same splitting field and thus the same Galois group.

5A) If $A = \langle a, b : 45a = 63b = 105(a + b) = 0\rangle$, then describe A as a direct sum of cyclic groups and determine $|A|$.
Answer: State the correct theory and then proceed to do SNF as follows:

$$\begin{pmatrix} 45 & 0 \\ 0 & 63 \\ 105 & 105 \end{pmatrix} \to \begin{pmatrix} 45 & 0 \\ 0 & 63 \\ 15 & 105 \end{pmatrix} \to \begin{pmatrix} 15 & 105 \\ 0 & 63 \\ 45 & 0 \end{pmatrix} \to \begin{pmatrix} 15 & 0 \\ 0 & 63 \\ 45 & 315 \end{pmatrix} \to$$
$$\begin{pmatrix} 15 & 0 \\ 0 & 63 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 15 & 60 \\ 0 & 63 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 15 & 60 \\ -15 & 3 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & -15 \\ 60 & 15 \\ 0 & 0 \end{pmatrix} \to$$
$$\begin{pmatrix} 3 & 0 \\ 60 & 315 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 3 & 0 \\ 0 & 315 \\ 0 & 0 \end{pmatrix}$$

and thus $A \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{315}$ and the order of A is 945.

5B) Give a proof or a counterexample.
(a) If R is a PID and M is a finitely generated torsion free R-module, then M is free.
(b) If R is an ID and M is a finitely generated torsion free R-module, then M is free.

Answer: (a) If R is a PID and M is finitely generated torsion free R-module then M is free. $M \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$ with $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$. Since M is torsion free each ideal I_k is the zero ideal and thus $M \cong R^n$.

(b) $R = \mathbb{Z}[x]$ and the ideal $\langle 2, x \rangle = M$ is an R-module. The module M is finitely generated and torsion free. However M is not free since the ideal isn't principal no single element generates it. Any two or more elements are linearly independent since $ab - ba = 0$. Thus the module cannot have a basis.