# January 1995
# Algebra Qualifying Exam
Solutions

1A) If $A = \begin{pmatrix} 5 & 12 \\ 12 & -5 \end{pmatrix}$, find an orthogonal matrix $M$ that diagonalizes $A$.

**Answer:** $A$ has characteristic polynomial $(5-x)(-5-x) - 144 = x^{12} - 169$ which gives eigenvalues $\pm 13$. The corresponding eigenvectors are $5x_1 + 12x_2 = \pm 13 x_1$ and $12x_1 - 5x_2 = \pm x_2$ giving eigenvectors of

$$\begin{pmatrix} 1 \\ 3/2 \end{pmatrix}, \begin{pmatrix} 1 \\ -3/2 \end{pmatrix}$$

So as these eigenvectors are orthogonal already, we only need to normalize them to 1. Thus we take the matrix

$$\frac{1}{\sqrt{13}} \begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix} = M$$

Which gives $M^{-1}AM = M^T AM = \begin{pmatrix} 13 & 0 \\ 0 & -13 \end{pmatrix}$

1B) Suppose $V$ is a finite dimensional vector space and $T : V \to V$ is a linear transformation for which every nonzero vector is an eigenvector. Prove that $T$ is a scalar multiple of the identity transformation.

**Answer:** Linear means that $T(\alpha v + \beta w) = \alpha Tv + \beta Tw$. Consider the standard basis for $V$ as $\{e_1, ..., e_n\}$. Let $\alpha$ be an eigenvalue for $(1, 1, 1, ..., 1) = \bar{e}$. Then $T(\bar{e}) = \alpha \bar{e} = \alpha e_1 + \cdots + \alpha e_n = T(e_1) + \cdots + T(e_n)$ so the eigenvalues for all basis elements are the same. Consider $v \in V$:

$$\begin{aligned} T(v) &= T(\beta_1 e_1 + \cdots + \beta_n e_n) = \beta_1 T(e_1) + \cdots + \beta_n T(e_n) \\ &= \beta_1 \alpha e_1 + \cdots + \beta_n \alpha e_n = \alpha v. \end{aligned}$$

Thus the only possibility is a scalar multiple of the identity transformation.

2A) Suppose $p$ is a prime and $G$ is a finite group. A subgroup $K$ of $G$ is called a normal $p$-complement if $K \lhd G$ and there is a Sylow $p$-subgroup $P$ such that $K \cap P = 1$ and $KP = G$. Show that if $G$ has a normal $p$-complement then it is unique. Give an example.

**Answer:** Example: Let $G = S_3$ and $K = \mathbb{Z}_3$ which is normal as $[G : K] = 2$. There are 3 Sylow 2-subgroups with $\mathbb{Z}_2 \cap \mathbb{Z}_3 = 1$ (if not then there is an element of order 2 in $\mathbb{Z}_3$, a contradiction). $\mathbb{Z}_2\mathbb{Z}_3 = S_3$ because $S_3$ has 6 elements. $K$ is unique as there is only one $\mathbb{Z}_3$ in $S_3$.

Proof: Suppose there is $K, L$ normal $p$-complements, $|G| = p^\alpha m$ with $(p, m) = 1$. Let $P_k$ and $P_l$ be Sylow $p$-subgroups with $P_k^x = xP_kx^{-1} = P_l$ (as all Sylow subgroups are conjugate).

$$\begin{aligned} 1 &= K \cap P_k \implies 1 = 1^x = (K \cap P_k)^x = K \cap P_l \\ KP_x &= G \implies G = G^x = (KP_k)^x = \left(Kxx^{-1}P_k\right)^x = KP_l. \end{aligned}$$

Thus we can talk about just $P_l = P$. Now consider the following:

$$\begin{aligned} G/K &= KP/K = P/(K \cap P) = P \text{ and} \\ G/L &= LP/L = P \implies |K| = |L| = m \end{aligned}$$

And $\Phi : G \to G/K$ takes $L \to 1$ because $G/K = P$ so $L \subset K$ because the order of $L$ and $K$ are the same.

2B) Let $n$ be a positive integer and $M_n(\mathbb{C})$ be the set of $n \times n$ matrices with complex entries. If $A \in M_n(\mathbb{C})$, denote its determinant by $A$. Let $GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) : \det A \neq 0\}$ and let $SL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) : \det A = 1\}$. Show that $GL_n(\mathbb{C})$ is a group under matrix multiplication, that $SL_n(\mathbb{C})$ is a normal subgroup of $GL_n(\mathbb{C})$ and identify the quotient group $GL_n(\mathbb{C})/SL_n(\mathbb{C})$. You may use basic properties of matrices without deriving them.

**Answer:** Group: Identity element is usual identity matrix $I_n$ and has $\det I_n = 1$.

Inverse: $\det A \neq 0$ implies that $A$ is invertible

Associativity: for all matrices $A(BC) = (AB)C$

Closure: $\det(AB) = \det(A)\det(B)$

(ii) $SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$. Check that $\det(A^{-1}SA) = \det(A^{-1})\det(S)\det(A) = \det(S)$ and $\det(S) = 1$ and $S \in SL_n(\mathbb{C})$.

(iii) $GL_n(\mathbb{C})/SL_n(\mathbb{C})$: Consider the map

$$\varphi : GL_n(\mathbb{C}) \to \mathbb{C}$$

by $\varphi(A) = \det A$ has kernel $K = \{B : \det(B) = 1\} = SL_n(\mathbb{C})$. And this is onto $\mathbb{C} - \{0\}$. So by the FHT $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \cong \mathbb{C} - \{0\}$, which is the multiplicative group of $\mathbb{C}^*$.

3A) Determine the Galois group (over $\mathbb{Q}$) of $f(x) = x^5 + 3x^3 - 2x^2 - 6$.
**Answer:** $f(x) = x^3(x^2+3) - 2(x^2+3) = (x^3-2)(x^2+3)$ has roots $\pm\sqrt{3}i$, $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ where $\omega = e^{2\pi i/3}$. So the splitting field is $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}) = K$. The degree of the splitting field is 6. The Galois group is $S_3$.

3B) Say whether each of the following is true or false. Give a proof or counterexample.

(a) Let $K$ be a field of characteristic 0 and let $L$ be an extension of degree 2. Then $L$ is Galois over $K$.

(b) Let $K$ be a field of characteristic 0 and let $L$ be an extension of degree 3. Then $L$ is Galois over $K$.

**Answer:** (a) As $K$ is a field of characteristic 0 and $L$ is an extension of $K$, then $L$ must be separable. Any degree 2 extension is normal and any normal, separable extension is Galois.

(b) Take $\mathbb{Q}(\sqrt[3]{2})$ has characteristic zero. It has minimal polynomial $x^3 - 2$ but it has two complex nonreal roots and thus is not normal over $\mathbb{Q}$.

4A) A commutative ring $R$ with 1 is said to be a local ring if it has exactly one maximal ideal $M$. Prove that every element of $R$ is either a unit or an element of $M$.
**Answer:** Let $r \in R$. Suppose that $r \notin M$. Then there does not exist $I \lhd R$ such that $r \in I$ unless $I = R$. Consider $\langle r \rangle$. It cannot be contained in $M$ because $r \notin M$. So $\langle r \rangle \cap M = 0$ or $\langle r \rangle = R$. Thus the only possibility is $\langle r \rangle = R$.

4B) A commutative ring $R$ is called Boolean if $x^2 = x$ for all $x \in R$.

(a) Show that in a Boolean ring $2x = 0$.

(b) Prove that in a Boolean ring then each prime ideal $P \neq R$ is maximal.

**Answer:** (a) $2x = (x+x)^2 = x^2 + 2x + x^2 = 2x^2 + 2x$ and so $2x^2 = 2x = 0$.

(b)Consider $R/P$. Because $P$ is prime $ab \in P$ (equivalently, $\bar{a}\bar{b} = \bar{0}$) implies $a \in P$ or $b \in P$ (i.e. $\bar{a} = 0$ or $\bar{b} = 0$). So $R/P$ is an integral domain. Now for all $x \in R$, $(x+P)(x+P) = x^2 + P = x + P$. So $R/P$ is also a Boolean ring in addition to being an integral domain. But we know that an integral domain has no idempotents except 0 and possibly unity or else if $x \neq 1$ or 0 then $x^2 = x \implies x(x-1) = 0$ which is a contradiction. Thus $R/P = \{\bar{0}\}$ or $R/P = \{\bar{0}, \bar{1}\}$. However, $R/P = (\bar{0})$ implies that $R = P$ which is not true. So $R/P = \{\bar{0}, \bar{1}\}$ which is clearly a field. Hence $P$ is maximal.

5A) Let $R$ be a commutative ring and $A$ an $R$-module. Let

$$TorA = \{a \in A : \exists r \neq 0 \in R \text{ such that } ra = 0\}$$

(a) If $f : A \to B$ is an $R$-homomorphism then show that $f(Tor(A)) \subseteq Tor(B)$.

(b) If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is an exact sequence of $R$-modules, then so is $0 \longrightarrow TorA \xrightarrow{f_T} TorB \xrightarrow{g_T} TorC \longrightarrow 0$ by the maps $f$ and $g$ restricted to the torsion submodules.

(c) If $g : B \to C$ is an epimorphism give an example to show that $g_T : TorB \to TorC$ need not be an epimorphism.

**Answer:** (a) Let $a \in TorA$. This implies there is a nonzero $r \in R$ such that $ra = 0$. As $0 = f(0) = f(ra) = r(f(a))$ we have that $f(a) \in TorB$.

(b) $f$ is 1-1 and therefore $f_T$ is 1-1 as all we are doing is restricting. We need to show that $\operatorname{Im} f_T = \ker g_T$. We know $\operatorname{Im} f = \ker g$ as we have an exact sequence. Let $b \in \operatorname{Im} f_T$. Then $b \in TorB$. There is a nonzero $r \in R$ such that $rb = 0$. Thus $g(rb) = 0$ and $r(g(b)) = 0$ so $b \in \ker g_T$. Also, if $b \in \ker g_T$ and $g(b) = 0$ then $r(g(b)) = 0$ and so $g(rb) = 0$ and so $rb = 0$ and so $b \in TorB$.

(c) Take $g : \mathbb{Z} \to \mathbb{Z}_6$ and $\mathbb{Z}$ has $Tor\mathbb{Z} = \{0\}$ and $g(0) = \bar{0}$. But $Tor(\mathbb{Z}_6) = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$.

5B) True or false (proof or counterexample):

(a) Every submodule of a free module is free.

(b) $R$ is commutative with 1; $M$ an $R$-module implies that $M$ is a finite set if and only if finitely generated and every element is a torsion element.

**Answer:** (a) False, take $\mathbb{Z}_4$ as a $\mathbb{Z}_4$ module. This is free as it has a basis of $\bar{1}$. Take $M = 2\mathbb{Z}_4$ as a $\mathbb{Z}$-submodule. There is no linearly independent set to use for a basis. Consider the only nonzero element $\bar{2}$. But we have that $\bar{2}\bar{2} = \bar{4} = \bar{0}$ and so $\bar{2}$ is linearly dependent.

(b) Take $\mathbb{Z} \oplus \mathbb{Z}$ as a ring (not even an ID as $(0,1)(1,0) = (0,0)$. Take $M = 0 \oplus \mathbb{Z}$ as a $\mathbb{Z} \oplus \mathbb{Z}$-module. It is finitely generated by $(0,1)$. All elements are torsion: $(*,0)(0,a) = (0,0)$ for all $(0,a) \in M$ but it is not a finite set.