August 2002
Algebra Qualifying Exam
Sample Solutions

1A) Give a concrete example of a real matrix A such that $A^5 = I$ and A is not diagonalizable over $\mathbb{R}$. Show that A is diagonalizable over $\mathbb{C}$.
Answer: We know that $A^5 - I = 0$ and thus the minimal polynomial of A must divide $x^5 - 1$. As $x^5 - 1 = (x-1)\left(x^4 + x^3 + x^2 + x + 1\right)$, we know that the matrix corresponding to the rational canonical form of $x^4 + x^3 + x^2 + x + 1$ will have $A^5 = 1$ but will not be diagonalizable as a matrix is diagonalizable if and only if its minimal polynomial factors into distinct linear terms. Thus we take

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

If we consider A over $\mathbb{C}$ then we know that $x^4+x^3+x^2+x+1$ factors into linear terms as $(x-\omega)\left(x-\omega^2\right)\left(x-\omega^2\right)\left(x-\omega^3\right)$ for ω a primitive n^{th} root of unity. Therefore the matrix is diagonalizable.

1B) Let V be a vector space over a field K, with a non-degenerate bilinear pairing

$$\langle , \rangle : V \times V \to K.$$

(a) Show that for any linear map $A : V \to V$, there is a unique linear map $A^* : V \to V$ such that $\langle Av, w\rangle = \langle v, A^* w\rangle$ for all $v, w \in V$. The map A^* is called *adjoint* of A with respect to the pairing $\langle , \rangle$.
(b) Suppose that $V = K^n$ for some positive integer n. Describe all non-degenerate pairings on V with the property that, for all linear maps $A : V \to V$, the matrix for the adjoint of A with respect to the pairing is the transpose of the matrix for A.
Answer: Let K be a field and V our vector space. A K-bilinear pairing on $V \times V$ is a map

$$f : V \times V \to K$$

having the following properties: For each $v \in V$, the map

$$v \mapsto f(w, v)$$

is K-linear and for each $w \in V$ the map

$$w \mapsto f(w, v)$$

is K-linear. We now just write $\langle v, w\rangle_f$ or $\langle v, w\rangle$ to denote $f(v, w)$. If $v \in V$ we write $v \perp w$ if $\langle v, w\rangle = 0$. Similarly for any subset $S \subseteq V$ we define $v \perp S$ if $v \perp w$ for all $w \in S$. We then say that v is perpendicular to S. We let $S^{\perp}$ consist of all elements of V which are perpendicular to S. It is obviously a subspace of V. We define perpendicularity on the other side in the same way. We define the kernel of f to be $V^{\perp}$. We say that f is nondegenerate if the kernel is zero. We now denote $L(V, K)$ the set of all bilinear maps of $V \times V$ to K. It is clear that this set is also a vector space, addition of maps being the usual one, and also the multiplication of maps by elements of K.

The form f gives rise to a linear map

$$\varphi_f : E \to Hom_K(V, K)$$

such that

$$\varphi_f(v)(w) = f(v, w) = \langle v, w\rangle,$$

for all $v, w \in V$. We call $Hom_K(V, K)$ the dual vector space of V and denote it by V^*. We have an isomorphism

$$L(V, K) \leftrightarrow Hom_K(V, Hom_K(V, K))$$

given by $f \mapsto \varphi_f$, its inverse being defined in the natural way: If

$$\varphi : V \to Hom_K(V, K)$$

is a linear map, we let f be such that

$$f(v,w) = \varphi(v)(w).$$

We often say that f is non-singular if φ_f is an isomorphism, in other words if our bilinear pairing can be used to identify V with V^*. We now have an isomorphism

$$End_K(V) \mapsto L(V,K)$$

depending on the fixed non-singular bilinear map $f : V \times V \to K$.

Let $A \in End_K(V)$ be a linear map of V to itself. Then the map

$$(v,w) \mapsto \langle Av, w\rangle = \langle Av, w\rangle_f$$

is bilinear and in this way we associate linearly with each $A \in End_K(V)$ a bilinear map in $L(V,F)$.

Conversely, let $h : V \times V \to K$ be bilinear. Given $v \in V$ the map $h_v : V \to K$ such that $h_v(w) = h(v,w)$ is linear and is in the dual space V^*. By assumption, there exists a unique element $v' \in V$ such that for all $w \in V$ we have

$$h(v,w) = \langle v', w\rangle$$

It is clear that the association $v \mapsto v'$ is a linear map of V into itself. Thus with each bilinear map $V \times V \to K$ we have associated a linear map $V \to V$.

Then it follows that the mappings described in the previous paragraphs are inverse isomorphisms between $End_K(V)$ and $L(V,R)$. They do depend on the given f.

Now we get as a result of all of the above with $A : V \to V$ linear and $(v,w) \mapsto \langle Av, w\rangle$ its associated bilinear map. There exists a unique linear map

$$A^t : V \to V$$

such that

$$\langle Av, w\rangle = \left\langle v, A^t w\right\rangle$$

for all $v, w \in K$.

(b) I think it is just the standard inner product.

2A) Give a concrete example of each of the following:
(a) A group whose commutator subgroup is strictly contained in its center.
(b) A group whose center is strictly contained in its commutator subgroup.
Answer: (a) Consider any abelian group G. Then we know that $\langle G\rangle = 1$. However for any abelian group G we know that $Z(G) = G$ and $1 < G$.
(b) Consider S_3 (or any symmetric group). We know that $Z(S_3) = 1$ (all symmetric group S_n, $n \geq 3$ are centerless). The commutator subgroup $\langle S_3\rangle = A_3$. Note that for the Dihedral group of order 8 we have that the commutator subgroup has order two and so does the center. They are actually the same and so it is not an example.

2B) Suppose that G is a finite group that acts faithfully and transitively on a finite set S. If $G_a = Stab_G(a)$, $a \in S$, show that there does not exist nontrivial $N \lhd G$ with $N \leq G_a$.
Answer: Recall that a group action of G acting on S is a mapping from $G \times S \to S$ with $(x,s) \to xs$ which satisfies (a) $(xy)s = x(ys)$ and $1_G s = s$ for all $x, y \in G$ and $s \in S$. If a group G acts faithfully on a finite set S then we know that $\varphi : G \to Perm(S)$ is a monomorphism. Another way of considering this is if we define the kernel of the action as the set of elements of G that act trivially on every element of A ($\{g \in G : ga = a \text{ for all } a \in S\}$). The action acts faithfully if the kernel is trivial. If G acts transitively on a set S then for any $s, t \in S$ we can find a $g \in G$ such that $gs = t$. Another way to think of a transitive action is that there is only one orbit.
We first prove the following fact: $Stab_G(xs) = xStab_G(s)x^{-1}$.

$Stab_G(xs) = \{g \in G : gxs = xs\}$. Let $g \in Stab_G(xs)$. Then $gxs = xs$ and thus $x^{-1}gxs = s$ and thus $g \in xStab_G(s)x^{-1}$. Now take $g' \in xStab_G(s)x^{-1}$ thus $x^{-1}g'xs = s$ and so $g'xs = xs$ and so $g' \in Stab_G(xs)$. As G is transitive, for all $s, t \in S$ there is a $g \in G$ such that $gs = t$. Now assume that there is an $N \lhd G$ with $N \leq G_a$. Take $n_1 \neq 1 \in N$. Thus $n_1 \in Stab_G(s)$. Thus $n_1 a = a$. Take any arbitrary $t \in S$. Thus $ga = t$ and from our previous fact we know that $Stab_G(t) = gStab_G(a)g^{-1}$ and so $n_1 t = t$ as $n_1 = gn_2 g^{-1}$

for some $n_2 \in N$ as N is normal. Thus the action is not faithful as we have found $n_1 \in G$ where $n_1 a = a$ for all $a \in S$.

3A) If R is a ring and $a, b \in R$ are both nonzero and both are not zero divisors show that a and b have the same additive order.
Answer: Consider $a, b \neq 0$ with $ab \neq 0$ and $ba \neq 0$. Without loss of generality assume that the order of a is m and b is n with $m \leq n$. Then

$$n(ab) = ab + \cdots + ab = a(b + \cdots + b) = a(nb) = 0.$$

Thus we know that $n \mid m$ and so $m = n$.

3B) Let R be a commutative ring with 1, and suppose that there is exactly one maximal ideal in R. Show that every element of R not in the maximal ideal is a unit.
Answer: Let M the maximal ideal and $x \in R \setminus M$. Consider the ideal generated by x, $\langle x \rangle$. Then as M is maximal, we have either that $\langle x \rangle \subseteq M$ or $\langle x \rangle = R$. We know that $\langle x \rangle$ is not in M as $x \notin M$. Thus $\langle x \rangle = R$ and thus x must be a unit.

4A) (a) Let a and b be nonzero rational numbers. Prove that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}\left(\sqrt{b}\right)$ if and only if there exists a rational c such that $a = bc^2$.
(b) Let $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{-3}, \sqrt{5}\right)$. Prove that K does not contain a square root of -1. [Hint: Use Galois theory and part (a)].
Answer: (a) If b has a square root in $\mathbb{Q}$ then $\mathbb{Q}\left(\sqrt{b}\right) = \mathbb{Q}$ and so also a has to have a square root in $\mathbb{Q}$ then we have a c such that $a = bc^2$. So assume a and b do not have square roots in $\mathbb{Q}$. Assume that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}\left(\sqrt{b}\right)$. This implies that $\sqrt{a} \in \mathbb{Q}\left(\sqrt{b}\right)$. Thus we can write $\sqrt{a} = q_1 + q_2\sqrt{b}$ for $q_i \in \mathbb{Q}$. Thus $a = \left(q_1 + q_2\sqrt{b}\right)^2 = q_1^2 + 2q_1q_2\sqrt{b} + q_2^2 b$. Thus this is only a rational number if q_1 or $q_2 = 0$. If $q_2 = 0$ then $a = q_1^2$ which is not possible as a does not have a square root. So $q_1 = 0$ and we have $a = q_2^2 b$ and take $q_2 = c$. Similarly in the other direction.

(b) By considering all possible subfields and seeing that $\mathbb{Q}\left(\sqrt{2}\right) \neq \mathbb{Q}\left(\sqrt{-3}\right) \neq \mathbb{Q}\left(\sqrt{5}\right)$ by using (a) we need to have $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{-1}\right)$, etc. But just use (a) and it is not possible.

4B) Suppose that K is a field of characteristic $p > 0$ and $F = K(t)$, the field of rational operatornametions in an indeterminate t. Set $f(x) = x^{2p} - tx^p + t \in F[x]$.
(i) Show that $f(x)$ is irreducible in $F[x]$.
(ii) Let s be a root of $x^p - t \in F[x]$, set $E = F(s)$, and let L be a splitting field for $f(x)$ over E. Show that $[L : E] \leq 2$.
Answer: (i) As t is an indeterminate, we know that t is prime in F. Thus by the Eisenstein criterion with $p = t$ we have that f is irreducible. (ii) As f is irreducible we know that $[L : F] \leq (2p)!$. Note that $f(x) = g\left(x^2\right)$ for $g(x) = x^p - tx + t$. As g is irreducible in $F[x]$, we know that f splits over the splitting field for g over in a degree 2 extension as the roots of $g\left(x^2\right)$ are $\pm\sqrt{\alpha_i}$ for α_i the roots of $g(x)$. As $x^p - t$ is also irreducible in $F[x]$ we know that if α is a root then so is any $\alpha + a$ for $a \in F$. So we know that $g(x)$ splits over $F(\alpha)$. Thus it is clear that $[L : E] \leq 2$.

5A) Determine a $\mathbb{Z}$-module monomorphism $f : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$. Show that $1 \otimes f : \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4$ is the zero map but that $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \neq 0$ and $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \neq 0$.
Answer: Consider the map $\bar{0} \to \bar{0}$ and $\bar{1} \to \bar{2}$, i.e. $f(x) = 2x$. We show that this is a $\mathbb{Z}$-module homomorphism.

$$\begin{aligned} f(x+y) &= 2(x+y) = 2x + 2y = f(x) + f(y) \text{ and} \\ f(a \cdot x) &= 2(a \cdot x) = ax + ax = a(x+x) = a(2x) = a \cdot f(x) \text{ for } a \in \mathbb{Z} \end{aligned}$$

Now we compute the map $1 \otimes f$.

$$(1 \otimes f)(x \otimes y) = x \otimes 2y = 2x \otimes y = 0 \otimes y = 0$$

However we know that $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$ and $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \cong \mathbb{Z}_2$. In general we have that $\mathbb{Z}_m \otimes \mathbb{Z}_n \cong \mathbb{Z}_{(m,n)}$. We prove it in the simple case of $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2$. Consider the map

$$\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \text{ by } x \to 1 \otimes x$$

1-1: Assume that $\varphi(x) = \varphi(y)$. Then $1 \otimes x = 1 \otimes y \implies 1 \otimes (x - y) = 0$ and thus $x - y = 0$ and so $x = y$. For onto, assume that you have $x \otimes y$. Just take $f(x)$ as $f(x) = 1 \otimes x$ and this is all we have as only possibilities are $1 \otimes 1$ or $0 \otimes 1 = 1 \otimes 0 = 0 \otimes 0$.

5B) Let A be the abelian group generated by x_1, x_2, x_3, x_4 and x_5 subject to the relations

$$x_2 - x_1 = x_3 - x_2 = x_4 - x_3 = x_5 - x_4 = x_1 - x_5.$$

Show that A contains an element of exact order 5.
Answer: This is equivalent to

$$-2x_1 + x_2 + x_5 = -x_1 - x_2 + x_3 + x_5 = -x_1 - x_3 + x_4 + x_5 = -x_1 - x_4 + 2x_5 = 0$$

We write this down in the 4×5 matrix as follows:

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

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

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 2 \\ 0 & -1 & -1 & 1 & 1 \\ 0 & 0 & -1 & -1 & 2 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 2 \\ 0 & 0 & -4 & 1 & 3 \\ 0 & 0 & -1 & -1 & 2 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -4 & 1 & 3 \\ 0 & 0 & -1 & -1 & -2 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 2 \\ 0 & 0 & -4 & 1 & 3 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 2 \\ 0 & 0 & 0 & 5 & -5 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 5 & -5 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 5 & -5 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \end{bmatrix}$$

Therefore we have that $G \cong \mathbb{Z} \oplus \mathbb{Z}_5$.