August 2003
Algebra Qualifying Exam
Solutions

1A) Let V be a vector space, $W \subset V$ a subspace. Prove or give a counterexample: if $T : V \to V$ is a linear transformation such that

- $T(w) = w$ for all $w \in W$ and
- $T(v + W) = v + W$ for all $v \in V$,

then T is the identity map.
Answer: Counter example. Consider the map with standard basis that maps $(0,1) \to (0,1)$ and $(1,0) \to (1,1)$. Take $w = Span\{(0,1)\}$. Then $(a,b) \to (a, a+b) = a(1,1) + b(0,1)$.

1B) If $A = \begin{pmatrix} -8 & 18 \\ -6 & 13 \end{pmatrix}$ find a square root for A, i.e. find a matrix B such that $B^2 = A$.
Answer: We will attempt to diagonalize the matrix, $D = P^{-1}AP$, then find B such that $B^2 = D$ and then PBP^{-1} will be a root for A. First we compute the characteristic polynomial of A. $\det(A - xI) = x^2 - 5x + 4 = (x-1)(x-4)$ and thus we have eigenvalues $1, 4$. The corresponding eigenvectors are solutions of

$$\begin{bmatrix} -9 & 18 \\ -6 & 12 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} -12 & 18 \\ -6 & 9 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

We get $t(2,1)^T$ and $s(3,2)^T$. Thus $P = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$ and $P^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$. Just to check (as any diagonalizable matrix is diagonal with its eigenvalues as the entries on the diagonal) we compute $P^{-1}AP = D$:

$$\begin{aligned} \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} \begin{pmatrix} -8 & 18 \\ -6 & 13 \end{pmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} &= \begin{bmatrix} 2 & -3 \\ -4 & 8 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = D \end{aligned}$$

For a square root of D we can take $B = \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 2 \end{bmatrix}$. As problem asks for one, we take just the positive ones. Thus PBP^{-1} is a root of A as $(PBP^{-1})^2 = PBP^{-1}PBP^{-1} = PB^2P^{-1} = PDP^{-1} = A$. Thus take

$$\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} -2 & 6 \\ -2 & 5 \end{bmatrix}$$

Check: $\begin{bmatrix} -2 & 6 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} -2 & 6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} -8 & 18 \\ -6 & 13 \end{bmatrix}$

2A) A group G is called a CA-group if the centralizer $C_G(x)$ is abelian if $1 \neq x \in G$. Write G^* for $G \setminus \{1\}$. Suppose that G is a CA-group.

(a) Show that the relation ˜ defined by $x \tilde{} y$ if and only if $xy = yx$ is an equivalence relation on G^*.

(b) If K is an equivalence class in G^* show that $K \cup \{1\}$ is a subgroup of G.

Answer: (a) $xx = xx$ so $x \tilde{} x$. Assume $x \tilde{} y$ then $xy = yx = xy$ and so $y \tilde{} x$. Now assume that $x \tilde{} y$ and $y \tilde{} z$. Then if $xy = yx$ and $yz = zy$ then y is in the centralizer of x, z is in the centralizer of y and vice versa. Thus it is immediate that $xz = zx$ and thus $x \tilde{} z$.

(b) To show that $K \cup \{1\}$ is a subgroup we must show that for $x, y \in K \cup \{1\}$ we have that $xy^{-1} \in K \cup \{1\}$. Assume that $xy \in K \cup \{1\}$. We show that $xyz = zxy$ will give us that $zxy^{-1} = xy^{-1}z$.

$$\begin{aligned} zxy^{-1} &= zxyy^{-1}y^{-1} \\ &= xyzy^{-1}y^{-1} \\ &= xyy^{-1}y^{-1}z \\ &= xy^{-1}z \end{aligned}$$

2B) An inner automorphism of a group G is an automorphism of the form $x \to gxg^{-1}$ for some $g \in G$. Show that every automorphism of S_3 (the symmetric group on 3 letters) is an inner automorphism.

Answer: $x \to gxg^{-1}$ is clearly an automorphism and thus $G/Z(G)$ is isomorphic to a subgroup of S_3. As $Z(S_3) = 1$, we know that S_3 is isomorphic to a subgroup of S_3. Thus it has size at least 6. To be an automorphism we must send two cycles to two cycles. S_3 is generated by the two cycles (12), (13), and $(2,3)$. Thus the only choice we have to send (12) is one of three places, then (13) to two of the remaining and thus the image of $(2,3)$ is determined. Thus $|Aut(S_3)| \leq 6$ and thus $Aut(S_3) \cong S_3$ and the only isomorphisms were given as inner automorphisms.

3A) Let R be a commutative ring. We say R is noetherian if every ideal in R is finitely generated.

(a) Show that R is noetherian if and only if the ideals in R satisfy the ascending chain condition.

(b) Do the ideals in a noetherian ring satisfy the descending chain condition? Prove or give a counter example.

Answer: (a) Assume that R has every ideal is finitely generated. Consider the ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Let

$$J = \bigcup_{i=1}^{\infty} I_i$$

Note first that J is an ideal as it is an ascending chain of ideals. J is finitely generated by say $x_1, ..., x_n$ by assumption. As $x_i \in J$ for all i, each i lies in one of the ideals in the chain, say I_{j_i}. Let $m = \max\{j_1, ..., j_n\}$. Then $x_i \in I_m$ for all i so the ideal they generate is contained in I_m, i.e. $J \subseteq I_m$. This implies that $M_m = N = M_k$ for all $k \geq m$ which proves the ACC.

(b) Take the ring of integers $\mathbb{Z}$. This is a noetherian ring. However consider the descending chain of ideals $2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq ... \supseteq 2^n\mathbb{Z} \supseteq \cdots$. This never terminates and thus does not satisfy the DCC (it is not artinian).

3B) Show that no principal ideal in the polynomial ring $\mathbb{Z}[x]$ can be a maximal ideal.
Answer: Assume that I is a principal ideal in $\mathbb{Z}[x]$, say $I = (f(x))$. If $\deg f > 0$ then clearly $p \notin (f(x))$ and thus $(f(x)) \subset (f(x), p) \neq \mathbb{Z}[x]$. If $\deg f = 0$ then say that f is the constant n. Then $\mathbb{Z}[x]/(n) \cong \mathbb{Z}_n[x]$ which is clearly not a field and thus not a maximal ideal.

4A) If $f(x) = x^3 - 17 \in \mathbb{Q}[x]$ show that the Galois group of $f(x)$ over $\mathbb{Q}$ is solvable but not abelian.
Answer: First note that f is irreducible by the Eisenstein criterion with $p = 17$. Thus G is a transitive subgroup of S_3. One root that we have is $17^{1/3}$ which is a degree 3 extension. What is missing are 3^{rd} roots of unity. This is a degree 2 extension. Thus $\mathbb{Q}\left(17^{1/3}, i\right)$ is a degree $3 \cdot 2 = 6$ extension and thus $G \cong S_3$. The group is nonabelian as $(12)(123) = (23) \neq (13) = (123)(12)$.
Now recall the definition of solvable. A group is called solvable if there is a chain of subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, ..., s-1$. (Or you can use the commutator definition in Grove).
We have that $A_3 \lhd S_3$ (as it is index 2) and as A_3 has size 3 it is abelian and thus have the sequence $1 \lhd A_3 \lhd S_3$.

4B) Let $L/\mathbb{Q}$ be a Galois extension with Galois group G, and let H be a subgroup of G. Let F be the fixed field of H. Show that there is a one-to-one correspondence between subfields of L which are isomorphic to F and conjugates of H in G.
Answer: If the intermediate field F corresponds to the subgroup H and σ is any automorphism in G, then the field $\sigma F = \{\sigma(x) : x \in F\}$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$. For this reason σF is called a conjugate subfield of F.

Proof: The fixed field of $\sigma H \sigma^{-1}$ is the set of all $x \in L$ such that $\sigma\tau\sigma^{-1}(x) = x$ for every $\tau \in H$. Thus

$$\left\{x \in L : \sigma^{-1}(x) \in \mathcal{F}(H)\right\} = \sigma(\mathcal{F}(H)).$$

5A) Let R be a commutative ring and let M and N be R-modules. Show that there is a natural isomorphism of R-modules

$$End_R(M \oplus N) \cong End_R(M) \oplus Hom_R(M, N) \oplus Hom_R(N, M) \oplus End_R(N)$$

and give a structure on the right hand side that makes this into an isomorphism of rings.
Answer: We first prove that $Hom_R(L, M \oplus N) \cong Hom_R(L, M) \oplus Hom_R(L, N)$ and then similarly it is true that $Hom_R(M \oplus N, L) \cong Hom_R(M, L) \oplus Hom_R(N, L)$ and then use $L = M \oplus N$. Let $\pi_1 : M \oplus N \to M$ be the natural projection from $M \oplus N$ to M and similarly π_2 be the natural projection to N. If $f \in Hom_R(L, M \oplus N)$ then the compositions $\pi_1 \circ f$ and $\pi_2 \circ f$ give elements in $Hom_R(L, M)$ and $Hom_R(L, N)$, respectively. This defines a map from $Hom_R(L, M \oplus N)$ to $Hom_R(L, M) \oplus Hom_R(L, N)$. You can verify for yourself that this is an R-module homomorphism. Conversely, given $f_1 \in Hom_R(L, M)$ and $f_2 \in Hom_R(L, N)$, define the map $f \in Hom_R(L, M \oplus N)$ by $f(d) = (f_1(d), f_2(d))$. This defines a map from $Hom_R(L, M) \oplus Hom_R(L, N)$ to $Hom_R(L, M \oplus N)$ that can be checked to see is a

homomorphism inverse to the map above, proving the isomorphism. Similarly we do the exact same thing to show that

$$Hom_R(M \oplus N, L) \cong Hom_R(M, L) \oplus Hom_R(N, L)$$

Using both of these we see that

$$\begin{aligned} Hom_R(M \oplus N, M \oplus N) &\cong Hom_R(M \oplus N, M) \oplus Hom_R(M \oplus N, N) \\ &\cong Hom_R(M, M) \oplus Hom_R(N, M) \oplus Hom_R(M, N) \oplus Hom_R(N, N) \\ &\cong End_R(M) \oplus Hom_R(M, N) \oplus Hom(N, M) \oplus End_R(N) \end{aligned}$$

To make this a ring isomorphism (using the fact that our ring is commutative) we simply define multiplication as composition of our maps.

5B) Let $R = \mathbb{Z}[x]$ and let M be the ideal $\langle 3, x \rangle$ in R viewed as an R-module. Show that M is not a free R-module.
Answer: Assume that M is a free R-module. Thus M has a basis. Assume that we pick a basis in $\langle 3, x \rangle$ of f. It is clear that there is some $r_1, r_2 \in R$ such that $r_1 f = 3$ and $r_2 f = x$. However f must have degree 1 and also be divisible by 3. This would implie that $f = 3g$ for some $g \in \mathbb{Z}[x]$ and therefore $r_2 3g = x$ which is not possible as 3 is not a unit in $\mathbb{Z}$. Thus a basis must have size at least 2. Assume that b_1 and b_2 are in the basis. Then $a_1 b_1 + a_2 b_2 = 3$ and $a_1' b_1 + a_2' b_2 = x$ for some $a_1, a_1', a_2, a_2' \in R$. Thus $a_1 x b_1 + a_2 x b_2 = 3x$ and $3a_1' b_1 + 3a_2 b_2 = 3x$ and thus $(a_1 x - 3a_1') b_1 + (a_2 x - 3a_2) b_2 = 0$. We need to show that one of the coefficients is not zero. Assume that $a_1 x = 3a_1'$. Then a_1 is a multiple of 3 as x does not divide 3 and 3 is prime in $\mathbb{Z}[x]$. Using a degree and divisibility argument show that one of the two is not zero.