January 2003
Algebra Qualifying Exams
Sample Solutions

1A) Suppose A and B are invertible complex $n \times n$ matrices and that $AB = cBA$ for some $c \in \mathbb{C}$. Show that $c^n = 1$.
Answer: Assume that $AB = cBA$. Then

$$\begin{aligned} \det(A)\det(B) &= \det(AB) = \det(cBA) = c^n \det(BA) \\ &= c^n \det(B)\det(A) = c^n \det(A)\det(B) \end{aligned}$$

and so $c^n = 1$.

1B) Prove or give a counterexample: if k is a field, n a positive integer and A an invertible $n \times n$ matrix with coefficients in k such that A^n is the identity matrix, then A is diagonalizable.
Answer: Counterexample. Consider the rational canonical form of a matrix with minimal polynomial $x^2 + x + 1$ over $\mathbb{R}$. This has no roots over $k = \mathbb{R}$ and we know that a matrix is diagonalizable if and only if its minimal polynomial has distinct roots over k. Thus look at the matrix

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

Just to check we see that

$$\begin{aligned} A^2 &= \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \\ A^3 &= \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

2A) Suppose G is a group, x is an element of finite order in G, and $p \in \mathbb{N}$ is a prime.Show that x can be written as a product $x = yz$, where y is a p-element and z is a p'-element, i.e. the order of y is a power of p and the order of z is relatively prime to p. Futher show that y and z are unique.
Answer: We generalize this problem and thus the result for 2A) is a special case of this:

Let x be an element of finte order n in a group G and let $n = p_1^{k_1} \cdots p_s^{k_s}$ where p_i are distinct primes. Then $x = x_1 x_2 \cdots x_s$ where x_i is a p_i-element of order $p_i^{k_i}$ and $x_i = x^{m_i}$ for some integer m_i $(i = 1, ..., s)$. Further, if $x = y_1 y_2 \cdots y_s$ where for $i, j = 1, ..., s$ we have that y_i is a p_i-element and $y_i y_j = y_j y_i$ then $y_i = x_i$.

Proof: Define $q_i = n/p_i^{k_i}$ for $i = 1, ..., s$. Since the gcd of all the q_i is 1 we can find integers m_i such that $q_1 m_1 + \cdots + q_s m_s = 1$. Write $x_i = x^{q_i m_i}$. Then x_i has order $p_i^{k_i}$ for $i = 1, ..., s$ and $x = x_1 \cdots x_s$.

To prove uniqueness we proceed as follows. By a simple induction argument we see that the order of the group $\langle y_2, y_3, ..., y_s \rangle = \langle y_2 \rangle \cdots \langle y_s \rangle$ is relatively prime to p_1 and so the intersection of this group with $\langle y_1 \rangle$ is 1. Since $1 = x^n = y_1^n y_2^n \cdots y_s^n$, we conclude that $y_1^n = 1$. Similarly, we see that the order of y_i divides n for $i = 1, ..., s$. It is then seen that $y_j^{q_i m_i}$ equals 1 if $i \neq j$ and equals y_i if $i = j$. Since $x = y_1 y_2 \cdots y_s$ we find $x_i = x^{q_i m_i} = y_i$ for $i = 1, ..., s$.

2B) Find the automorphism group of S_3, the symmetric group on 3 letters.
Answer: First we note that in general for a homomorphism we must have that elements of order n must be mapped to elements of order n. We also need a map with trivial kernel. Consider $G = S_3$ as the set $\{e, (12), (13), (23), (123), (132)\} = \langle (12), (123) \rangle$. We also know that e must be mapped to e. We also note that for each $g \in G$ the action of conjugation is an automorphism called an inner automorphism. Another helpful proposition is that $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$. Therefore we know that $Aut(G)$ is at least as big as S_3 as $Z(S_3) = e$.
The first automorphism that we always have is the identity automorphism φ_{id}. This maps $(12) \to (12)$. Then we can map $(12) \to (13)$ or $(12) \to (23)$. We can either fix (123) or send it to (132). Thus $Aut(S_3) \cong S_3$. In general, for $n \neq 6$, we have that $Aut(S_n) \cong S_n$.
We prove this as follows. First we prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e. for each $\sigma \in Aut(G)$ and each conjugacy class $\mathcal{K}$ of G the set $\sigma(\mathcal{K})$ is also a conjugacy

class of G. Then we let $\mathcal{K}$ be the conjugacy class of transpositions in S_n and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions. Next prove that for each $\sigma \in Aut(S_n)$ we must have $\sigma : (12) \to (a\ b_2)$ and $\sigma : (13) \to (a\ b_3)$, ..., $\sigma : (1\ n) \to (a\ b_n)$ for some distinct integers $a, b_2, ..., b_n \in \{1, 2, ..., n\}$. Now show that $(12), (13), ..., (1n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use the possible mapping choices to show that there are at most $n!$ automorphisms and thus $Aut(S_n) = Inn(S_n)$ for $n \neq 6$.
Another way to consider this problem is to note that $S_3 \cong SL_2(\mathbb{F}_2)$. Then all possible automorphisms of $SL_2(\mathbb{F}_2)$ are given by $SL_2(\mathbb{F}_2)$.

3A) Suppose R is a commutative ring with 1.
(a) Show that every maximal ideal M of R is prime.
(b) Show by example that R may have a prime ideal P that is not maximal.
Answer: (a) Let M be a maximal ideal. Then we have that R/M is simple and therefore as a ring R is simple if and only if R is a field, we know that R/M is a field. We also know that an ideal P is prime if and only if R/P is an integral domain. But as a field is an integral domain, we have that R/M is an integral domain and thus M is prime.
(b) Consider the commutative ring $\mathbb{Z}[x]$. We know that (x) is a prime ideal as $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an integral domain. However $\mathbb{Z}$ is not a field and thus (x) is not a maximal ideal. It is not maximal because for example it is contained in the maximal ideal $(2, x)$.

3B) Prove or give a counterexample. In a commutative ring R, the subset $I \subset R$ defined by $I = \{x \in R : x^2 = 0\}$ is an ideal.
Answer: Counterexample: To show it is an ideal we must show that for all $x_1, x_2 \in I$ and $r \in R$ we have that $x_1 + x_2 \in I$. But as $x^2 = 0$ we will have to look to a ring that is not an integral domain to find a counter example. Consider the ring $\mathbb{Z}[x, y]/(x^2, y^2)$. Then I has $x \in I$ and $y \in I$ but $x + y \in I$ as $(x + y)^2 = x^2 + 2xy + y^2$ is not zero in the quotient.

4A) Show that $f(x) = x^4 + 4$ is not irreducible over any field F. Determine its Galois group over over $\mathbb{Q}$ and also over the field $F = \mathbb{F}_8$ of 8 elements.
Answer: $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ which is true over any field. Then we find the roots of each equation.

$$\frac{-2 \pm \sqrt{4 - 8}}{2} \text{ and } \frac{2 \pm \sqrt{4 - 8}}{2}$$

Therefore over $\mathbb{Q}$ we only need adjoin i to $\mathbb{Q}$ and we get $G = \mathbb{Z}_2$.
Now we redo over $\mathbb{F}_8$. Recall that $\mathbb{F}_8 \cong \mathbb{F}_2/\langle x^3 + x + 1 \rangle$ as $\mathbb{F}_8 = \mathbb{F}_{2^3}$ is a degree 3 extension of $\mathbb{F}_2$. Thus the elements of $\mathbb{F}_8$ can be given as $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x + 1, x^2 + x\}$ subject to $x^3 + x + 1$. Note that $\mathbb{F}_8$ is a field of characteristic 2 and we have that $x^4 + 4 = x^4$ which splits completely. So the Galois group is trivial over $\mathbb{F}_8$ as it splits completely.

4B) Let $\alpha = e^{2\pi i/11}$.
(a) Show that α is an algebraic number.
(b) Show that $\mathbb{Q}(\alpha)$ is a Galois extension and find its Galois group.
Answer: (a) Consider the monic polynomial $x^{11} - 1$ with coefficients in $\mathbb{Z}$. We have that $\alpha^{11} - 1 = e^{2\pi i} - 1 = 1 - 1 = 0$. Therefore α is an algebraic number.
(b) An extension is a Galois extension if it is both normal and separable. If $f(x) \in F[x]$ is irreducible, the $f(x)$ is separable if and only if $f'(x) = 0$. Also, if $charF = 0$, then every polynomial is separable. As $f'(x) = 11x^{10}$ or as we note that $\mathbb{Q}$ has characteristic 0, we know that $f(x)$ is a separable polynomial. We could then easily show that it is normal. Or we note a corollary in Grove that states that if $charF = 0$ then K is Galois over F if and only if K is a splitting field over F for some set of polynomials in $F[x]$. As $\mathbb{Q}(\alpha)$ is a splitting field for α, we have that this extension is Galois.
Lastly, we know the roots of the irreducible polynomial $x^{10} + x^9 + \cdots + 1$ are $\alpha, ..., \alpha^{10}$. The extension is a degree 10 extension. Thus $|G| = 10$. Take $\alpha \to \alpha^2$ as a generator. The group G is therefore cyclic of order 10 and therefore $G \cong \mathbb{Z}_{10}$.

5A)suppose that A_1 and A_2 are finitely generated abelian groups, that A_1 has torsion subgroup of order m_1 and torsion free rank n_1 and that A_2 has torsion subgroup of order m_2 and torsion-free rank n_2. Determine the order of the torsion subgroup and torsion-free rank of $A_1 \otimes_Z A_2$.

Answer: The fundamental theorem of finitely generated abelian groups is as follows: Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, ..., n_s$ satisfying the following conditions:

(a) $r \geq 0$ and $n_j \geq 2$ for all j and

(b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.

Thus we can write A_1 as

$$A_1 \cong \mathbb{Z}^{n_1} \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s}$$

such that $\prod a_i = m_1$ and A_2 as

$$A_2 \cong \mathbb{Z}^{n_2} \times \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{b_t}$$

such that $\prod b_j = m_2$. We also know

$$\begin{aligned} A_1 \otimes_{\mathbb{Z}} A_2 &\cong \mathbb{Z}^{n_1} \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s} \otimes_{\mathbb{Z}} \mathbb{Z}^{n_2} \times \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{b_t} \\ &\cong \mathbb{Z}^{n_1} \otimes \mathbb{Z}^{n_2} \times \mathbb{Z}^{n_1} \otimes \mathbb{Z}_{b_1} \times \cdots \times \mathbb{Z}_{a_1} \otimes \mathbb{Z}_{b_1} \times \cdots \times \\ &\quad \mathbb{Z}_{a_s} \otimes \mathbb{Z}_{b_t} \end{aligned}$$

We know that each $\mathbb{Z}^{n_1} \otimes \mathbb{Z}_{b_i} = (\mathbb{Z}_{b_i})^{n_1}$ and $\mathbb{Z}_{a_j} \otimes \mathbb{Z}^{n_2} = \left(\mathbb{Z}_{a_j}\right)^{n_2}$. We also know that $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$ and so

$$\begin{aligned} \mathbb{Z}^{n_1} \otimes_{\mathbb{Z}} \mathbb{Z}^{n_2} &\cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n_1} \otimes \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n_2} \\ &\cong \underbrace{\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \times \cdots \times \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}}_{n_1 \cdot n_2} \\ &\cong \mathbb{Z}^{n_1 \cdot n_2} \end{aligned}$$

Thus the free rank is $n_1 \cdot n_2$.

For each a_i, b_j we know that $\mathbb{Z}_{a_i} \otimes_{\mathbb{Z}} \mathbb{Z}_{b_j} \cong \mathbb{Z}_{(a_i, b_j)}$. And thus the size of the torsion subgroup is

$$\prod_{i,j} (a_i, b_j) \cdot \prod a_i^{n_2} \cdot \prod b_j^{n_1}$$

5B) Let R be a commutative ring and suppose that you are given R-modules and R-module homomorphisms as in the diagram below:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle h_2} & & & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \longrightarrow & 0 \end{array}$$

Show that

(a) If there is a homomorphism $h_1 : M_1 \to N_1$ that makes the diagram commute, then there is a unique homomorphism $h_3 : M_3 \to N_3$ that makes it commute.

(b) If there is a homomorphism $h_3 : M_3 \to N_3$ that makes the diagram commute, then there is a unqiue homomorphism $h_1 : M_1 \to N_1$ that makes it commute.

Answer: (a) Assume there is such an h_1. Then we define h_3 as $g_2 h_2 f_2^{-1}$. We know that for all $m \in M_3$ there is an $m' \in M_2$ such that $f_2(m') = m$ as f_2 is surjective as the sequence is exact. We first show that this map is well-defined. Assume that there is m_1' and $m_2' \in M_2$ such that $f(m_1') = f(m_2') = m \in M_3$. We need to show that $g_2 h_2(m_1') = g_2 h_2(m_2')$. We know that $g_2 h_2(m_1' - m_2') = 0$ and so $m_1' - m_2' \in \ker(g_2 h_2)$. As $M_2 / \ker f_2 \cong M_3$ we know that our map is well-defined up to something in the kernel of f_2. Thus $m_1' = m_2' + x$, where $x \in \ker f_2$. Thus $x \in \operatorname{Im} f_1$ and as f_1 is one-to-one we take x' such that $f_1(x') = x$. Thus $g_2 h_2(x) = g_2 h_2 f_1(x') = g_2 g_1 h_1(x') = 0$ as the lower sequence is exact. Thus the map will be well-defined. Then that the diagram commutes is $h_3 f_2 = g_2 h_2 f_2^{-1} f_2 = g_2 h_2$.

(b) Assume there is such an h_3. We define h_1 as $g_1^{-1} h_2 f_1$. We need to make sure the map is well-defined by seeing if our choice of g_1^{-1} is well-defined. But as g_1 is one-to-one, we know that if $h_2 f_1 \in \operatorname{Im} g_1$ then the inverse is well-defined. If $h_2 f_1 \notin \operatorname{Im} g_1$ then $h_2 f_1 \in \ker g_2$ and so $g_2 h_2 f_1 \neq 0$ but by the commutativity with h_3 we know that $g_2 h_2 f_1 = h_3 f_2 f_1 = h_3 0 = 0$. Thus $h_2 f_1 \in \operatorname{Im} g_1$ and thus the map is well defined. Now we need only check that $g_1 h_1 = h_2 f_1$ and this follows as $g_1 h_1 = g_1 g_1^{-1} h_2 f_1 = h_2 f_1$.