Please justify all your answers, and label which solutions apply to which problems. We write \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) and \( \mathbb{F}_p \) for the integers, the rational numbers, the reals, the complex numbers and the field with \( p \) elements, respectively.

1. Show that the alternating group \( A_6 \) cannot act transitively on a set with 24 elements.

**Solution.** Suppose that the group \( G = A_6 \) acts transitively on a set \( X \) with 24 elements. Let \( x \in X \). Then the Stabilizer group \( G_x = \{ g \in G \mid g \cdot x = x \} \) has 360/24 = 15 elements. Groups with 15 elements are always commutative. The group \( G_x \) contains an element \( g \) of order 5 and an element \( h \) of order 3. The element \( g \) is a 5-cycle, and the element \( h \) is a 3-cycle or a product of two 3-cycles. The elements \( g \) and \( h \) cannot commute. Contradiction.

2. Let \( \text{Mat}_{2 \times 2}(\mathbb{C}) \) be the space of \( 2 \times 2 \) matrices with complex entries. Define a linear map \( L \) from \( \text{Mat}_{2 \times 2}(\mathbb{C}) \) to itself by \( L(X) = AX -XA \), where \( A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \). Compute the Jordan form of \( L \). (Your answer should be a \( 4 \times 4 \) matrix.)

**Solution.** We choose a basis of \( \text{Mat}_{2 \times 2}(\mathbb{C}) \): \( e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \), \( e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \), \( e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \), \( e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \).

The matrix of \( L \) with respect to this basis is:

\[
\begin{pmatrix}
0 & 0 & 1 & 0 \\
-1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

The matrix of \( L \) with respect to the basis \(-e_2, e_1, e_3, e_4\) is:

\[
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

which is in Jordan normal form.

3. Let \( R \) be the ring \( \mathbb{Z}[x]/(x^2 - 2) \). Which of the following ideals of \( R \) are prime: \( (0) \), \( (2) \), \( (3) \), \( (7) \)? Which are maximal?

**Solution.** We can define a surjective ring homomorphism \( \varphi : \mathbb{Z}[x] = \mathbb{Z} + \mathbb{Z}\sqrt{2} \) by sending \( x \) to \( \sqrt{2} \). This yields an isomorphism \( R = \mathbb{Z}[x]/(x^2 - 2) \cong \mathbb{Z}[\sqrt{2}] \). Since \( \mathbb{Z}[\sqrt{2}] \) is a domain, \( (0) \) is a prime ideal. However, \( \mathbb{Z}[\sqrt{2}] \) is not a field, so \( (0) \) is not maximal. The ideal \( (1) \) is the whole ring, and by definition this ideal is not maximal or prime. The ring \( R/(2) \cong \mathbb{Z}[x]/(x^2 - 2, 2) \cong \mathbb{F}_2[x]/(x^2) \) has a zero divisor, namely \( x \). So \( R/(2) \) is not a domain, and \( (2) \) is not prime or maximal. The ring \( R/(3) \cong \mathbb{Z}[x]/(x^2 - 2, 3) \cong \mathbb{F}_3[x]/(x^2 - 2) \) is a field because \( x^2 - 2 \) is irreducible over \( \mathbb{F}_3 \) (since it has no root). So \( (3) \) is maximal and prime. Finally, \( R/(7) \cong \mathbb{Z}[x]/(x^2 - 2, 7) \cong \mathbb{F}_7[x]/(x^2 - 2) \) is not a domain because \( (x - 3) \) is a zero divisor (\( (x - 3)(x + 3) = x^2 - 2 \) over \( \mathbb{F}_7 \)). So \( (7) \) is not prime or maximal.

4. Let \( p \) be prime and let \( a \) be a rational number which is not a \( p \)-th power. Show that \( z^p - a \) is irreducible over \( \mathbb{Q} \). (You may use that \( \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \), where \( \zeta_p \) is a nontrivial \( p \)-th root of unity.)
Solution. Let \( \alpha \) be a root of \( z^p - a \). Then the roots of \( z^p - a \) are \( \alpha, \zeta_p \alpha, \zeta_p^2 \alpha, \ldots, \zeta_p^{p-1} \alpha \).

Let \( G = \text{Gal}(\mathbb{Q}(\zeta_p, \alpha)/\mathbb{Q}) \). If \( g \) is an element of \( G \), then \( g \) sends \( \alpha \) to \( \alpha \zeta_p^B \) for some \( B \) and sends \( \zeta_p \) to \( \zeta_p^A \). Then \( g \) sends \( \zeta_p^x \alpha \) to \( \zeta_p^{Ax+B} \alpha \). So \( G \) is a subgroup of the group of all maps of the form \( x \mapsto Ax + B \) where \( A \in \mathbb{F}_p \) and \( B \in \mathbb{F}_p \).

There exists a nontrivial group homomorphism \( \varphi : G \to \mathbb{F}_p^\times \) that sends the map \( x \mapsto Ax + B \) to \( A \in \mathbb{F}_p^\times \). If the kernel of \( \varphi \) is trivial, then \( G \) is cyclic. Say \( G \) is generated by \( x \mapsto Ax + B \) where \( A \neq 0, 1 \). Then \( G \) fixes one element and \( z^p - a \) has a root in \( \mathbb{Q} \) which is not the case.

So \( G \) has a nontrivial kernel. This means that \( G \) contains a \( p \) cycle and \( G \) acts transitively on the roots. This implies that \( z^p - a \) is irreducible.

5. Let \( V \) be a finite dimensional vector space over an arbitrary field \( k \) and let \( A \) be an endomorphism of \( V \). Show that \( V \) can be uniquely written as \( V_0 \oplus V_1 \) where \( A(V_0) \subseteq V_0 \), \( A(V_1) \subseteq V_1 \), \( A|_{V_0} \) is nilpotent and \( A|_{V_1} \) is invertible. (\( A|_{V_0} \) and \( A|_{V_1} \) are the restrictions of \( A \) to \( V_0 \) and \( V_1 \) respectively.)

Solution. Let \( n \) be the dimension of \( V \), and define \( V_0 \) and \( V_1 \) as the kernel and image of \( A^n \) respectively. It is clear that \( A(V_0) \subseteq V_0 \) and \( A(V_1) \subseteq V_1 \) and that \( A|_{V_0} \) is nilpotent. We claim that kernel of \( A^m \) is equal to \( V_0 \) for all \( m > n \). If \( p(X) \) is the characteristic polynomial of \( A \), then the ideal \((p(X), X^m)\) in \( k[X] \) is equal to \((X^l)\) for some \( l \) and \( l \leq n \) because \( p(X) \) has degree \( n \). It follows that \( X^n \in (p(X), X^m) \) and we can write \( X^n = f(X)p(X) + g(X)X^m \). If we plug in \( X = A \) and use Cayley-Hamilton, then we have \( A^n = f(A)p(A) + g(A)A^m = g(A)A^m \). Now it is clear that the kernel of \( A^m \) is contained in \( V_0 \). Suppose that \( v \in V_1 \cap V_0 \). Then we can write \( v = A^n(w) \) for some \( w \in V \) and \( A^n(v) = A^2n(w) = 0 \). It follows that \( v = A^n(w) = 0 \). So \( V_1 \cap V_0 = \{0\} \). Since \( V_1 \cong V/V_0 \), we have \( \dim V_0 + \dim V_1 = \dim V \). It follows that \( V = V_0 \oplus V_1 \). Any element of the kernel of \( A|_{V_1} \) lies in \( V_0 \cap V_1 \) so \( A|_{V_1} \) has trivial kernel and is therefore invertible.
QR Exam Algebra, September 2014, Afternoon

Please justify all your answers, and label which solutions apply to which problems.

1. Set

\[ M = \begin{pmatrix} 2 & 4 & 10 \\ 1 & 3 & 7 \\ 1 & 1 & 15 \end{pmatrix}. \]

Let \( G \) be the abelian group \( \mathbb{Z}^3/M\mathbb{Z}^3 \). (The quotient of \( \mathbb{Z}^3 \) by the image of the map \( M \).)

Write \( G \) as a direct sum of cyclic groups of prime power order.

**Solution.**

Using elementary row/column operations:

\[
\begin{pmatrix} 2 & 4 & 10 \\ 1 & 3 & 7 \\ 1 & 1 & 15 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 3 & 7 \\ 2 & 4 & 10 \\ 1 & 1 & 15 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 3 & 7 \\ 0 & -2 & -4 \\ 0 & -2 & 8 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 12 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 12 \end{pmatrix}
\]

This is the Smith normal form. So the invariant factors are 4, 2, 3, and the elementary divisors are 2, 4, 3. We have \( \mathbb{Z}^3/M\mathbb{Z}^3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \).

2. Let \( \alpha \) and \( \beta \) be algebraic numbers of degrees \( a \) and \( b \) over \( \mathbb{Q} \).

(a) If \( \mathbb{Q}(\alpha)/\mathbb{Q} \) and \( \mathbb{Q}(\beta)/\mathbb{Q} \) are Galois, show that \( [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \) divides \( ab \).

(b) Show that \( [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \) need not divide \( ab \) without the hypothesis that \( \mathbb{Q}(\alpha)/\mathbb{Q} \) and \( \mathbb{Q}(\beta)/\mathbb{Q} \) are Galois.

**Solution.**

(a) The composite field extension \( \mathbb{Q}(\alpha, \beta) : \mathbb{Q} \) is also Galois. Let \( G, G_\alpha, G_\beta \) be the Galois groups of \( \mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha), \mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta) \) and \( \mathbb{Q}(\alpha, \beta) : \mathbb{Q} \) respectively. Let \( c \) be the number of elements of \( G \), which is also the degree of the extension \( \mathbb{Q}(\alpha, \beta) : \mathbb{Q} \). Since \( \mathbb{Q}(\alpha) : \mathbb{Q} \) is Galois, \( G_\alpha \subseteq G \) is normal, and \( G/G_\alpha \) is the Galois group of \( \mathbb{Q}(\alpha) : \mathbb{Q} \). It follows that \( G/G_\alpha \) has \( a \) elements, and \( G_\alpha \) has \( c/a \) elements. Similarly, \( G_\beta \) has \( c/b \) elements. Since \( \mathbb{Q}(\alpha, \beta) \) is the composition of \( \mathbb{Q}(\alpha) \) and \( \mathbb{Q}(\beta) \) we have \( G_\alpha \cap G_\beta = \{e\} \). It follows that \( G_\alpha G_\beta \) is a subgroup of \( G \) with \( (c/a) \cdot (c/b) \) elements. So \( (c/a) \cdot (c/b) \) divides \( c \) and therefore \( c \) divides \( ab \).

(b) Let \( \alpha \) and \( \beta \) be two distinct roots of the irreducible polynomial \( X^3 - 2 \). Then we have \( a = b = 3 \), and the degree of \( \mathbb{Q}(\alpha, \beta) : \mathbb{Q} \) is 6.

3. Suppose that \( n \geq 2 \) and \( A \) is a complex \( n \times n \) matrix.

(a) Show that there exists a linear map \( L : \mathbb{C}^n \to \mathbb{C}^n \) such that \( L(v \wedge w) = Av \wedge w + v \wedge Aw \).

(b) Prove that if \( A \) is skew-symmetric, then \( L \) is not invertible.

**Solution.**

(a) Define \( \Theta : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n \) by \( \Theta(v, w) = Av \wedge w + v \wedge Aw \). Then \( \Theta \) is bilinear, and

\[
\Theta(w, v) = Aw \wedge v + w \wedge Av = -v \wedge Aw - Av \wedge w = -\Theta(w, v).
\]
This shows that $\Theta$ is alternating. By the universal property, there exists a unique linear map $L : \bigwedge^2(C^n) \to \bigwedge^2(C^n)$ such that $L(v \wedge w) = \Theta(v, w)$.

(b) Suppose that $A$ is skew-symmetric. Suppose that $\lambda \neq 0$ is an eigenvalue of $A$. Then $A^t = -A$ also has an eigenvalue $\lambda$, and $A$ has an eigenvalue $-\lambda$. If $v$ and $w$ are eigenvectors for the eigenvalues $\lambda$ and $-\lambda$ respectively, then we have

$$L(v \wedge w) = Av \wedge w + v \wedge Aw = \lambda(v \wedge w) - \lambda(v \wedge w) = 0.$$  

Now $v$ and $w$ are linearly independent, so $v \wedge w \neq 0$ and we conclude that $L$ has a nontrivial kernel. The other case is where the only eigenvalue of $A$ is 0. Then $A$ is nilpotent. If $A = 0$ then $L = 0$ and is not invertible. Otherwise, there exists a vector $v$ with $A^2v = 0$ and $Av \neq 0$. Let $w = Av$. Then $v$ and $w$ are linearly independent because $Av \neq 0$ and $Aw = 0$. So $v \wedge w \neq 0$ and

$$L(v \wedge w) = Av \wedge w + v \wedge Aw = w \wedge w + v \wedge 0 = 0.$$  

Again, $L$ has a nontrivial kernel.

4. Show that a group of order 140 has a normal subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Solution.

Suppose that $G$ is a group of order 140. The number of 5-Sylow subgroups divides $140/5 = 28$ and is congruent to 1 modulo 5. It follows that there is a unique 5-Sylow subgroup $H_5 \cong \mathbb{Z}/5\mathbb{Z}$. The number of 7-Sylow subgroups divides $140/7 = 20$ and is congruent to 1 modulo 7. It follows that there is a unique 7 Sylow subgroup $H_7 \cong \mathbb{Z}/7\mathbb{Z}$. Clearly, $H_5 \cap H_7$ is not equal to $H_5$, so $H_5 \cap H_7$ is trivial. So $H_5H_7$ is a group of order 35, and $H_7$ is a normal subgroup. The automorphism group of $H_7$ has order 6, so $H_5$ can only act trivially on $H_7$. This shows that $H_5H_7 \cong H_5 \times H_7 \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

5. Let $p$ be an odd prime. Let $f(x)$ be an irreducible polynomial of degree $p$ with rational coefficients whose splitting field has Galois group the dihedral group of order $2p$. Show that $f$ has either all real roots or precisely one real root.

Solution. Let $D$ be the Galois group of the splitting field of $f(x)$. Let $\sigma$ denote complex conjugation. Since $\sigma^2 = \text{Id}$, either $\sigma$ has order 1 or 2 as an element of $D$. If $\sigma$ has order 1, then all roots of $f$ are fixed by $\sigma$, hence real, and we are done. Suppose, then that $\sigma$ has order 2. Choose a root $\beta$ of $D$ and let its stabilizer be $H$. Then the stabilizers of the various roots of $f$ are the conjugates of $H$. Each order 2 element of $D$ lies in precisely one such conjugate, so $\sigma$ fixes exactly one root of $f$, as desired.