Test 1 - Solutions

1. *Let M be a left R-module where R is a commutative ring with 1. For $r \in R$, define $\varphi_r : M \to M$ by $\varphi_r(m) = rm$.*

   (a) *Prove that φ_r is a R-module homomorphism.*
   For all $x, y \in M$ and $s \in R$,

   $$\varphi_r(x + sy) = r(x + sy) = rx + rsy = rx + sry = \varphi_r(x) + s\varphi_r(y).$$

   Note, we used that R is commutative in the step using $rs = sr$.

   (b) *Prove that $\psi : R \to End(M)$ given by $\psi(r) = \varphi_r$ is ring homomorphism.*
   For all $r, s \in R$ and $m \in M$,

   $$\begin{aligned}\psi(r+s)(m) &= \varphi_{r+s}(m)\\ &= (r+s)m\\ &= rm + sm\\ &= \varphi_r(m) + \varphi_s(m)\\ &= (\varphi_r + \varphi_s)(m)\\ &= (\psi(r) + \psi(s))(m)\end{aligned}$$

   So, $\psi(r + s) = \psi(r) + \psi(s)$.
   Also,

   $$\begin{aligned}\psi(rs)(m) &= \varphi_{rs}(m)\\ &= (rs)m\\ &= \varphi_r(sm)\\ &= \varphi_r(\varphi_s(m))\\ &= (\varphi_r \circ \varphi_s)(m)\end{aligned}$$

   So, $\psi(rs) = \psi(r)\psi(s)$. Thus, ψ is a ring homomorphism.

   (c) *Prove that for all $r \in R$, $rM = \{rm \mid m \in M\}$ is a submodule of M.*
   Since $rM = \phi_r(M)$, it is the image of a module homomorphism, so it is a submodule of M.

   (d) *Suppose $e \in R$ such that $e^2 = e$, and M be a left R module. Prove*

   $$M = eM \oplus (1 - e)M.$$

   By the previous part, both eM and $(1 - e)M$ are submodules of M. Now for all $m \in M$, $m = em + 1m - em = em + (1 - e)m$, thus $eM + (1 - e)M = M$. To see that the sum is direct, suppose $m \in eM \cap (1 - e)M$. Then $m = ex$ and $m = (1 - e)y$ for some $x, y \in M$. But, on one hand, $em = e(ex) = e^2x = ex = m$. On the other hand

   $$em = e(1 - e)y = (e - e^2)y = 0y = 0.$$

   Thus, $m = em = 0$. So, $M = eM \oplus (1 - e)M$.

2. *Consider 9×9 matrices over $\mathbf{Q}$, up to conjugation, with minimal polynomial*

$$f = x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1 = (x^2+1)^2(x+1)^2.$$

Determine the possible rational canonical forms, and for each, give its characteristic polynomial.

The minimal polynomial gives one invariant factor, and here it is a 6 by 6 block. The rest can either be a single 3×3 block, and 2×2 and a 1×1, or three 1×1 blocks. Each block is a companion matrix of a polynomial dividing the minimal polynomial. In the first case, we need a cubic factor of f, and there is only one: $(x^2+1)(x+1)$. In the second case, we need a quadratic and a linear factor, but the linear factor has to divide the quadratic one, so they must be $(x+1)^2$ and $x+1$. In the last case, all of the blocks correspond to linear factors, so each is $x+1$.

We will write C_g for the companion matrix of g, so

$$C_f = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix} \qquad C_{(x+1)^2} = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix} \qquad C_{x+1} = \begin{pmatrix} -1 \end{pmatrix}$$

The the possibilities for the rational canonical forms (in block form) and their characteristic polynomials are:

Matrix	**Char. polynomial**
$\begin{pmatrix} C_f & 0 \\ 0 & C_{(x^2+1)(x+1)} \end{pmatrix}$	$f \cdot (x^2+1)(x+1)$
$\begin{pmatrix} C_f & 0 & 0 \\ 0 & C_{(x+1)^2} & 0 \\ 0 & 0 & C_{x+1} \end{pmatrix}$	$f \cdot (x+1)^3$
$\begin{pmatrix} C_f & 0 & 0 & 0 \\ 0 & C_{x+1} & 0 & 0 \\ 0 & 0 & C_{x+1} & 0 \\ 0 & 0 & 0 & C_{x+1} \end{pmatrix}$	$f \cdot (x+1)^3$

3. *Suppose F is a subfield of K, $f \in F[x]$ irreducible and $\alpha, \beta \in K$ such that $f(\alpha) = f(\beta) = 0$. Prove that there exists an isomorphism $\phi : F(\alpha) \to F(\beta)$ such that $\phi(\alpha) = \beta$ and $\phi(a) = a$ for all $a \in F$.*

If $c \in F^*$ is the leading coefficient of f, then $c^{-1}f$ is monic and we have $c^{-1}f(\alpha) = 0$ and $c^{-1}f(\beta) = 0$, so we can replace f by the monic irreducible polynomial $c^{-1}f$.

We have an isomorphism $\psi_1 : F[x]/\langle f \rangle \to F(\alpha)$ induced by the evaluation homomorphism at α. Writing $\bar{a}$ for the coset $a + \langle f \rangle$, this map satisfies $\psi_1(\bar{b}) = b$ for all $b \in F$ and $\psi_1(\bar{x}) = \alpha$.

Similarly, we have the isomorphism $\psi_2 : F[x]/\langle f \rangle \to F(\beta)$ induced by the evaluation homomorphism at β satisfying $\psi_2(\bar{b}) = b$ for all $b \in F$ and $\psi_2(\bar{x}) = \beta$. Then $\phi = \psi_2 \circ \psi_1^{-1}$ is the desired isomorphism.

4. *For each part, say whether or not the given value is constructable (by the standard straightedge and compass rules), and briefly justify your answer.*

   (a) $\sqrt[4]{5}$

   This is constructable since 5 is constructable, so $\sqrt{5}$ is constructable, so $\sqrt{\sqrt{5}} = \sqrt[4]{5}$ is constructable.

   (b) $\sqrt[5]{6}$

   This is not constructable. It is a root of $x^5 - 6$ which is irreducible by Eisenstein's criterion with $p = 2$ (or $p = 3$). Since its degree 5, is not a power of 2, the roots are not constructable.

   (c) π^2

   This is not constructable. If π^2 was constructable, then $\pi = \sqrt{\pi^2}$ would be constructable, but π is not algebraic over $\mathbf{Q}$.

   (d) $\frac{\sqrt{2+\sqrt{3}}}{5}$

   This is constructable because it can be produced by a sequence of field operations and taking square roots.

5. *Suppose $m \in \mathbf{Z}^+$ is odd and $m > 1$. Prove*

$$\Phi_{2m}(x) = \Phi_m(-x)$$

   where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial.

   Suppose ζ is a primitive mth root of unity. We note that $-\zeta$ is a primitive $2m$th root of unity. This follows since $\mathbf{C}^*$ is an abelian group, ζ has order m, -1 has order 2, and $\gcd(m, 2) = 1$ since m is odd.

   Thus, if ζ is a root of $\Phi_m(x)$, then $-\zeta$ is a root of $\Phi_{2m}(x)$. But

$$\begin{aligned} \deg(\Phi_{2m}) &= \phi(2m) \\ &= \phi(2)\phi(m) && \text{because } m \text{ is odd} \\ &= \phi(m) \\ &= \deg(\Phi_m) \end{aligned}$$

   So, the roots of Φ_{2m} are the $\phi(m)$ values $-\zeta$ where ζ is a root of Φ_m. Thus,

$$\Phi_{2m}(x) = \prod_{\substack{\zeta \in \mathbf{C} s.t. \\ \Phi_m(\zeta)=1}} x - (-\zeta) = (-1)^{\phi(m)} \prod_{\substack{\zeta \in \mathbf{C} s.t. \\ \Phi_m(\zeta)=1}} -x - \zeta = (-1)^{\phi(m)} \Phi_m(-x)$$

   So it suffices to show that for $m \geq 3$, $\phi(m)$ is even. If m is divisible by an odd prime p, then $(p-1) \mid \phi(m)$ and $p - 1$ is even, so $\phi(m)$ is even. Otherwise, $m = 2^j$ for some $j \geq 2$, so $\phi(m) = 2^{j-1}$ which is even.

6. *Suppose K is a finite degree extension field of F with $[K : F]$ relatively prime to 6. Prove that for all $a \in K$, $F(a) = F(a^3)$.*

   Note that a is a root of $x^3 - a^3 \in F(a^3)[x]$, so its minimum polynomial $m(x)$ over $F(a^3)$ divides this.

We have $F \subseteq F(a^3) \subseteq F(a) \subseteq K$, so the degrees multiply implying $[F(a) : F(a^3)]$ divides $[K : F]$. Thus, $[F(a) : F(a^3)]$ is also relatively prime to 6. But $[F(a) : F(a^3)] = \deg(m)$, so $\deg(m)$ cannot be 2 or 3, forcing it to be 1. Thus $[F(a) : F(a^3)] = 1$, which implies $F(a) = F(a^3)$.