IMSC 2048 — Practice Final Examination Solutions

Question 1 (10 marks)

(a) The leading principal minors of $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$ are:

- $\Delta_1 = \det(2) = 2 > 0$
- $\Delta_2 = \det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = 4 - 1 = 3 > 0$
- $\Delta_3 = \det(A) = 2(4-1) - 1(2-0) + 0 = 6 - 2 = 4 > 0$

By Sylvester's criterion, since all leading principal minors are positive, β is positive definite.

(b) Let $\{v_1, v_2, v_3\}$ be the orthogonal basis before normalization. We use Gram–Schmidt with the inner product $\beta(x, y) = x^T A y$.

$$v_1 = e_1. \quad \beta(v_1, v_1) = 2.$$
$$v_2 = e_2 - \frac{\beta(e_2, v_1)}{\beta(v_1, v_1)} v_1 = (0,1,0)^T - \frac{1}{2}(1,0,0)^T = \left(-\frac{1}{2}, 1, 0\right)^T.$$

Calculate $\beta(v_2, v_2) = v_2^T A v_2 = 2(-\frac{1}{2})^2 + 2(1)^2 + 2(-\frac{1}{2})(1)(1) = \frac{1}{2} + 2 - 1 = \frac{3}{2}$.

$$v_3 = e_3 - \frac{\beta(e_3, v_1)}{\beta(v_1, v_1)} v_1 - \frac{\beta(e_3, v_2)}{\beta(v_2, v_2)} v_2.$$

We have $\beta(e_3, v_1) = 0$. $\beta(e_3, v_2) = (0,0,1)A(-\frac{1}{2}, 1, 0)^T = (0,1,2)(-\frac{1}{2}, 1, 0)^T = 1$.

$$v_3 = (0,0,1)^T - 0 - \frac{1}{3/2}\left(-\frac{1}{2}, 1, 0\right)^T = (0,0,1)^T - \left(-\frac{1}{3}, \frac{2}{3}, 0\right)^T = \left(\frac{1}{3}, -\frac{2}{3}, 1\right)^T.$$

Calculate $\beta(v_3, v_3) = v_3^T A v_3 = \frac{1}{9}(1,-2,3)A(1,-2,3)^T = \frac{1}{9}(1,-2,3)(0,0,4)^T = \frac{12}{9} = \frac{4}{3}$.

Normalizing these vectors yields the orthonormal basis $\{f_1, f_2, f_3\}$:

$$f_1 = \frac{v_1}{\sqrt{2}} = \left(\frac{1}{\sqrt{2}}, 0, 0\right)^T$$
$$f_2 = \frac{v_2}{\sqrt{3/2}} = \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, 0\right)^T$$
$$f_3 = \frac{v_3}{\sqrt{4/3}} = \left(\frac{1}{2\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{\sqrt{3}}{2}\right)^T.$$

Question 2 (10 marks)

(a) Is β nondegenerate? Consider the determinant of B. Note that B acts on pairs (x_1, x_3) and (x_2, x_4) independently. Reordering basis elements to e_1, e_3, e_2, e_4, the matrix becomes block diagonal with two equal blocks $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Since $\det \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = -2$, the determinant of B is $(-2) \times (-2) = 4$. Because $\det(B) \neq 0$, the form β is non-degenerate.

(b) Let $x = (x_1, x_2, x_3, x_4)^T$. We write $\beta(x, x) = x^T B x$:

$$\begin{aligned} \beta(x, x) &= x_1^2 + 2x_1x_3 - x_3^2 + x_2^2 + 2x_2x_4 - x_4^2 \\ &= (x_1^2 + 2x_1x_3 + x_3^2) - 2x_3^2 + (x_2^2 + 2x_2x_4 + x_4^2) - 2x_4^2 \\ &= (x_1 + x_3)^2 - 2x_3^2 + (x_2 + x_4)^2 - 2x_4^2. \end{aligned}$$

Using the change of variables $y_1 = x_1 + x_3$, $y_2 = \sqrt{2}x_3$, $y_3 = x_2 + x_4$, $y_4 = \sqrt{2}x_4$, we have $\beta(y) = y_1^2 - y_2^2 + y_3^2 - y_4^2$. The positive index of inertia is $p = 2$ and the negative index of inertia is $q = 2$. The signature is $(2, 2)$.

(c) Let $W \subseteq V$ be a subspace such that $\beta(w, w) = 0$ for all $w \in W$. We want to find the maximal dimension of W. Let $U_+ \subset V$ be the given 2-dimensional subspace corresponding to coordinates y_1, y_3 (i.e. where $y_2 = y_4 = 0$). For any non-zero vector $u \in U_+$, we have $\beta(u, u) = y_1^2 + y_3^2 > 0$. Since $\beta(w, w) = 0$ for all $w \in W$, the intersection $W \cap U_+$ must be the trivial subspace $\{0\}$. By the dimension formula, $\dim(W + U_+) = \dim W + \dim U_+ - \dim(W \cap U_+) = \dim W + 2$. Since $W + U_+$ is a subspace of V (which has dimension 4), we have $\dim W + 2 \leq 4$, which implies $\dim W \leq 2$.

To show that dimension 2 is attainable, consider the subspace defined by $y_1 = y_2$ and $y_3 = y_4$. It is spanned by two linearly independent vectors: w_1 (with y-coordinates $(1, 1, 0, 0)$) and w_2 (with y-coordinates $(0, 0, 1, 1)$). For any vector $w = aw_1 + bw_2 \in \operatorname{span}\{w_1, w_2\}$, its y-coordinates are (a, a, b, b), and giving:

$$\beta(w, w) = a^2 - a^2 + b^2 - b^2 = 0.$$

Thus, the maximal dimension is exactly 2.

Question 3 (15 marks)

(a) The conjugacy classes of $D_4 = \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$ are: $\{e\}$ (size 1), $\{r^2\}$ (size 1), $\{r, r^3\}$ (size 2), $\{s, sr^2\}$ (size 2), and $\{sr, sr^3\}$ (size 2).

(b) Since there are 5 conjugacy classes, there are exactly 5 irreducible representations of D_4, say $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$. The sum of the squares of their dimensions is 8. Thus, $1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8$. There are four 1-dimensional representations. We factor modulo the commutator subgroup $[D_4, D_4] = \langle r^2 \rangle$. The abelianization $D_4/\langle r^2 \rangle \cong V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which gives the four 1-dimensional representations. The final one is the 2-dimensional geometric representation acting on the square.

Character table of D_4:

Class	$\{e\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, sr^2\}$	$\{sr, sr^3\}$
Size	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Row orthogonality for χ_1 and χ_5:

$$\frac{1}{8}\sum_{g \in G} \chi_1(g)\overline{\chi_5(g)} = \frac{1}{8}\left(1(1)(2) + 1(1)(-2) + 2(1)(0) + 2(1)(0) + 2(1)(0)\right) = \frac{2-2}{8} = 0.$$

(c) The subgroup $H = \langle r \rangle \cong C_4$ has exactly 4 elements and 4 conjugacy classes, so 4 irreducible 1-dimensional representations (characters $\rho_k(r) = i^k$). Values of the restricted characters on $\{e, r, r^2, r^3\}$:

- $\text{Res}(\chi_1) = (1, 1, 1, 1) = \rho_0$
- $\text{Res}(\chi_2) = (1, 1, 1, 1) = \rho_0$
- $\text{Res}(\chi_3) = (1, -1, 1, -1) = \rho_2$
- $\text{Res}(\chi_4) = (1, -1, 1, -1) = \rho_2$
- $\text{Res}(\chi_5) = (2, 0, -2, 0) = \rho_1 + \rho_3$

Verification for χ_5: $\rho_1(h) + \rho_3(h)$ gives values $(1 + 1, i + (-i), -1 + (-1), -i + i) = (2, 0, -2, 0)$, matching exactly.

Question 4 (15 marks)

(a) Let χ be an irreducible character of an abelian group G. For any abelian group, all irreducible representations have dimension 1. Thus $\chi(e) = 1$. Also, characters take values in roots of unity since $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(e) = 1$. Therefore, for any $g \in G$, $|\chi(g)| = 1 = \chi(e)$. Hence $Z(\chi) = G$.

(b) For any finite group G, let $n = \chi(e)$ be the dimension of the representation. By column orthogonality on the column $\{e\}$:

$$\sum_{\psi \text{ irrep}} |\psi(e)|^2 = |G|$$

However, we are specifically dealing with the sum over group elements for a single character via inner product:

$$\langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = 1$$

Break the sum into two parts: $g \in Z(\chi)$ and $g \notin Z(\chi)$.

$$|G| = \sum_{g \in Z(\chi)} |\chi(g)|^2 + \sum_{g \notin Z(\chi)} |\chi(g)|^2$$

For $g \in Z(\chi)$, by definition $|\chi(g)| = \chi(e)$. There are $|Z(\chi)|$ such elements. Hence $\sum_{g \in Z(\chi)} |\chi(g)|^2 = |Z(\chi)|\chi(e)^2$. For $g \notin Z(\chi)$, $|\chi(g)| \geq 0$, so $\sum_{g \notin Z(\chi)} |\chi(g)|^2 \geq 0$. Therefore, $|G| \geq |Z(\chi)|\chi(e)^2$. Rearranging gives:

$$\chi(e)^2 \leq \frac{|G|}{|Z(\chi)|} = [G : Z(\chi)].$$

(c) Based on the equation from (b):

$$|G| = |Z(\chi)|\chi(e)^2 + \sum_{g \notin Z(\chi)} |\chi(g)|^2$$

For equality $\chi(e)^2 = [G : Z(\chi)]$ (or equivalently $|G| = |Z(\chi)|\chi(e)^2$) to hold, we must have the remainder term be exactly zero:

$$\sum_{g \notin Z(\chi)} |\chi(g)|^2 = 0$$

Since $|\chi(g)|^2 \geq 0$ for all terms, the sum is zero if and only if each individual term is zero. That is, $|\chi(g)|^2 = 0 \implies \chi(g) = 0$ for all $g \in G \setminus Z(\chi)$.

Question 5 (10 marks)

(a) $F = \mathbb{F}_3(t)$, $K = F[x]/(x^3 - t)$. The minimal polynomial of $\alpha = t^{1/3}$ is $x^3 - t$. It is irreducible over F (Eisenstein or no roots). So $[K : F] = 3$. In characteristic 3, the derivative is $3x^2 = 0$. Hence $x^3 - t = (x - \alpha)^3$. The polynomial has multiple roots. The only root α belongs to K, and generates K. Since the minimal polynomial has repeated roots, the extension is **inseparable**. Since K is the splitting field of $x^3 - t$, it is **normal**. But because it is inseparable, it is **not Galois**.

(b) $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[4]{2})$. The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$, which is irreducible by Eisenstein's criterion ($p = 2$). So $[K : F] = 4$. Since the base field has characteristic 0, all irreducible polynomials are separable. So K/F is **separable**. The roots of $x^4 - 2$ are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. Since $K \subset \mathbb{R}$, K does not contain polynomial roots $i\sqrt[4]{2}$. Hence the extension is **non-normal**. Therefore, it is **not Galois**.

(c) $F = \mathbb{Z}/p\mathbb{Z}$, $K = F[x]/(x^p - x + 1)$. The polynomial $f(x) = x^p - x + 1$ is an Artin–Schreier polynomial. Over $\mathbb{F}_p$, its derivative $f'(x) = -1 \neq 0$, so it has no multiple roots. It is **separable**. Furthermore, for any root α, $\alpha + 1$ is also a root: $(\alpha + 1)^p - (\alpha + 1) + 1 = \alpha^p + 1 - \alpha - 1 + 1 = \alpha^p - \alpha + 1 = 0$. Thus all roots are $\alpha, \alpha + 1, \ldots, \alpha + p - 1$, all of which belong to $F(\alpha)$. Thus K is the splitting field of f, making it **normal**. Being both normal and separable, it is **Galois**. Notice f has no roots in $\mathbb{F}_p$ (Fermat's little theorem $b^p = b$, so $b^p - b + 1 = 1 \neq 0$). In fact f is irreducible over $\mathbb{F}_p$. So $[K : F] = p$.

Question 6 (10 marks)

(a) The minimal polynomial of a primitive n-th root of unity ζ_n over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_n(x)$. For $n = 8$, we can compute it using $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. The roots of $x^4 - 1$ are 4-th roots of unity, so primitive 8-th roots are roots of $x^4 + 1$. Thus the minimal polynomial is $\Phi_8(x) = x^4 + 1$. The degree is $[K : \mathbb{Q}] = \deg(\Phi_8) = 4$.

(b) A splitting field of $x^8 - 1$ must contain all its roots. The roots are ζ_8^k for $k = 0, 1, \ldots, 7$. All these roots are contained in $K = \mathbb{Q}(\zeta)$ since they are powers of ζ. And since K is generated by one of these roots, it's the minimal field containing all roots. Thus K is the splitting field. Since char $= 0$, extensions are separable; as a splitting field it is normal. Thus $K/\mathbb{Q}$ is a Galois extension.

(c) Since $[K : \mathbb{Q}] = 4$, the Galois group has order 4. An automorphism σ is determined by its action on the generator ζ, mapping it to another primitive root ζ^a where $\gcd(a, 8) = 1$. The possibilities are $a \in \{1, 3, 5, 7\}$. Thus we have:

- $\sigma_1 : \zeta \mapsto \zeta$ (identity)
- $\sigma_3 : \zeta \mapsto \zeta^3$
- $\sigma_5 : \zeta \mapsto \zeta^5 = -\zeta$
- $\sigma_7 : \zeta \mapsto \zeta^7 = \zeta^{-1} = -\zeta^3$ (using $\zeta^4 = -1$)

Each element (except identity) is order 2 since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. Thus the group has the property that every non-identity element has order 2. This implies $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (the Klein four-group).

Question 7 (15 marks)

(a) Since $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the degree of the extension is $|G| = 4$. The group has three subgroups of order 2. By Galois correspondence, there are three distinct intermediate fields exactly of degree 2 over $\mathbb{Q}$. A quadratic extension of $\mathbb{Q}$ must be of the form $\mathbb{Q}(\sqrt{a})$ where a is a non-square rational. Pick two of these intermediate fields, say $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$. Then K must contain both, so $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq K$. But since $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$ and the two fields are distinct ($\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$), we have $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = 2$, yielding total degree 4. Thus $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

(b) The elements of G permute the roots of the minimal polynomials. The minimal polynomial of $\sqrt{a}$ is $x^2 - a$, roots $\pm\sqrt{a}$. The minimal polynomial of $\sqrt{b}$ is $x^2 - b$, roots $\pm\sqrt{b}$. Each automorphism maps $\sqrt{a} \mapsto \pm\sqrt{a}$ and $\sqrt{b} \mapsto \pm\sqrt{b}$. The 4 automorphisms correspond to the 4 choices of signs:

- $id : (\sqrt{a}, \sqrt{b}) \mapsto (\sqrt{a}, \sqrt{b})$
- $\sigma_1 : (\sqrt{a}, \sqrt{b}) \mapsto (-\sqrt{a}, \sqrt{b})$
- $\sigma_2 : (\sqrt{a}, \sqrt{b}) \mapsto (\sqrt{a}, -\sqrt{b})$
- $\sigma_3 : (\sqrt{a}, \sqrt{b}) \mapsto (-\sqrt{a}, -\sqrt{b})$

(c) When $a = 2, b = 3$. Intermediate fields correspond to the subgroups of G:

- Order 4: $G \iff \mathbb{Q}$
- Order 2 subgroup $\{id, \sigma_1\}$: Fixed field is $\mathbb{Q}(\sqrt{3})$ since σ_1 leaves $\sqrt{3}$ fixed.
- Order 2 subgroup $\{id, \sigma_2\}$: Fixed field is $\mathbb{Q}(\sqrt{2})$ since σ_2 leaves $\sqrt{2}$ fixed.
- Order 2 subgroup $\{id, \sigma_3\}$: $\sigma_3(\sqrt{2}\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}$. Fixed field is $\mathbb{Q}(\sqrt{6})$.
- Order 1 $\{id\} \iff K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Or $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ since $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ has degree 4.

Question 8 (15 marks)

(a) The polynomial $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion with prime $p = 2$, since $2 \mid 2$ but $2^2 = 4 \nmid 2$.

(b) The roots of $f(x) = x^4 - 2$ are $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. The splitting field K contains $\sqrt[4]{2}$ and $i\sqrt[4]{2}$, thus their quotient i is securely contained in K. And taking $\sqrt[4]{2}$ and i, we can construct all roots. Hence $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Degree: $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ since $x^4 - 2$ is irreducible. And $i \notin \mathbb{R}$ while $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, thus $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Total degree $[K : \mathbb{Q}] = 4 \times 2 = 8$.

(c) K is the splitting field of $x^4 - 2$ in characteristic 0, so $K/\mathbb{Q}$ is a Galois extension. $|G| = 8$. We define two automorphisms: $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \sigma(i) = i$. $\tau(\sqrt[4]{2}) = \sqrt[4]{2}, \tau(i) = -i$. Notice σ has order 4 since $\sigma^4(\sqrt[4]{2}) = i^4\sqrt[4]{2} = \sqrt[4]{2}$. And τ has order 2. Compose $\tau \circ \sigma \circ \tau^{-1}(\sqrt[4]{2}) = \tau(\sigma(\sqrt[4]{2})) = \tau(i\sqrt[4]{2}) = -i\sqrt[4]{2}$. On the other hand, $\sigma^{-1}(\sqrt[4]{2}) = -i\sqrt[4]{2}$. Thus $\tau\sigma\tau^{-1} = \sigma^{-1}$. This relation uniquely identifies $G = \langle \sigma, \tau \mid \sigma^4 = e, \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$ as the dihedral group D_4.

(d) Yes, D_4 is a solvable group. E.g., we have the subnormal series series $\{e\} \subset \langle \sigma^2 \rangle \subset \langle \sigma \rangle \subset G$, where all successive quotients are abelian (specifically isomorphic to $\mathbb{Z}/2\mathbb{Z}$). Since the Galois group of $f(x)$ over $\mathbb{Q}$ is solvable, the equation $f(x) = 0$ is solvable by radicals over $\mathbb{Q}$.