MA 3D50 SOLUTIONS

THE UNIVERSITY OF WARWICK

THIRD YEAR EXAMINATION: June 2007

MA3D50 GALOIS THEORY SOLUTIONS

Time Allowed: **3 hours**

Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer book.

Calculators are not needed and are not permitted in this examination.

ANSWER 4 QUESTIONS.
If you have answered more than the required 4 questions in this examination, you will only be given credit for your 4 best answers.

The numbers in the margin indicate approximately how many marks are available for each part of a question.

Each question consists of 2 or 3 unrelated parts (a), (b), ...

1. (a) Let K be a field. Prove that every ideal in the polynomial ring $K[x]$ is generated by just one element. **[6]**

Solution. Let $I \subset K[x]$ be an ideal. If I is the zero ideal there is nothing to prove, so suppose $I \neq (0)$. Let $f \in I$ be nonzero of minimal degree. We claim $(f) = I$. The inclusion $\subset$ is obvious; for the reverse inclusion, let $g \in I$. We need to prove $f \mid g$. On division with remainder we get $g = f \cdot q + r$ with $q, r \in K[x]$, $\deg r < \deg f$. By minimality of the degree of f we find $r = 0$. So $f \mid g$. [Belongs to preliminaries.] $\square$

(b) (i) Prove that $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible. **[4]**

(ii) Let $\varepsilon := \exp(2\pi i/5)$, $L = \mathbb{Q}(\varepsilon) \subset \mathbb{C}$. Prove that there exists a unique field automorphism σ of L such that $\sigma(\varepsilon) = \varepsilon^2$. Briefly state results from the lectures that you're using. **[4]**

(iii) Prove that $L/\mathbb{Q}$ is Galois and that $\langle 1 \rangle$, $\langle \sigma \rangle$, $\langle \sigma^2 \rangle$ are precisely the subgroups of $G := \mathrm{Gal}(L/\mathbb{Q})$. Briefly state results from the lectures that you're using. **[5]**

(iv) Putting $\alpha := 2\varepsilon + \sqrt{5}$, prove $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\alpha)$. Briefly state results from the lectures that you're using. **[6]**

Solution. (i). We have $f(x) = (x^5 - 1)/(x - 1)$ so $f(y + 1) = ((y + 1)^5 - 1)\, y^{-1} = y^4 + 5\, y^3 + 10\, y^2 + 10\, y + 5$ which is Eisenstein at 5. [Special case of seen result.]

(ii). Note that f is the minimum polynomial of ε over $\mathbb{Q}$. By our theorems, for every root ρ of f, there is a unique element of $\mathrm{Gal}(L/\mathbb{Q})$ taking ε to ρ. We have $f(\varepsilon^2) = 0$ so the result follows.

(iii). The order of σ is clearly 4. Now $4 \leq G \leq [L:\mathbb{Q}] = \deg f = 4$. So $\#G = 4$. One of our theorems says that $\#G = [L:\mathbb{Q}]$ implies that $L/\mathbb{Q}$ is Galois. Also, $G = \langle\sigma\rangle$ is cyclic of order 4 and the subgroups of G are precisely $\langle 1\rangle$, $\langle\sigma\rangle$, $\langle\sigma^2\rangle$.

(iv). Put $\gamma = \varepsilon + \varepsilon^{-1}$. Then $\gamma^2 = \varepsilon^2 + 2 + \varepsilon^{-2}$ so $\gamma^2 + \gamma - 1 = 0$ and $2\,\gamma = -1 + \sqrt{5}$. So $\sqrt{5} \in L$ and $\alpha \in L$ and $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$. To prove the reverse inclusion, note that $\sigma^2(\alpha) = 2\,\varepsilon^{-1} + \sqrt{5} \neq \alpha$. So $\mathbb{Q}(\alpha)^\dagger = \{1\}$. The main theorem of Galois theory states that if $L/\mathbb{Q}$ is Galois (which it is by (iii)) then $\dagger$ is a bijection with inverse $*$. So $\mathbb{Q}(\alpha) = \{1\}^* = L$.

[Parts (ii)–end: Similar to seen exercises.] □

---

2. (a) In the following, briefly state results from the lectures that you're using.

(i) Put $f = x^6 + a\,x^5 + a\,x + 1 \in \mathbb{C}[x]$. Find an explicit $g \in \mathbb{C}[y]$ such that $x^{-3} f(x) = g(x + x^{-1})$. Prove that f can be solved by radicals. **[3]**

(ii) Prove or disprove the following. Put $h = x^5 + a\,x^4 + a\,x + 1 \in \mathbb{C}[x]$. Then h can be solved by radicals. **[4]**

Solution. (i). Write $y = x + x^{-1}$. We have

$$\begin{aligned} x^{-3}\,f &= (x^3 + x^{-3}) + a\,(x^2 + x^{-2}) \\ &= (x^3 + 3x + 3x^{-1} + x^{-3}) + a\,(x^2 + 2 + x^{-2}) - 3(x + x^{-1}) - 2\,a \\ &= y^3 + a\,y^2 - 3\,y - 2\,a \end{aligned}$$

so $g := y^3 + a\,y^2 - 3\,y - 2\,a$ does it. In the lectures we showed that cubics can be solved by radicals; in particular, g can. A root of f is then a solution of the quadratic equation $x + x^{-1} = \alpha$ where α is a root of g. Therefore, f can be solved by radicals as well. [Unseen.]

(ii). True: -1 is a root of h, so $h = (x+1)\,\ell$ for some polynomial ℓ of degree 4. In the lectures we showed that quartics can be solved by radicals, and therefore ℓ can. [Unseen]. □

(b) Let A be an integral domain and K its field of fractions.

(i) What does it mean, by definition, for an ideal in a ring to be a prime ideal? List without proof the prime ideals in the polynomial ring $\mathbb{C}[t]$. **[3]**

(ii) Let $P \subset A$ be a prime ideal, and let P^2 be the ideal of A generated by **[7]**

$$\{pq \mid p, q \in P\}.$$

Let $f = \sum_{k=0}^{n} a_k\, x^k \in A[x]$ be a polynomial such that

(1) $a_n \notin P$;
(2) $a_k \in P$ if $0 \leq k < n$;
(3) $a_0 \notin P^2$.

Prove that f cannot be written gh with $g, h \in A[x]$ of degree $< n$.

(iii) State Gauss' lemma and deduce that if $f \in \mathbb{C}[t][x]$ is irreducible then it is irreducible in $\mathbb{C}(t)[x]$. **[3]**

(iv) Prove that $f := t^7 + x^5 + t\,x^3 + t \in \mathbb{C}(t)[x]$ is irreducible. **[5]**

Solution. (i) An ideal P is prime if $ab \in P$ implies $a \in P$ or $b \in P$. The prime ideals in $\mathbb{C}[t]$ are precisely the zero ideal and the ideals of the form $(t-\alpha)\,\mathbb{C}[t]$ for some $\alpha \in \mathbb{C}$. [Belongs to the preliminaries.]

(ii). We are asked to prove Eisenstein's criterion. Assume $f = gh$, g, h of degree $< n$, and write $g = \sum b_i x^i$ and $h = \sum c_i x^i$. Then $b_0 c_0 = a_0 \in P \smallsetminus P^2$ so precisely one among b_0, c_0 is in P, say, it is b_0. By induction on k we prove $b_k \in P$ if $k < n$. We have

$$P \ni a_k = c_0 b_k + \sum_{i=1}^{k} c_i b_{k-i}$$

and all $b_{k-i} \in P$ so $c_0 b_k \in P$. Also, $c_0 \notin P$ and P is a prime ideal so $b_k \in P$ as required. Since the degree of g is $< n$ we find $g \in P \cdot A[x]$ contradicting (1). [From the lectures.]

(iii). Gauss' lemma states that if A is a UFD and $f \in A[x]$ is irreducible then it is irreducible in $K[x]$. Choose $A = \mathbb{C}[t]$ which is known to be a UFD and the required result follows. [From the lectures.]

(iv). Choose $A = \mathbb{C}[t]$. Then f is Eisenstein at $P = (t)$. By (ii), f is irreducible in $A[x]$. By (iii), it is irreducible in $K[x] = \mathbb{C}(t)[x]$. [Unseen.] □

---

3. (a) (i) Let $f = x^3 - 3\,x + 1$. Prove that f is irreducible in $\mathbb{Q}[x]$. **[3]**

(ii) Prove directly that if $\gamma \in \mathbb{C}$ is a root of f then so is $\gamma^2 - 2$. **[2]**

(iii) Let $\alpha \in \mathbb{C}$ be a root of f and put $K = \mathbb{Q}(\alpha)$. Prove that $K/\mathbb{Q}$ is a Galois extension. Briefly state results from the lectures that you're using. **[6]**

(iv) Choose yourself a nontrivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$ and write down its matrix with respect to the $\mathbb{Q}$-basis $(1, \alpha, \alpha^2)$ of K. **[4]**

Solution. [Parts (i)–(iii): Similar to seen exercises. Part (iv): unseen.]

(i). It's irreducible mod 2.

(ii). Let γ be a root of f. Then

$$\begin{aligned} f(\gamma^2-2) &= (\gamma^2-2)^3 - 3\,(\gamma^2-2) + 1 \\ &= (\gamma^6 - 6\,\gamma^4 + 12\,\gamma^2 - 8) + (-3\,\gamma^2 + 6) + 1 \\ &= \gamma^6 - 9\,\gamma^4 + 9\,\gamma^2 - 1 = (\gamma^3 - 3\,\gamma)^2 - 1 \\ &= (\gamma^3 - 3\,\gamma - 1)(\gamma^3 - 3\,\gamma + 1) = (\gamma^3 - 3\,\gamma - 1)\,f(\gamma) = 0. \end{aligned}$$

(iii). A theorem from the course says splitting fields are always finite and normal. Another theorem says finite, normal, separable implies Galois. Clearly, $K/\mathbb{Q}$ is separable (because the characteristic is zero) so it remains to prove that it is a splitting field.

Let $\beta := \alpha^2 - 2$. Then α, β are two roots of f, by (b). Also $\alpha \neq \beta$ because otherwise α satisfies a quadratic equation, contradicting (a). So $f = (x-\alpha)(x-\beta)(x+\alpha+\beta)$ splits in $K[x]$. So $K/\mathbb{Q}$ is the splitting field of f.

(iv). Since f is irreducible, G acts transitively on the roots of f. So there exists $\sigma \in G$ such that $\sigma(\alpha) = \alpha^2 - 2$. This σ is unique because K is generated by α, and it is our nontrivial element of G chosen. We have $\sigma(\alpha^2) = \sigma(\alpha)^2 = (\alpha^2-2)^2 = \alpha^4 - 4\,\alpha^2 + 4 = (\alpha^4 - 4\,\alpha^2 + 4) - \alpha\,(\alpha^3 - 3\,\alpha + 1) = -\alpha^2 - \alpha + 4$ so

$$\sigma = \begin{pmatrix} 1 & -2 & 4 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}. \qquad \square$$

(b) Let L/K be a field extension. Let A, B be subfields of L and suppose $K \subset A \cap B$. Let C be the subfield of L, generated by $A \cup B$.

(i) Prove or disprove the following. If A/K and B/K are finite, then so is C/K. **[6]**

(ii) A field extension Q/P is said to be *purely transcendental* (pt) if every element of $Q \smallsetminus P$ is transcendental over P. **[4]**
Prove or disprove the following. If A/K and B/K are purely transcendental, then so is C/K.
[Hint. You may use that the field of rational functions $K(t)/K$ is pt.]

Solution. [Both parts unseen.]

(i) True. Let $B = K(\beta_1, \ldots, \beta_n)$, $A_k = A(\beta_1, \ldots, \beta_k)$. Then $C = A_n$. Now β_k is algebraic over K hence certainly over A_{k-1}. So A_k/A_{k-1} is finite. By the tower law,

$$[C : K] = [A_n : A_0][A : K] = [A : K] \prod_{k=1}^{n} [A_k : A_{k-1}]$$

which is finite, so C/K is finite.

(ii). False. Let $K \subset K(\alpha) = M$ be any algebraic extension with $\alpha \notin K$ and put $L = M(t)$ (rational functions). Put $A = K(t)$, $B = K(\alpha t)$. Then t is transcendental over M hence certainly over K, so A/K is pt by the hint. Also, αt is transcendental over M because if $f(\alpha t) = 0$ ($f \in M[x]$) then $g(t) = 0$ where $g(x) := f(\alpha x)$. Again, it follows that αt is transcendental over K so B/K is pt. Finally, $\alpha = (\alpha t)/t \in C \setminus K$ is algebraic, so C/K is not pt. □

---

4. (a) (i) Suppose that the polynomial $f = x^2 + px + q \in \mathbb{C}[x]$ factorizes as $f = (x + \alpha)(x + \beta)$. Compute $g = (x + \alpha + \beta^2)(x + \beta + \alpha^2)$ explicitly, giving its coefficients in terms of p, q. **[3]**

(ii) Prove or disprove the following. Let $f \in \mathbb{C}[x_1, \ldots, x_4]$ be a symmetric polynomial in four variables. Define $g_i \in \mathbb{C}[a, b, c]$ $(1 \leq i \leq 4)$ by **[3]**

$$\begin{aligned} g_1 &= a^2(b + c), \\ g_2 &= b^2(c + a), \\ g_3 &= c^2(a + b), \\ g_4 &= a^4 + b^4 + c^4. \end{aligned}$$

Then $h := f(g_1, g_2, g_3, g_4) \in \mathbb{C}[a, b, c]$ is symmetric.

Solution. [Both parts similar to seen exercises.]

(i). We have $\alpha + \beta = p$, $\alpha\beta = q$ so

$$\begin{aligned} \alpha^2 + \beta^2 &= (\alpha + \beta)^2 - 2\alpha\beta = p^2 - 2q, \\ \alpha^3 + \beta^3 &= (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta) = p^3 - 3pq. \end{aligned}$$

Write $u = \alpha + \beta^2$, $v = \beta + \alpha^2$. We get

$$\begin{aligned} u + v &= (\alpha + \beta) + (\alpha^2 + \beta^2) = p + p^2 - 2q, \\ uv &= \alpha\beta + (\alpha^3 + \beta^3) + \alpha^2\beta^2 = q + (p^3 - 3pq) + q^2, \\ g &= x^2 + (u + v)x + uv = x^2 + (p + p^2 - 2q)x + (q + p^3 - 3pq + q^2). \end{aligned}$$

(ii). True. Permutation of $\{a, b, c\}$ doesn't change $\{g_1, \ldots, g_4\}$ setwise so h is symmetric. Indeed, $\{g_1, g_2, g_3\}$ and g_4 are fixed. □

(b) (i) Define the *characteristic* of a ring A. **[2]**

(ii) Let A be a ring of characteristic p, a prime number. Define $F : A \to A$ by $F(a) = a^p$. Prove that F is a ring homomorphism. **[4]**

(iii) Let A, F be as in (ii). Let $n \geq 0$ and $B = \{a \in A \mid F^n(a) = a\}$. Prove that B is a subring of A. **[2]**

(iv) Let p be a prime number, $n \geq 1$, $q = p^n$, $\mathbb{F}_p := \mathbb{Z}/p$ and let K be a splitting field of $h := x^q - x$ over $\mathbb{F}_p$. Prove that every element of K is a root of h. **[6]**

(v) Let L be a field of 8 elements. How many elements $a \in L$ satisfy $a^5+a+1 = 0$? **[5]**

Solution. [Parts (i)–(iv): similar to the lectures. Part (v): unseen.]

(i). The characteristic of A is the least $m > 0$ such that $m = 0$ in A, or 0 if no such m exists.

(ii). We have $F(1) = 1^p = 1$. Let $a, b \in A$. Then $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$. Also, if $0 < k < p$ then

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in p\mathbb{Z}$$

so

$$F(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k\, b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k\, b^{p-k}$$
$$= a^p + b^p = F(a) + F(b).$$

So F is a ring homomorphism.

(iii). Let $a, b \in B$. Then $F^n(a-b) = F^n(a) - F^n(b) = a - b$ so $a - b \in B$. Also $F^n(ab) = F^n(a)F^n(b) = ab$ so $ab \in B$. So B is a subring of A.

(iv). Let F be the Frobenius map as before. Let B be the set of elements of K, fixed by F^n. By (iii), B is a subring of K.

In order to prove that B is a subfield of K, let $a \in B \setminus \{0\}$. Since K is finite, there are $0 < m < n$ with $a^m = a^n$. So $a^{n-m-1}a = 1$. So B is a subfield of K.

So K is generated by the subfield B. So $K = B$. Every element of B is fixed by F^n, that is, is a root of h.

(v). The factorisation of $x^5 + x + 1$ into irreducible polynomials is rs with $r = x^3 + x^2 + 1$, $s = x^2 + x + 1$.

Let $a \in L$, $s(a) = 0$, $K := \mathbb{F}_2(a)$. Then $3 = [L : K][K : \mathbb{F}_2]$ and $[K : \mathbb{F}_2] = \deg s = 2$, contradiction.

Straightforward calculation shows that $(x^5 + x^4 + x^3 + x)\, r = x^8 - x$. But $x^8 - x$ splits into linear factors in $L[x]$, as we know from the lectures. So r splits into linear factors.

Answer is 3.

---

5. (a) Let $n \geq 1$. Let $L = \mathbb{C}(t_1, \ldots, t_n)$ be the field of rational functions in n variables (that is, the field of fractions of the polynomial ring $\mathbb{C}[t_1, \ldots, t_n]$). Let the symmetric group act on L by

$$r(t_i) = t_{r(i)} \quad \text{and} \quad r(a) = a$$

for all $r \in S_n$, $i \in \{1, \ldots, n\}$, $a \in \mathbb{C}$.

(i) Give the definition of σ_k, the kth elementary symmetric polynomial of $t_1, \ldots, t_n$. **[2]**

(ii) We put $M = \mathbb{C}(\sigma_1, \ldots, \sigma_n) \subset L$ and **[8]**

$$K = L^{S_n} := \{f \in L \mid r(f) = f \text{ for all } r \in S_n\}.$$

State the main theorem of symmetric polynomials, and prove $K = M$.

(iii) Prove that L/K is Galois and $\mathrm{Gal}(L/K) \cong S_n$. Briefly state results from the lectures that you're using. **[3]**

Solution. (i). $\sigma_k = \sum t_{i_1} \cdots t_{i_k}$ where the sum ranges over $\{(i_1, \ldots, i_k) : 1 \leq i_1 < \cdots < i_k \leq n\}$. [From the lectures.]

(ii). $M \subset K$ is obvious. For the reverse inclusion, let $f \in K$, say, $f = p_0/q_0$ for polynomials $p_0, q_0 \in \mathbb{C}[t_1, \ldots, t_k]$. Define

$$q := \prod_{\sigma \in S_n} \sigma(q_0), \qquad p := f \cdot q.$$

Then p, q are polynomials, because q is divisible by q_0 and $p/q = p_0/q_0$. Also, f, q are symmetric hence so is $fq = p$. So $p, q \in \mathbb{C}[t_1, \ldots, t_n]$ are symmetric polynomials. The main theorem of symmetric polynomials says that every symmetric polynomial in $\{t_k\}_k$ is a polynomial in $\{\sigma_k\}_k$. So $p, q \in M$ and hence $f = p/q \in M$. [Unseen.]

(iii). A theorem says that if a finite group G acts on a field L, then L/L^G is Galois with Galois group G. [Similar to seen applications.] □

(b) Recall that a field extension $K \subset L$ is separable if and only if no irreducible polynomial $f \in K[x]$ has a multiple root in L. **[7]**

Let p be a prime number, $\mathbb{F}_p$ a field of p elements, $L := \mathbb{F}_p(t)$ (rational functions), $K := \mathbb{F}_p(t^p) \subset L$. Is $K \subset L$ separable? Is it normal? Is it finite? Is it Galois?

Solution. [Seen.] Normal and finite, but not separable nor Galois.

Let $f = x^p - t^p = (x-t)^p$. Then t is a root of f. So the minimum polynomial $g := \mathrm{Min}_K(t)$ is a divisor of f. So $g = (x-t)^k$ for some k with $1 \leq k \leq p$. Looking at the coefficient of x^{k-1} in g we find $t \in K$ or $k = p$. Now $t \in K$ is absurd so $k = p$. So $(x-t)^p = \mathrm{Min}_K(t)$ is irreducible over K with a multiple root in L, and L/K is not separable.

Galois is equivalent to finite, normal, separable, so L/K is not Galois.

Clearly, L/K is a splitting field of f, hence normal and finite. □

(c) Let $K \subset L$ be fields. Let $\mathcal{F}$ denote the set of intermediate fields and $\mathcal{G}$ the set of subgroups of $G := \mathrm{Gal}(L/K)$.

(i) Define the map $\mathcal{F} \to \mathcal{G}$, $F \mapsto F^*$ that features in Galois theory. **[1]**

(ii) Let $F \in \mathcal{F}$ and $g \in G$. Prove that $gF^*g^{-1} = (gF)^*$. **[4]**

Solution. [Both parts from the lectures.]

(i). $F^* = \{h \in G \mid h(x) = x \text{ for all } x \in F\}$.

(ii). Let $h \in G$. Then

$$\begin{aligned} h \in (gF)^* &\iff h(x) = x \text{ for all } x \in gF \\ &\iff h(gy) = gy \text{ for all } y \in F \\ &\iff (g^{-1}hg)y = y \text{ for all } y \in F \\ &\iff g^{-1}hg \in F^* \iff h \in gF^*g^{-1}. \end{aligned}$$

□
