MA 3D50 GALOIS THEORY solutions — June 2008

Questions 1, 4 and 5 consist of two or three unrelated parts (a), (b), ...

1. (a) (i) State without proof the tower law. **[2]**

(ii) Let L/K be a finite field extension, that is, $[L : K] < \infty$. Prove that L/K is algebraic. **[5]**

(iii) Let $K \subset M$ be fields. Let L be the set of those elements of M that are algebraic over K. Prove that L is a subfield of M. State any results you use. **[5]**

Solution. Remarks: all of these are bookwork.

(i). Let $K \subset L \subset M$ be fields. Then $[M : K]$ if and only if $[M : L]$ and $[L : K]$ are. If they are then $[M : K] = [M : L][L : K]$.

(ii). Let $\alpha \in L$. We need to prove that α is algebraic over K. Let $n := [L : K]$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ elements of an n-dimensional vector space, so are dependent. Say $\sum_{i=0}^{n} b_i \alpha^i = 0$ with $b_i \in K$ and not all zero. Then $f(\alpha) = 0$ where $f := \sum_{i=0}^{n} b_i x^i$ which proves that α is algebraic over K as required.

(iii). Let $\alpha, \beta \in L$. We need to prove that $K(\alpha, \beta) \subset L$. As β is algebraic over K it is over $K(\alpha)$. So $[K(\alpha, \beta) : K(\alpha)] < \infty$. Also, α is algebraic over K so $[K(\alpha) : K] < \infty$. By (i) $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < \infty$. So $K(\alpha), \beta)/K$ is algebraic. So $K(\alpha, \beta) \subset L$ as required. □

(b) Prove or disprove the following. Let $K \subset L \subset M$ be fields and let $\alpha \in M$ be algebraic over K. Then $[L(\alpha) : L] \leq [K(\alpha) : K]$. **[5]**

Solution. (unseen). True. Let f be the minimum polynomial of α over K. The equation $f(\alpha) = 0$ shows that α is algebraic over L. Let g be the minimum polynomial of α over L. Then $g \mid f$ so $\deg g \leq \deg f$, that is, $[L(\alpha) : L] \leq [K(\alpha) : K]$. □

(c) Let $\mathbb{F}_q$ be a finite field of q elements. Prove from first principles the following identity in $\mathbb{F}_q[x]$: **[8]**

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x.$$

[But you may use results about finite groups, and that $K[x]$ is a unique factorisation domain for all fields K.]

Solution. (Shortcut to a bookwork result). Note that $\mathbb{F}_q^*$ is a group of order $q - 1$. By Lagrange's theorem, $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$. On putting $f = x^q - x \in \mathbb{F}_q[x]$ we find $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$. In other words, $(x - \alpha) \mid f$ for all $\alpha \in \mathbb{F}_q$. As $\mathbb{F}_q[x]$ is a UFD, we find $\prod_{\alpha \in \mathbb{F}_q}(x - \alpha) \mid f$. But left and right hand sides in the latter have equal degrees and are both monic, so they are necessarily equal. □

---

2. Let K be a field and let $f \in K[x]$ be a polynomial.

(a) Let $g \in K[x]$ be nonconstant and irreducible. Prove that there exists a field extension $K \subset L$ and an element $\alpha \in L$ such that $g(\alpha) = 0$. **[4]**

(b) Define what a *splitting field* for (K, f) is. **[3]**

(c) Prove that a splitting field for (K, f) exists. [Hint: induction on the degree of f.] **[8]**

(d) Let $\mathbb{C}(t)$ denote the field of rational functions in one variable t. Let $M/\mathbb{C}(t)$ be a splitting field for $f(x) = x^6 - t^2$. Compute $[M : \mathbb{C}(t)]$ and briefly justify. **[4]**

(e) Find splitting fields M/L and L/K such that M/K is not a splitting field, and prove your claims. **[6]**

Solution. Remarks: (a)–(c) are bookwork; (d) and (e) are unseen.

(a). Put $L = K[x]/(g)$. Then L is a field because g is irreducible. Put $\alpha := x + (g) \in L$. Then $g(\alpha) = g(x) + (g) = (g) = 0$. Finally, we have a composition map $K \to K[x] \to K[x]/(g) = L$ so L/K is an extension.

(b). A splitting field for (K, f) is a field extension L/K such that there exist $\alpha_1, \ldots, \alpha_n \in L$ and $c \in K$ such that $f = c\prod_i (x - \alpha_i)$ and $L = K(\alpha_1, \ldots, a_n)$.

(c). We may suppose f to be monic. Let n be the degree of f. Induction on n. True for $n = 0$ (choose $L = K$).

First suppose that f is irreducible. Let $L = K(\alpha)$ be an extension such that $f(\alpha) = 0$ (existing by (i)). Then there exists $g \in L[x]$ such that $f = (x - \alpha) \cdot g$. Now g has smaller degree than f, so by the induction hypothesis, there exists a splitting field M for (L, g), say, $g = \prod_i (x - \beta_i)$ with $\beta_i \in M$. We have $f = (x - \alpha) \cdot g = (x - \alpha) \cdot \prod_i (x - \beta_i)$ and $M = L(\beta_1, \ldots, \beta_n) = K(\alpha, \beta_1, \ldots, \beta_n)$, that is, M is a splitting field for (K, f) as required.

Finally, suppose that f is reducible, say, $f = gh$ with $g, h \in K[x]$ nonconstant. By the induction hypothesis, there exists a splitting field L for (K, g), say, with $g = \prod_{i=1}^{m} (x - \alpha_i)$ and $\alpha_i \in L$. By the induction hypothesis again, there exists a splitting field M for (L, h), say, with $h = \prod_{j=1}^{n} (x - \beta_j)$ and $\beta_j \in M$. We prove that M is a splitting field for f. We have $f = gh = \prod_i (x - \alpha_i) \prod_j (x - \beta_j)$. Also, $M = L(\beta_1, \ldots, \beta_n) = K(\alpha_1, \ldots, a_m)(\beta_1, \ldots, \beta_n) = K(\alpha_1, \ldots, a_m, \beta_1, \ldots, \beta_n)$. This proves that M is a splitting field as required.

(d). We have $x^6 - t^2 = (x^3 - t)(x^3 + t)$. Let α be a cube root of t in the splitting field. Then the other roots of $x^6 - t^2$ are of the form $\varepsilon^k \alpha$ where $\varepsilon = \exp(2\pi i/6)$. Thus, the splitting field is generated by α. Moreover, $x^3 - t$ is irreducible, because it is Eisenstein at t in $\mathbb{C}[t]$. So α is of degree 3 over $\mathbb{C}(t)$ and $[M : \mathbb{C}(t)] = 3$.

(e). Put $\beta = 2^{1/4} \in \mathbb{R}$, $K = \mathbb{Q}$, $L = K(\beta^2)$, $M = K(\beta)$. Then M/L is a splitting field for $x^2 - \beta^2$ and L/K for $x^2 - \beta^4$.

Claim: the minimum polynomial over K for β is $f := x^4 - 2$. Proof of claim. We have $f(\beta) = 0$. Moreover, f is Eisenstein at 2 so irreducible. This proves the claim.

Suppose that M/K is a splitting field. Some theorem says it is then normal. So the minimum polynomial f for β over K splits into linear factors over M. But f has only two roots in $\mathbb{R}$ whence in $M \subset \mathbb{R}$ and they are simple roots, contradiction. So M/K is not a splitting field. □

---

3. Let $\alpha \in \mathbb{C}$ be a root of the polynomial $f = x^3 - x^2 - 4x - 1$.

(a) Prove that $f \in \mathbb{Q}[x]$ is irreducible, carefully stating any results you use. **[6]**

(b) Prove that $-(1+\alpha)^{-1}$ is also a root of f. **[6]**

(c) Prove or disprove that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, carefully stating any results you use. **[7]**

(d) Write $\varepsilon = \exp(2\pi i/3)$. Prove that f is irreducible in $\mathbb{Q}(\varepsilon)[x]$. **[6]**

Solution. Remarks: all of these are similar to examples.

(a). A theorem states that if p is a prime number and the image $\bar{f} \in \mathbb{F}_p[x]$ of some polynomial $f \in \mathbb{Z}[x]$ is irreducible and of the same degree as f, then f is irreducible in $\mathbb{Q}[x]$. Choose $p = 2$. Then $\bar{f}$ has no zero in $\mathbb{F}_2$. As f has degree 3, this proves that $\bar{f}$ is irreducible. Also, $\deg f = \deg \bar{f}$ and the theorem applies to prove that f is irreducible.

(b). We have

$$f\Big(\frac{-1}{1+\alpha}\Big)(1+\alpha)^3 = -1 - (1+\alpha) + 4(1+\alpha)^2 - (1+\alpha)^3 = -1 + (-1-\alpha) + (4+8\alpha+4\alpha^2) - (1+3\alpha+3\alpha^2+\alpha^3) = -\alpha^3 + \alpha^2 + 4\alpha + 1 = -f(\alpha) = 0.$$

(c). True. A theorem states that Galois is equivalent to splitting field and separable. Moreover, separability follows from characteristic zero.

Well, $\mathbb{Q}$ has characteristic zero, so separability is ensured. It remains to prove that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a splitting field. It is for f as we shall show. Note that $\gamma := -(1+\alpha)^{-1}$ is distinct from α, because otherwise α would be of degree at most 2 over $\mathbb{Q}$, contradicting (i). Moreover, f has two distinct roots α and γ and has degree 3 so splits over $\mathbb{Q}(\alpha)$. Clearly, $\mathbb{Q}(\alpha)$ is generated by the three roots of f. This proves it's a splitting field as required.

(d). Suppose f is reducible over $\mathbb{Q}(\varepsilon)$. Then α has degree 1 or 2 over $\mathbb{Q}(\varepsilon)$ because $\deg(f) = 3$. Also $[\mathbb{Q}(\varepsilon,\alpha) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon,\alpha) : \mathbb{Q}(\varepsilon)][\mathbb{Q}(\varepsilon) : \mathbb{Q}] \in \{1\cdot 2, 2\cdot 2\} = \{2,4\}$. But $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides $[\mathbb{Q}(\varepsilon,\alpha) : \mathbb{Q}]$, a contradiction. So f is irreducible over $\mathbb{Q}(\varepsilon)$. □

---

4. (a) Let $K \subset L$ be fields and let $G = \mathrm{Gal}(L/K)$ be the Galois group. Suppose that G is finite. Let $\mathcal{G}$ be the set of subgroups of G. Let $\mathcal{F}$ be the set of subfields of L containing K. For $F \in \mathcal{F}$, let F^* be the set of $g \in G$ such that $g(x) = x$ for all $x \in F$. For $H \in \mathcal{G}$, let $H^\dagger$ be the set of $x \in L$ such that $g(x) = x$ for all $g \in H$.

(i) Let $F \in \mathcal{F}$. Prove that $F^* \in \mathcal{G}$. **[4]**

(ii) Let $F_1, F_2 \in \mathcal{F}$ and suppose that $F_1 \subset F_2$. Prove that $F_1^* \supset F_2^*$. **[4]**

(iii) State the main theorem of Galois theory. **[2]**

(iv) Prove or disprove the following, carefully stating every result you use. Suppose that $H^{\dagger *} = H$ for all $H \in \mathcal{G}$. Then L/K is normal. **[6]**

Solution. Remarks: (i)–(iii) are bookwork; (iv) unseen.

(i). Clearly $1 \in F^*$. Let $f, g \in F^*$. Then, for all $x \in F$, we have $(fg^{-1})(x) = f(g^{-1}(x)) = f(x) = x$. So $fg^{-1} \in F^*$. So F^* is a subgroup of G as required.

(ii). Let $g \in F_2^*$. Then $g(x) = x$ for all $x \in F_2$. So $g(x) = x$ for all $x \in F_1$ (because $F_1 \subset F_2$). Therefore, $g \in F_1^*$.

(iii). If L/K is Galois then $*$ and $\dagger$ are inverse bijections.

(iv). False. Take $K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha) \subset \mathbb{R}$ where $\alpha = 2^{1/3} \in \mathbb{R}$. We know that L/K is not normal.

We claim that $G = 1$. In order to prove the claim, let $g \in G$. Then $2 = g(2) = g(\alpha^3) = (g(\alpha))^3$. So $g(\alpha)$ is a real cube root of 2 hence is α. So $g = 1$.

The above claim implies $H^{\dagger *} = H$ for all $H \in \mathcal{G}$ and the disproof is finished. □

(b) Let L/K be an algebraic field extension. Let $\lambda \in L$ be nonzero and such that λ and λ^2 have the same minimum polynomial over K. Prove that λ is a root of unity. **[9]**

Solution. (Unseen). Let $f(x) := x^2$. Let g be the minimum polynomial of λ. Let A be the set of roots of g in L. We claim that $\beta^2 \in A$ for all $\beta \in A$.

Proof of the claim. As $g(\lambda^2) = 0$ we have $g(x) \mid g(x^2)$ by definition of minimum polynomial, say, $g(x^2) = g(x)\,h(x)$. Let $\beta \in A$. As $g(\beta) = 0$ we have $g(\beta^2) = g(\beta)\,h(\beta) = 0 \cdot h(\beta) = 0$ and hence $\beta^2 \in A$. This proves the claim.

Using the claim and the fact that $\lambda \in A$ we find that $f^k(\lambda) \in A$ for all $k \geq 0$. As A is finite, there are $0 \leq k < \ell$ such that $f^k(\lambda) = f^\ell(\lambda)$, that is, $\lambda^{2^k} = \lambda^{2^\ell}$ whence $\lambda^{2^k - 2^\ell} = 1$ and λ is a root of unity. □

---

5. (a) Let $t_1, \ldots, t_n$ be variables. Express the polynomial **[6]**

$$S = \sum_{1 \leq i < j < k \leq n} t_i\, t_j\, t_k\, (t_i + t_j + t_k)$$

in terms of the elementary symmetric polynomials $\sigma_k(t_1, \ldots, t_n)$.

Solution. (Similar to examples). We have

$$\begin{aligned}\sigma_1\, \sigma_3 &= \Big(\sum_i t_i\Big)\Big(\sum_{i<j<k} t_i\, t_j\, t_k\Big) \\ &= \Big(\sum_{i<j<k} t_i\, t_j\, t_k\, (t_i + t_j + t_k)\Big) + 4\Big(\sum_{i<j<k<\ell} t_i\, t_j\, t_k\, t_\ell\Big) = S + 4\,\sigma_4\end{aligned}$$

so $S = \sigma_1\, \sigma_3 - 4\sigma_4$. □

(b) Put $\alpha = 8^{1/4} \in \mathbb{R}$ and $\beta = \alpha + \alpha^2$.

(i) Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. [Hint: express $\beta(\beta - 2\alpha^2)$ in terms of α.] **[6]**

(ii) Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and prove your result. **[5]**

Solution. (Both similar to examples). (i). We have $\beta(\beta - 2\alpha^2) = (\alpha + \alpha^2)(\alpha - \alpha^2) = \alpha^2 - \alpha^4 = \alpha^2 - 8$. From $\beta(\beta - 2\alpha^2) = \alpha^2 - 8$ it follows that α^2 can be expressed in terms of β. Therefore so can $\alpha = \beta - \alpha^2$. This proves $\mathbb{Q}(\beta) \supset \mathbb{Q}(\alpha)$. The reverse inclusion is immediate from the formula $\beta = \alpha + \alpha^2$.

(ii). α is a root of $x^4 - 8$. So $2\alpha^{-1}$ is a root of $x^4 - 2$ which is Eisenstein at 2 hence irreducible. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(2\alpha^{-1}) : \mathbb{Q}] = \deg(x^4 - 2) = 4$. □

(c) Let $K \subset L \subset M$ be fields. Let $\alpha \in M$ and let $f \in L[x]$ be a nonzero polynomial all of whose coefficients are algebraic over K, and such that $f(\alpha) = 0$. Prove that α is algebraic over K. You may use without proof that a field extension is finite iff it is algebraic and finitely generated. **[8]**

Solution. (Variation of a theorem in the lectures). Let $f = \sum_{i=0}^{n} b_i\, x^i$ with $b_i \in L$. Put $L_0 := K(b_0, \ldots, b_n)$. We know that b_i is algebraic over K; it follows that L_0/K is finite. We know that α is algebraic over K whence over L_0; it follows that $L_0(\alpha)/L_0$ is finite. The tower law tells us $[L_0(\alpha) : K] = [L_0(\alpha) : L_0][L_0 : K]$. So $L_0(\alpha)/K$ is finite and therefore algebraic. In particular, α is algebraic over K. □
