UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level M)

GALOIS THEORY SOLUTIONS

MATH 2700

(Paper Code MATHM-2700)

January 2015, 2 hours 30 minutes

This paper contains **five** *questions*
A candidate's **FOUR** *best answers will be used for assessment.*

Calculators are **not** *permitted in this examination.*

Do not turn over until instructed.

[H]=standard, from class, or similar to homework, [B]=bookwork, [U]=unseen

1. (a) (2+2+3+2 marks) [B] Suppose that $K \subseteq L$ are fields, and that $\alpha \in L$.

   (i) Define $[L : K]$, the degree of the field extension $L : K$.

   Solution: $[L : K]$ is the dimension of L as a vector space over K.

   (ii) Define what it means for $L : K$ to be a finite extension.

   Solution: $L : K$ is a finite extension if $[L : K]$ is finite.

   (iii) Suppose α is algebraic over K. Briefly explain why $K[\alpha] = K(\alpha)$.

   Solution: When α is algebraic over K, then $K[\alpha]$ is a field. But $K(\alpha)$ is the quotient filed of $K[\alpha]$, and this is simply $K[\alpha]$ when α is algebraic over K.

   (iv) Suppose still that α is algebraic over K. Is it possible that $[K(\alpha) : K] = \infty$? Briefly explain your answer.

   Solution: Were one to have $[K(\alpha) : K] = \infty$, then $1, \alpha, \alpha^2, \ldots$ would be linearly independent over K, and hence α could not be algebraic over K. So it is not possible that $[K(\alpha) : K] = \infty$.

   (b) (2+2+2+3 marks) [B+U] Suppose that $K \subseteq L$ are fields such that $L : K$ is a finite extension.

   (i) Define what it means for $f \in K[X]$ to split over L.

   Solution: The polynomial f splits over L if f factors into linear factors in $L[X]$.

   (ii) Define what it means for $L : K$ to be a splitting field extension.

   Solution: The extension $L : K$ is a splitting field extension if it is a minimal extension of K in which the elements of S split, for some $S \subseteq K[X]$.

   (iii) Define what it means for $L : K$ to be normal.

   Solution: An extension $L : K$ is normal if $L : K$ is algebraic and, for any irreducible polynomial $f \in K[X]$, either f has no root in L, or f splits in L.

   (iv) Suppose that $L : K$ is a normal extension, and that M is a field having the property that $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.

   Solution: Since $L : K$ is normal, then for any $\alpha \in L$, one has that the minimal polynomial $f = m_\alpha(K)$ of α over K splits over L. We know that $g = m_\alpha(M)$ divides f, so all roots of g are roots of f, and hence lie in L. Thus g splits over L, and $L : M$ is normal.

   (c) (4+3 marks) [U] Suppose that L is a subfield of $\mathbb{C}$ having the property that $L : \mathbb{Q}$ is an infinite, normal field extension.

   (i) Suppose that φ is an automorphism of $\mathbb{C}$. Show that whenever $\alpha \in L$, then $\varphi(\alpha) \in L$. Hence deduce that $\varphi(L) \subseteq L$.

   Solution: Since $\varphi(1) = 1$ (and φ is a homomorphism), one finds that φ fixes $\mathbb{Q}$ pointwise. Given $\alpha \in L$, one has that α is algebraic, and so the minimal polynomial $m_\alpha(\mathbb{Q})$ exists. In addition, one has $\varphi(m_\alpha(\mathbb{Q})) = m_\alpha(\mathbb{Q})$, so $\varphi(\alpha)$ is another root of $m_\alpha(\mathbb{Q})$. Since $L : \mathbb{Q}$ is normal, all the roots of $m_\alpha(\mathbb{Q})$ lie in L, and so $\varphi(\alpha) \in L$. Thus $\varphi(L) \subseteq L$.

Continued...

(ii) Prove that whenever ψ is an automorphism of $\mathbb{C}$, then $\psi(L) = L$.

Solution: Let ψ be an automorphism of $\mathbb{C}$. Consider $\alpha \in L$, and put $\beta = \psi^{-1}(\alpha)$. Since ψ^{-1} is an automorphism of $\mathbb{C}$, one sees that $\psi^{-1}(m_\alpha(\mathbb{Q})) = m_\alpha(\mathbb{Q})$. Thus β is a root of $m_\alpha(\mathbb{Q})$, and so β lies in L. From part (i), meanwhile, one has $\psi(L) \subseteq L$, so that $\alpha = \psi(\beta) \in L$, whence $L \subseteq \psi(L)$. Thus $L \subseteq \psi(L) \subseteq L$, whence $L = \psi(L)$, as desired. [Or, to show that $L \subseteq \psi(L)$, proceed as follows. We have $\psi(L) \subseteq L$ for any automorphism of $\mathbb{C}$. Given an automorphism ψ of $\mathbb{C}$, one has that ψ^{-1} is also an automorphism of $\mathbb{C}$, and hence $\psi^{-1}(L) \subseteq L$. Thus $L = \psi \circ \psi^{-1}(L) \subseteq \psi(L)$.]

2. (a) (3+3 marks) [B+U/H] (i) State Eisenstein's criterion for irreducibility of polynomials in $\mathbb{Z}[t]$.

Solution: Suppose that $f = f_0 + f_1 t + \cdots + f_n t^n \in \mathbb{Z}[t]$ satisfies the condition that the coefficients $f_0, \ldots, f_n$ have no common factor. Suppose further that for some prime number p one has $p | f_i$ $(0 \leq i < n)$, $p \nmid f_n$ and $p^2 \nmid f_0$. Then f is irreducible over $\mathbb{Z}$.

(ii) Determine whether or not the polynomial $3t^{2014} + 24t + 2$ is irreducible over $\mathbb{Z}$, and explain your reasoning.

Solution: We apply Eisenstein's criterion with $p = 2$, noting that the coefficients of the polynomial in question have no common factor, and that all but the lead coefficient are divisible by 2, and further that the constant coefficient is not divisible by 4. Thus $3t^{2014} + 24t + 2$ is indeed irreducible.

(b) (3+3 marks) [B+B] Let L be a field extension of K.

(i) What does it mean for $\alpha \in L$ to be algebraic over K?

Solution: One says that α is algebraic over K when there exists a non-zero polynomial $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ in $K[x]$ such that $f(\alpha) = f_0 + f_1 \alpha + \cdots + f_n \alpha^n = 0$.

(ii) Define, when $\alpha \in L$ is algebraic over K, the minimal polynomial of α over K.

Solution: The minimal polynomial of the algebraic number α is the monic polynomial f in $K[x]$ of least positive degree with the property that $f(\alpha) = 0$. [There are equivalent definitions based on the kernel of the evalution map being equal to the ideal (f), so mark with care].

(c) (6 marks) [H] Calculate the minimal polynomial of $\sqrt{3 + \sqrt[3]{6}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt{3 + \sqrt[3]{6}}) : \mathbb{Q}$.

Solution: Write $\alpha = \sqrt{3 + \sqrt[3]{6}}$. Then $\alpha^2 - 3 = \sqrt[3]{6}$, and hence $(\alpha^2 - 3)^3 = 6$. On putting $f(x) = (x^2 - 3)^3 - 6 = x^6 - 9x^4 + 27x^2 - 33$, we see that $f(\alpha) = 0$, and thus it follows that the minimal polynomial of α divides f. But by applying Eisenstein's criterion using the prime 3, we see that f is irreducible, and hence f is the minimal polynomial of α over $\mathbb{Q}$. The degree of the field extension $\mathbb{Q}(\sqrt{3 + \sqrt[3]{6}}) : \mathbb{Q}$ is therefore equal to $\deg f = 6$.

Continued...

(d) (7 marks) [U] Let $L : K$ be a field extension and suppose that γ is an element of L whose minimal polynomial over K has degree 9. Prove that if $h \in K[t]$ is a non-zero quadratic polynomial, then the minimal polynomial of $h(\gamma)$ over K has degree 9.

Solution: One has $K \subseteq K(h(\gamma)) \subseteq K(\gamma) \subseteq L$. Then by the Tower Law, we find that

$$[K(\gamma) : K] = [K(\gamma) : K(h(\gamma))][K(h(\gamma)) : K],$$

whence $[K(\gamma) : K(h(\gamma))]$ divides $[K(\gamma) : K]$. But the degree of the minimal polynomial of γ over K is 9, so that $[K(\gamma) : K] = 9$. We therefore see that $[K(\gamma) : K(h(\gamma))] = 1$, 3 or 9. But over the field $K(h(\gamma))$, the element γ satisifies the quadratic equation $h(t) - h(\gamma) = 0$, and thus the minimal polynomial of γ over $K(h(\gamma))$ divides the latter quadratic polynomial, so has degree either 1 or 2. Consequently, we must have $[K(\gamma) : K(h(\gamma))] = 1$ or 2. In view of our earlier observation, we are forced to conclude that the latter degree is 1, and then the previous application of the Tower Law implies that $[K(h(\gamma)) : K] = 9$, which is to say that the minimal polynomial of $h(\gamma)$ over K has degree 9.

3. (a) (10 marks)[B] Define what it means for a field extension $L : K$ to be

(i) algebraically closed: *Solution:* The extension $L : K$ is algebraically closed if it is an extension of K in which the elements of S split, for all $S \subseteq K[X]$.

(ii) simple: *Solution:* An extension $L : K$ is simple if there exists an element $\gamma \in L$ for which $L = K(\gamma)$.

(iii) Galois: *Solution:* An extension $L : K$ is Galois if it is finite, normal and separable.

(iv) *Solution:* separable: An extension $L : K$ is separable if every element of L is algebraic over K, and each element has a minimal polynomial f over K, say of degree n, which has n distinct roots in a splitting field for f over K.

(v) cyclic: *Solution:* An extension $L : K$ is cyclic if it is Galois and the Galois group $\mathrm{Gal}(L : K)$ is cyclic.

(b) (15 marks) Indicate whether each of the following statements is true or false. For those that are false, please provide a short (one or two sentence) justification. Each fully correct answer is worth 1 mark.

(i) Every algebraic extension of $\mathbb{Q}$ is normal.

Solution: [B] False. Consider the example $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $t^3 - 2$, and this has splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cubic root of unity. The polynomial $t^3 - 2$ does not split completely over $\mathbb{Q}(\sqrt[3]{2})$, and hence $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ is not normal.

(ii) If $L : K$ is a finite extension of fields, then every element of L is algebraic over K.

Solution: [B] True.

(iii) Every field extension of finite degree is a splitting field extension.

Solution: [B] False. A finite extension $L : K$ is a splitting field extension iff it is normal. $\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}$ is a finite extension, but the minimal polynomial for $\sqrt[3]{5}$ does not split over $\mathbb{Q}(\sqrt[3]{5})$.

Continued...

(iv) There is an isomorphism $\varphi : \mathbb{Q}(\sqrt{11}) \to \mathbb{Q}(\sqrt{-11})$ so that $\varphi(\sqrt{11}) = \sqrt{-11}$.

Solution: [U] False. Proceed by contradiction. If the statement were true, then one would have

$$-11 = (\sqrt{-11})^2 = \varphi(\sqrt{11})^2 = \varphi(11) = 11.$$

(v) If $L : K$ is a field extension and $\tau \in L$ is transcendental over K, then $\tau^3 + \tau + 1$ is transcendental over K.

Solution: [B] True.

(vi) If K_1 and K_2 are subfields of a field L, and $[L : K_1] = [L : K_2]$, then K_1 and K_2 are isomorphic fields.

Solution: [H] False. Consider the example $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt{3})$.

(vii) If $L : K$ is a field extension, and α and β are distinct elements of L having the same minimal polynomial over K, then $K(\alpha)$ and $K(\beta)$ are isomorphic fields.

Solution: [B] True.

(viii) A splitting field of a degree n irreducible polynomial in $\mathbb{R}[t]$ has degree $n!$ over $\mathbb{R}$.

Solution: [U] True.

(ix) If $L : K$ is a field extension and $L = K(\alpha)$, then for any $\beta \in L$, there exist $a, b \in K$ with $\beta = a + b\alpha$.

Solution: [U] False. Consider $L = \mathbb{Q}(\alpha)$ with $\alpha = 2^{1/3}$, and $\beta = (2^{1/3})^2$. The minimal polynomial of α over $\mathbb{Q}$ is easily seen to be $t^3 - 2$. Were β to be of the shape $a + b\alpha$ for some $a, b \in \mathbb{Q}$, then α would have a minimal polynomial of degree at most 2, contradicting that it has minimal polynomial $t^3 - 2$ of degree 3.

(x) The polynomial $x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.

Solution: [U] False. The polynomial $x + 1$ is a factor.

(xi) Suppose that $L : M$ and $M : K$ are field extensions, and the field extension $L : K$ is separable. Then $M : K$ is separable.

Solution: [B] True.

(xii) Every field extension of $\mathbb{Q}$ of finite degree has only finitely many subfields.

Solution: [H] True.

(xiii) If $L : \mathbb{Q}$ is a simple field extension, then the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ is simple.

Solution: [U] False. Consider the example $L = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. The field extension $L : \mathbb{Q}$ is simple, and yet $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so that $\Gamma(L : \mathbb{Q})$ is isomorphic to $C_2 \times C_2$, and the latter is not a simple group (it has a normal subgroup $C_2 \times \{\mathrm{id}\}$.

(xiv) If K is a field and γ is an element in an extension field of K, then every element of $K(\gamma)$ is expressible as a polynomial in γ with coefficients in K.

Solution: [H] False. Suppose that $L : K$ is a field extension and $\alpha \in L$ is transcendental over K. Then $1/\alpha$ lies in $K(\alpha)$, and yet $1/\alpha$ cannot be expressed as a polynomial in α.

(xv) Suppose $L : K$ is a Galois extension with $\mathrm{Gal}(L : K) \simeq S_n$. Then, for any subgroup H of S_n, there is a field M with the property that $L : M$ is a Galois extension with $\mathrm{Gal}(L : M) \simeq H$.

Solution: [B] True.

Continued...

4. (a) (4 marks) [B] State the Fundamental Theorem of Galois Theory.

Solution: Suppose that $L : K$ is finite. Let $G = \mathrm{Gal}(L : K)$, and let $K_0 = \phi(G)$, the set of elements of L fixed by the action of G. Also, when M is a field intermediate between L and K_0, let $\gamma(M) = \mathrm{Gal}(L : M)$. Then (i) The map ϕ from the set of subgroups of G onto the set of fields intermediate between L and K_0 is injective, and γ is the inverse map; (ii) A subgroup H of G is normal if and only if $\phi(H) : K_0$ is a normal extension; (iii) Suppose that $H \lhd G$. Then whenever $\sigma \in G$, one has $\sigma|_{\phi(H)} \in \mathrm{Gal}(\phi(H) : K_0)$. Furthermore, the map $\sigma \to \sigma|_{\phi(H)}$ is a homomorphism of G onto $\mathrm{Gal}(\phi(H) : K_0)$ with kernel H, so that $\mathrm{Gal}(\phi(H) : K_0) \simeq G/H$.

(b) (4+4+4 marks) [$\approx$ H+U] Let $L : \mathbb{Q}$ be a splitting field extension for $f(X) = (X^2 - 2)(X^2 + 7)$.

(i) Determine the degree of the extension $L : \mathbb{Q}$, justifying your answer.

Solution: One has $L = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$. We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$. The minimal polynomial for $\sqrt{-7}$ over $\mathbb{Q}(\sqrt{2})$ divides $X^2 + 7$. Since $\sqrt{-7} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, one sees that $X^2 + 7$ has no root in $\mathbb{Q}(\sqrt{2})$, and hence is irreducible over $\mathbb{Q}(\sqrt{2})$. Thus $[L : \mathbb{Q}(\sqrt{5})] = 2$, and so

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

(ii) Describe the Galois group $\mathrm{Gal}(L : \mathbb{Q})$ (that is, give generators and relations for the Galois group).

Solution: The group $\mathrm{Gal}(L : \mathbb{Q})$ is generated by σ and τ, where these maps fix $\mathbb{Q}$ pointwise, and $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{-7}) = \sqrt{-7}$, and $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{-7}) = -\sqrt{-7}$. Thus $\sigma\tau(\sqrt{2}) = \tau\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma\tau(\sqrt{-7}) = \tau\sigma(\sqrt{-7}) = -\sqrt{-7}$. Then σ, τ, $\sigma\tau$ each have order 2, and $\mathrm{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau : \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iii) Apply the Fundamental Theorem of Galois Theory to find all fields M for which $\mathbb{Q} \subsetneq M \subsetneq L$, explaining carefully how you applied the Fundamental Theorem in this process.

Solution: We know that $\mathrm{Gal}(L : \mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. The fields M that we are to find are the fixed fields of the subgroups $H_1 = \langle \sigma \rangle$, $H_2 = \langle \tau \rangle$, and $H_3 = \langle \sigma\tau \rangle$. With M_i the fixed field of H_i, we have $M_1 = \mathbb{Q}(\sqrt{-7})$, $M_2 = \mathbb{Q}(\sqrt{2})$, $M_3 = \mathbb{Q}(\sqrt{-14})$.

(c) (5+4 marks) [U] Let $K : \mathbb{Q}$ be a splitting field extension for $g(X) = X^4 - 5$.

(i) Show that $[K : \mathbb{Q}] = 8$.

Solution: Let $\alpha = 5^{1/4} \in \mathbb{R}$, and let $\zeta \in \mathbb{C}$ be a primitive 4th root of unity. By Eisenstein's Criterion (with $p = 5$), one sees that g is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Further, one has $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, since ζ is a root of $\Phi_4 = X^2 + 1$ (which is irreducible over $\mathbb{Q}$). So $[K : \mathbb{Q}(\alpha)] = 1$ or 2. But $\zeta \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, so that $X^2 + 1$ must be irreducible over $\mathbb{Q}(\alpha)$. Hence we have $[K : \mathbb{Q}(\alpha)] = 2$, and so the Tower Law gives

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 4 = 8.$$

Continued...

(ii) Describe the Galois group $\mathrm{Gal}(K : \mathbb{Q})$.

Solution: The Galois group $\mathrm{Gal}(L : \mathbb{Q})$ is generated by σ and τ, where σ and τ leave $\mathbb{Q}$ fixed pointwise, and $\sigma(\alpha) = \alpha\zeta$ and $\sigma(\zeta) = \zeta$, and $\tau(\alpha) = \alpha$ and $\tau(\zeta) = \zeta^3 = -\zeta$. Thus $\mathrm{Gal}(K : \mathbb{Q}) = \langle \sigma, \tau : \sigma^4 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle$.

5. (a) (2+3 marks) [B] Let K be a finite field.

(i) Define the Frobenius map on K.

Solution: The Frobenius map $\sigma : K \to K$ is defined by $\sigma(\alpha) = \alpha^p$, where p is the characteristic of K.

(ii) Let $m = |K|$. Show that every element of K is a root of the polynomial $t^m - t$.

Solution: We know that $K^\times$ is a multiplicative group of order $m - 1$. Thus, for any $\beta \in K \setminus \{0\}$, we have $\beta^{m-1} = 1$. Thus, for any $\beta \in K$, we have that $\beta^m = \beta$, and so β is a root of the polynomial $X^m - X$.

(b) (2+2+6 marks) [U/≈H] Let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. Put $f(t) = t^p - t + 1$, and let $K = \mathbb{F}_p(\alpha)$, where α is a root of f.

(i) Show that for all $\xi \in \mathbb{F}_p$, the element $\alpha + \xi$ is a root of f.

Solution: When $\xi \in \mathbb{F}_p$, one has

$$(\alpha + \xi)^p - (\alpha + \xi) + 1 = (\alpha^p - \alpha + 1) + (\xi^p - \xi) = 0.$$

Here we used that $\alpha^p - \alpha + 1 = 0$, and by Fermat's Little Theorem also $\xi^p = \xi$.

(ii) Let σ be the Frobenius map on K. Show that for $1 \leq d < p$, one has that $\sigma^d(\alpha)$ is a root of f.

Solution: Observe first that $\sigma(\alpha) = \alpha^p = \alpha - 1$, since $\alpha^p - \alpha + 1 = 0$. It therefore follows by induction that $\sigma^d(\alpha) = \alpha - d$ for each positive integer d, and by part (i) one sees that $\alpha - d$ is a root of f for any $d \in \mathbb{F}_p$.

(iii) Show that f is irreducible over $\mathbb{F}_p$.

Solution: Since $\sigma \in \mathrm{Gal}(K : \mathbb{F}_p)$, we have $\sigma^d \in \mathrm{Gal}(K : \mathbb{F}_p)$ (or equivalently, since σ fixes $\mathbb{F}_p$ pointwise, so too does σ^d). Thus σ^d leaves $m_\alpha(\mathbb{F}_p)$ fixed, and hence maps roots of $m_\alpha(\mathbb{F}_p)$ to roots of $m_\alpha(\mathbb{F}_p)$. Then $\alpha - d = \sigma^d(\alpha)$ must be a root of $m_\alpha(\mathbb{F}_p)$. Then $\alpha, \alpha - 1, \ldots, \alpha - (p-1)$ are distinct roots of $m_\alpha(\mathbb{F}_p)$, whence $\deg(m_\alpha(\mathbb{F}_p)) \geq p$. But we have also that $m_\alpha(\mathbb{F}_p)$ divides f, and thus it follows that $\deg(f) = p$. But f is monic, and so $f = m_\alpha(\mathbb{F}_p)$, which is irreducible.

(c) (2+3+3+2 marks) [B/H] Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $L = \mathbb{F}_p(t)$ be the field of fractions associated to the polynomial ring $\mathbb{F}_p[t]$.

(i) Let M denote a splitting field for the polynomial $X^p - t \in L[X]$. Show that for some $\beta \in M$, one has $X^p - t = (X - \beta)^p$.

Solution: Write $h(x) = x^p - t$. Since M is a splitting field for h, there exists some $\beta \in M$ with $h(\beta) = 0$. In particular, one has $\beta^p = t$. But since the binomial coefficients $\binom{p}{r}$ are divisible by p, and hence zero in $\mathbb{F}_p$ for $1 \leq r < p$, we have $(X - \beta)^p = X^p - \beta^p = X^p - t$.

Continued...

(ii) For the sake of contradiction (to be derived in (iii)), suppose that $X^p - t = fg$, where f and g are monic polynomials in $L[X]$ of positive degree. Show that one must have $f = (X - \beta)^s$ for some integer s with $1 \leq s \leq p - 1$, and deduce that $\beta^s \in L$.

Solution: If h factors in the shape $X^p - t = fg$ over $L[X]$, then over $M[X]$ one has $fg = (X - \beta)^p$. Then by the uniqueness of factorisations in a polynomial ring, one finds that $f = (X - \beta)^s$ for some non-negative integer s. But by hypothesis, the polynomials f and g each have positive degree, and so $1 \leq s \leq p-1$. Since $f \in L[X]$, it follows that the constant coefficient of f, namely $(-\beta)^s$, lies in L, whence $\beta^s \in L$.

(iii) Now show that $\beta \in L$, and hence obtain a contradiction to the above factorisation of $X^p - t$

Solution: One has $\beta^p = t \in L$ and $\beta^s \in L$. Since p and s are coprime, there exist integers u and v with $us + pv = 1$, whence $\beta = (\beta^s)^u(\beta^p)^v \in L$. But then there exist non-zero polynomials $a, b \in \mathbb{F}_p[t]$ with $\beta = a/b$. This implies that $t = \beta^p = a^p/b^p$, whence $a^p = tb^p$. The degree of the polynomial on the left hand side of the last relation is divisible by p, while on the right hand side the degree is congruent to 1 modulo p, a contradiction. This establishes that the hypothesised factorisation does not in fact exist.

(iv) Prove that $[M : L] = p$.

Solution: Parts (ii) and (iii) show that the polynomial h is irreducible over L. On the other hand, since $h = (X - \beta)^p$, it is apparent that a splitting field for h is $L(\beta)$ and that h is the minimal polynomial of β over L. Then $[M : L] = [L(\beta) : L] = \deg h = p$.

End of examination.