IMPERIAL

MATH70037

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Galois Theory

Date: Friday, May 10, 2024

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

You may use all results from the course, including lectures, lecture notes, problems sheets and courseworks without proof, unless otherwise specified. You may also use the assertions of previous parts of a question in solving later ones, without proof. All parts require full justification unless noted to the contrary.

A Galois extension means a finite, normal, and separated field extension. The automorphism group of a field extension $K \subseteq L$ refers to $\mathrm{Aut}_K(L)$.

1. True/False: mark with (T) or (F). No justification is needed or marked. You are free to guess though, there will be no penalty.

   (a) Let $f \in \mathbb{Z}[x]$ be a monic polynomial, and $g \in \mathbb{Q}[x]$ a monic factor. Then $g \in \mathbb{Z}[x]$. (2 marks)

   (b) Let $f \in \mathbb{Z}[x]$ be a polynomial and suppose that f is irreducible in $\mathbb{Q}[x]$. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is monic. (2 marks)

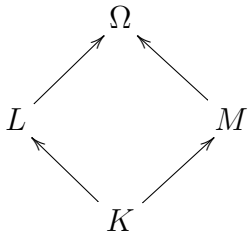
   (c) If $f \in \mathbb{Z}[x]$ is a polynomial whose reduction modulo p is separable, then f is separable. (2 marks)

   (d) Suppose that $f \in \mathbb{Z}[x]$ has degree n and that the automorphism group of the splitting field of f does not contain an n-cycle. Then for every prime p, if the reduction of f modulo p is separable, it is also reducible. (2 marks)

   (e) If $K \subseteq L \subseteq M$ are field extensions and $K \subseteq L$ and $L \subseteq M$ are normal, then so is $K \subseteq M$. (2 marks)

   (f) Suppose that $b \in \mathbb{Q}$ is not a square. Then the field $\mathbb{Q}(\sqrt{a+\sqrt{b}})$ is not a normal extension of $\mathbb{Q}$. (2 marks)

   (g) Consider the following tower of fields:

   Suppose that $[L : K] < \infty$. Then there is a subfield $\Omega' \subseteq \Omega$ containing both L and M with $[\Omega' : M] \leq [L : K]$. (2 marks)

   (h) Let $f \in K[x]$ be a polynomial of degree n with discriminant not a square. Then the automorphism group of the splitting field of f acts transitively on its roots. (2 marks)

   (i) Suppose that $K \subseteq L$ is a Galois extension with cyclic automorphism group of order n. Then $L = K(\sqrt[n]{a})$ for some $a \in K$ and $\sqrt[n]{a}$ some n-th root of a in L. (2 marks)

   (j) Suppose that $K \subseteq L = K(x, y)$ for some $x, y \in L$. Suppose $C_n = \langle g \rangle$ acts on L by automorphisms fixing K, such that $g \cdot x = \zeta x$ and $g \cdot y = \zeta^{-1} y$, where $\zeta \in K$ is a primitive n-th root of unity (meaning its multiplicative order is n). Then $K(x^n, xy, y^n) \subseteq K(x, y)$ is a Galois extension. (2 marks)

(Total: 20 marks)

2. (a) Factor completely the following polynomials over $\mathbb{Q}$:

(i) $x^{2024} - 2x^{2023} + 7x - 14$ (3 marks)

(ii) $x^4 - 6x^2 + 4$ (3 marks)

(iii) $x^6 - 1$. (3 marks)

[Hint for (iii): use cyclotomic polynomials.]

(b) Let $K \subseteq L$ be an extension of degree three. Show that $L = K(\alpha)$ for α the root of a cubic polynomial $f \in K[x]$. Supposing further that f is separable, show that L is the splitting field of f if and only if the discriminant of f is a square in K. (5 marks)

(c) Suppose that K contains a primitive cube root of unity (i.e., an element whose multiplicative order is three), and that $K \subseteq L$ is a Galois extension of degree three. Then show that L is the splitting field of a polynomial of the form $x^3 - a \in K[x]$. (3 marks)

(d) Suppose that $K \subseteq L \subseteq M$ are fields, $L \subseteq M$ is a finite extension, and $K \subseteq M$ is a normal extension. Show that every K-linear embedding $L \to M$ extends to an automorphism of M. (3 marks)

(Total: 20 marks)

3. (a) Compute the automorphism groups of the splitting fields of the following polynomials and find all intermediate fields (expressing them with explicit generator(s)).

(i) $x^3 + 4 \in \mathbb{Q}[x]$. (5 marks)

(ii) $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \in \mathbb{Q}[x]$. (5 marks)

(iii) $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. (5 marks)

(b) Find the automorphism group (but not intermediate fields) for the splitting field of $x^4+x+1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.
You should use the theory of Frobenius lifts (and do not use cubic resolvents). (5 marks)

(Total: 20 marks)

4. (a) Let $K \subseteq M$ be a Galois extension of order $p^m n$ for p prime and $p \nmid n$. Show that there is a subextension $K \subseteq L \subseteq M$ with $[L : K] = n$. Further, in the case $n = 1$, show that there is a subextension $K \subseteq L \subseteq M$ with $[L : K] = p$.

[Hint: Remember the Sylow theorem which states that given a group G of order $p^m n$ with p prime and n coprime to p, there exists a subgroup $H \leq G$ of order p^m. Also, there is another theorem stating that in a group of order p^m, there is a subgroup of index p.] (2 marks)

(b) Let p be a prime number, and let K be a field with the property that every extension of order not a multiple of p is trivial. Let $K \subsetneq L \subsetneq M$ be a tower of Galois extensions, with $K \subseteq M$ normal. Prove that there is a subextension $L \subseteq L' \subseteq M$ with $[L' : L] = p$.

[Hint: Use the previous part.] (4 marks)

(c) Now assume only that $K \subseteq M$ is a normal extension of order $p^m n$ for p prime and $p \nmid n$ (K can have any characteristic). Show that there is still a subextension $K \subseteq L \subseteq M$ with $[L : K] = n$.

[Hint: Use the following facts from the course:
1) Any finite extension $K_1 \subseteq K_2$ with $[K_2 : K_1]_s = 1$ is generated by iterated p-th root extensions, for $p > 0$ the characteristic of K_1;
2) For any finite normal extension $K \subseteq M$, there is a maximal subextension $K \subseteq M' \subseteq M$ such that $K \subseteq M'$ is separable, and $[M : M']_s = 1$;
3) For any finite normal extension $K \subseteq M$, there is a minimal subextension $K \subseteq M' \subseteq M$ such that $M' \subseteq M$ is separable, and it satisfies $[M' : K]_s = 1$.] (8 marks)

(d) Let $K = \mathbb{F}_p$ for p prime, $f \in K[x]$ be irreducible of degree n, L be a splitting field, and α_i be the roots of f in L (in any ordering).

(i) Show that α_i is a power of α_1 for all i. (3 marks)

(ii) Now suppose that α_i has multiplicative order m. Then show that $\deg f$ is the multiplicative order of p modulo m. (3 marks)

(Total: 20 marks)

5. Suppose that $K \subseteq L$ is a degree two field extension, and $L \subseteq M$ is a Galois extension of degree n.

(a) Show that there is a further extension M' of M such that $K \subseteq M'$ is normal and $[M' : K] \leq 2n^2$.
[Hint: Divide into cases whether L is or is not separable over K.] (5 marks)

(b) Now suppose that $K \subseteq M$ is Galois. Moreover, let $n = p$ be an odd prime. Finally, assume K contains a primitive p-th root of unity (an element whose multiplicative order is p). Then show that either $M = K(\sqrt[p]{a + \sqrt{b}})$ or $M = K(\sqrt[p]{a}, \sqrt{b})$ for some $a, b \in K$. (4 marks)

(c) Continue with the assumptions of (b). Prove that $\mathrm{Aut}_K M \cong D_p$ (the dihedral group of order $2p$) only if $M = K(\sqrt[p]{a + \sqrt{b}})$ and $a^2 - b$ is a p-th power in K.
[Hint: note that D_p does not have a normal subgroup of order 2.] (6 marks)

(d) Conversely, under the assumptions of (b), suppose that $M = K(\sqrt[p]{a + \sqrt{b}})$ and that $a^2 - b$ is a p-th power in K. Show that $\mathrm{Aut}_K M \cong D_p$. (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

This paper is also taken for the relevant examination for the Associateship.

MATH60037/70037

Galois Theory (Solutions)

Setter's signature	Checker's signature	Editor's signature
.....	.....	.....

1. (a) T (Gauss's Lemma: any primitive integral factor in $\mathbb{Q}[x]$ is also a factor in $\mathbb{Z}[x]$, and since f is monic it will have leading coefficient ± 1, hence be $\pm g$.)

seen ⇓

2, A

(b) F (It can have leading coefficient ± 1.)

sim. seen ⇓

2, B

(c) T (If two roots are equal, they remain so modulo p.)

sim. seen ⇓

2, A

(d) T (If the reduction modulo p is separable and irreducible, then, by Frobenius lifting, there is an n-cycle in the Galois group of the splitting field of f.)
Remark: if the reduction is inseparable, it is automatic that the reduction is also reducible, since it will be the p-th power of a polynomial, so the separability assumption is actually unnecessary.

sim. seen ⇓

2, B

(e) F (This is false, for example $\mathbb{Q}(\sqrt{a+\sqrt{b}}) \supseteq \mathbb{Q}(\sqrt{b}) \supseteq \mathbb{Q}$ when $b, c = a^2 - b$, and bc are all nonsquares, and the largest field is not a normal extension of $\mathbb{Q}$ as its Galois closure is the degree eight extension $\mathbb{Q}(\sqrt{a \pm \sqrt{b}})$.)

seen ⇓

2, A

(f) F (This is false because, for example, $\mathbb{Q}(\sqrt{5+\sqrt{5}})$ is normal, since $c = a^2 - b = 20$ and $b = 5$ are nonsquares but $bc = 100$ is a square, or explicitly because $\sqrt{5-\sqrt{5}} = \frac{2\sqrt{5}}{\sqrt{5+\sqrt{5}}} \in \mathbb{Q}(\sqrt{5+\sqrt{5}})$.)

sim. seen ⇓

2, A

(g) T (This is a theorem in the lecture notes, stated differently.)

sim. seen ⇓

2, A

(h) F (The discriminant not being a square means the Galois group is not in A_n, but it has nothing to do with transitivity, i.e., irreducibility of f.)

sim. seen ⇓

2, A

(i) F (This requires K to contain a primitive n-th root of unity to hold in general. For a counterexample, take $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ over $K = \mathbb{Q}$, which we saw in lectures is Galois with cyclic Galois group C_4, but is not generated by $\sqrt[4]{a}$ for any a, since this would have to be imaginary and imaginary numbers are not in L.)

sim. seen ⇓

2, A

(j) T (This is the fixed subfield for C_n, and $F \supseteq F^G$ is always Galois as we proved in lecture when $G \leq \mathrm{Aut}(F)$ is finite.)

sim. seen ⇓

2, A

2. (a) (i) We can first apply the rational root test: all rational roots are in the set $\{\pm 1, \pm 2, \pm 7, \pm 14\}$. A quick inspection shows that 2 is a root. Factoring this out yields $(x^{2023}+7)(x-2)$. The first factor is irreducible by Eisenstein, so this is the final factorisation. meth seen ⇓ 3, A

(ii) Applying our biquadratic theory we get that this has the form $(x^2-3)^2-5$, and the Galois group of its splitting field is $\mathbb{Q}(\sqrt{3\pm\sqrt{5}})$. So $a=3, b=5, c=4$, so b, bc are not squares but c is a square, and $2a \pm 2\sqrt{c} = 6 \pm 4$ are also not squares. So the Galois group is $C_2 \times C_2$ which acts transitively by our biquadratic theory. Hence this polynomial is irreducible. (However by our Frobenius lifting theory it will be reducible modulo every prime!) meth seen ⇓ 3, C

(iii) This has as its roots the sixth roots of unity, so factors into the cyclotomic polynomials as follows: $x^6-1 = \prod_{k|6} \Phi_k(x) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. It is also ok to leave these in terms of the $\Phi_k(x)$ if they are difficult to compute. For $\Phi_6(x)$ note that $\Phi_6(x) = \Phi_3(-x)$ since $-\omega$ is a primitive sixth root of unity. It is easy to check these are irreducible, but they also are because of the general theorem on cyclotomic polynomials. unseen ⇓ 3, B

(b) For the first assertion, if $\alpha \in L \setminus K$, the minimal polynomial must have degree three by the tower law. sim. seen ⇓

Next, if L is the splitting field of f and f is separable, then the Galois group is $A_3 \leq S_3$, which happens precisely when the discriminant of f is a square. Conversely if the discriminant is a square, then the splitting field of f has degree three, so must equal L. 2, A 3, B

(c) If this is a Galois extension of degree three, it has Galois group C_3, and since there are primitive cube roots of unity, Kummer theory implies that L is the splitting field of x^3-a for some a. seen ⇓ 3, A

(d) We can apply our result on towers of extensions (Lemma 4.2.3 of the current notes): since $L \subseteq M$ is finite, we have that the restriction map $\mathrm{Aut}(M) \to \mathrm{Emb}_K(L, M)$ is surjective. sim. seen ⇓ 3, B

3. Note that for the examples in $\mathbb{Q}$, it follows from the fact that $\mathbb{Q}$ is perfect that all finite extensions are separable, hence we only need to check normality.

(a.i) The splitting field is generated by $\sqrt[3]{4}$ and a primitive cube root of unity. So the degree of the extension L is six (the first generates a cubic subextension and the second a quadratic one). Hence the splitting field Galois group is S_3, by Galois theory, the maximum group.

sim. seen ⇓

2, A

The subfields are in bijection with the subgroups of S_3, so we have (aside from $\mathbb{Q}$ and the whole extension) one quadratic extension of $\mathbb{Q}$, $\mathbb{Q}(\omega)$, and three cubic, non-normal extensions, which here we could take to be $\mathbb{Q}(\sqrt[3]{4}), \mathbb{Q}(\omega\sqrt[3]{4})$, and $\mathbb{Q}(\omega^2\sqrt[3]{4})$.

meth seen ⇓

3, B

(a.ii) This is the cyclotomic polynomial $\Phi_7(x)$. Let L be its splitting field. We showed in the course that L was irreducible with Galois group $(\mathbb{Z}/7\mathbb{Z})^\times \cong C_6$.

seen ⇓

2, A

There are therefore two properly intermediate fields: L^{C_2} and L^{C_3}. They are each generated by any element not in $\mathbb{Q}$, as they have prime orders so have no properly intermediate fields, so we can take $L^{C_2} = \mathbb{Q}(\zeta + \zeta^{-1})$ and $L^{C_3} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

meth seen ⇓

3, C

(a.iii) To do this, first note that there are no roots (0 or 1), next that the only irreducible quadratic, x^2+x+1, is not a factor of this polynomial ($x^4+x^3+1 \neq (x^2+x+1)^2 = x^4+x^2+1$). So the polynomial is irreducible. Now its Galois group is automatically C_4, as finite extensions of finite fields are automatically Galois with cyclic Galois group.

seen ⇓

2, A

There is only one properly intermediate field, since there is only one proper nontrivial subgroup of C_4. To find it, write the splitting field as $M = \mathbb{F}_2[b]$ for $b^4+b^3+1 = 0$. We know that $M \cong \mathbb{F}_{16}$. The intermediate field is then $L \cong \mathbb{F}_4$. Explicitly, since $b \notin L$ we have that $b^3 \neq 1$, rather the multiplicative order of b is 5 or 15. It is not 5 since $b^5 - 1$ is not a multiple of $b^4 + b^3 + 1$. So it is 15. Then to get an element of order 3 we can take b^5. So $\mathbb{F}[b^5] = L$.

meth seen ⇓

3, C

(b) Reducing modulo 2, this polynomial, call it f, is irreducible, because it has no roots and is not $(x^2+x+1)^2 = x^4+x^2+1$. It is also separable there since its derivative is 1. So by the theory of Frobenius lifts, there is a cyclic permutation of order four in the Galois group of f over $\mathbb{Q}$. Next, we can reduce modulo three, where the result factors as $x^4 + x + 1 = (x-1)(x^3 + x^2 + x - 1)$. It is separable since, for $f = x^4 + x + 1$, we have $f' = x^3 + 1 = (x+1)(x^2 - x + 1)$ and so $\gcd(f, f') = 1$. So by the theory of Frobenius lifting we have also a three-cycle in the Galois group of the splitting field of f. Given a three-cycle and a four-cycle we get a group of order at least 12, so can get either A_4 or S_4 as the Galois group. But since the four-cycle is odd we can't get A_4, it must be S_4.

sim. seen ⇓

5, D

4. (a) By the Sylow theorem mentioned in the hint, we have that the Galois group $G = \mathrm{Aut}_K M$ has a subgroup $H \leq G$ with $|H| = p^m$. Then $[M^H : K] = n$. Next, if $n = 1$, using the second theorem we can find H with $[G : H] = p$. Then $[M^H : K] = p$.

sim. seen ⇓

2, A

(b) Let $[M : K] = p^m n$ for $p \nmid n$. Note that $M \supseteq K$ is separable since $L \supseteq K$ and $M \supseteq L$ are, and hence it is Galois. By (a), there is a subextension of M of degree n over K. By the assumption, it follows that $n = 1$, so $[M : K] = p^m$. By the tower law, $[M : L]$ is also a power of p. By (a) again, we can find a subextension L' with $[L' : L] = p$.

sim. seen ⇓

4, B

(c) There are two cases: where p is the characteristic, or where it is not the characteristic. If it is the characteristic, then for $M \supseteq K$, by Hint.(2), we can let L be a maximal intermediate field with $L \supseteq K$ separable, so that $[M : L]_s = 1$. It follows from Hint.(1) that $[M : L]$ is a power of p. Thus $L \supseteq K$ is Galois and has the same value of n as M, and we are reduced to (a).

unseen ⇓

4, D

Next consider the case where p is not the characteristic. Let the characteristic be q. If $q = 0$ we are in the situation of (a) since all finite extensions are separable. Otherwise, by Hint.(3), we can let L be a minimal subextension with $M \supseteq L$ separable, and $[L : K]_s = 1$. By Hint.(1), L is generated over K by adjoining q-th powers of elements. In particular $[L : K]$ is of order a power of q. Applying (a) we can find $L' \supseteq L$ in M with $[L' : L] = n/[L : K]$. Then $[L' : K] = n$ by the tower law.

4, D

(d) (i) The roots are obtained from each other by action of the Galois group. This group acts by powers of the Frobenius automorphism. Since the Frobenius automorphism takes an element to its p-th power, we obtain the desired statement.

unseen ⇓

3, C

(Alternatively, one can prove this using the fact that the multiplicative group of nonzero elements in L is cyclic.)

(ii) Now we have that the roots are $\alpha_1, \alpha_1^p, \alpha_1^{p^2}, \ldots$, and we get that if there are k roots, then $\alpha_1^{p^k} = \alpha_1$, and conversely. This is just saying that $p^k \equiv 1 \pmod{m}$.

3, D

(Alternative proof: since $|L| = p^k$ for k the number of roots, we certainly have $m \mid p^k - 1$ working in the multiplicative group $L^\times$. Also, $m \nmid p^j - 1$ for $j \mid k$ since α_1 is not in a proper subfield.)

5. (a) Write $L = K(b)$ for $b^2 \in K$. Since $L \subseteq M$ is Galois, it is the splitting field of a polynomial $f \in L[x]$. First, if $K \subseteq L$ is separable, let $\sigma \in \mathrm{Aut}_K L$ be the nontrivial element. We then have that $f\sigma(f) \in L^\sigma[x] = K[x]$. Let M' be the splitting field of $f\sigma(f)$. Then M' is normal. Moreover, $\sigma(M) \subseteq M$ is a field also of degree n over K, and $M' = M\sigma(M)$. We get that $[M' : L] \leq [M : L][\sigma(M) : L] = n^2$. By the tower law, $[M' : K] \leq 2n^2$. sim. seen ⇓ 3, M

Next, if $K \subseteq L$ is inseparable, then it has characteristic two. In this case, by the Fresher's Dream, $f^2 \in K[x]$. Since f and f^2 have the same roots, M is the splitting field of $f^2(x-b)^2$. Thus it is normal. So we can take $M = M'$. 2, M

(b) First, $L \supseteq K$ is a degree two extension and hence $L = K(\sqrt{b})$ for some b. Next, since $M \supseteq L$ is a Galois extension (as $M \supseteq K$ is Galois) of order p, it is cyclic. Since L contains a primitive p-th root of unity, M is given from L by adjoining the p-th root of an element, i.e., $\sqrt[p]{a + c\sqrt{b}}$ for some $c \in K$. sim. seen ⇓ 2, M

Suppose that $c \neq 0$. Then we can replace b by $c^2 b$ and we get $M = L(\sqrt[p]{a + \sqrt{b}})$. Since $L = K(\sqrt{b})$ and $\sqrt{b} = (\sqrt[p]{a + \sqrt{b}})^p - a$, we get that $M = K(\sqrt[p]{a + \sqrt{b}})$. 1, M

Next suppose that $c = 0$. Then $M = L(\sqrt[p]{a}) = K(\sqrt{b}, \sqrt[p]{a})$. 1, M

(c) First note that the Galois group of the extension $K(\sqrt{b}, \sqrt[p]{a})$ has elements determined by their actions on $\sqrt{b}, \sqrt[p]{a}$, where they have the form $\sqrt{b} \mapsto \pm\sqrt{b}$ and $\sqrt[p]{a} \mapsto \zeta^k \sqrt[p]{a}$ where ζ is a primitive p-th root of unity. The group of all such transformations has order $2p$ and is isomorphic to C_{2p}. So in this case we cannot get D_p. meth seen ⇓ 3, M

Next in the case $M = K(\sqrt[p]{a + \sqrt{b}})$, we similarly get that every conjugate must send $\sqrt{b}$ to $\pm\sqrt{b}$ and, knowing this, $\sqrt[p]{a + \sqrt{b}}$ to $\zeta^k \sqrt[p]{a \pm \sqrt{b}}$ for some k. As the Galois group has order $2p$, all of these possibilities must occur, so that M contains $K(\sqrt[p]{a^2 - b})$. As K contains the p-th roots of unity, the extension is Galois with group a subgroup of C_p, hence equal to C_p unless $a^2 - b$ is a p-th power. On the other hand, this Galois group is a quotient of G, and D_p does not have C_p as a quotient (for $p \geq 3$). Thus we obtain that $a^2 - b$ must be a p-th power. 3, M

(d) If $a^2 - b$ is a p-th power, then we get from unseen ⇓

$$(\zeta^k \sqrt[p]{a + \sqrt{b}})(\zeta^{-k} \sqrt[p]{a - \sqrt{b}}) = \sqrt[p]{a^2 - b} \in K,$$

that every Galois automorphism of M over K must preserve each ordered pair $(\zeta^k \sqrt[p]{a + \sqrt{b}}, \zeta^{-k} \sqrt[p]{a - \sqrt{b}})$. Now if we let $\sigma, \tau \in G$ be given by $\sigma(\sqrt{b}) = -\sqrt{b}, \sigma(\sqrt[p]{a + \sqrt{b}}) = \sqrt[p]{a - \sqrt{b}}$ and $\tau(\sqrt{b}) = \sqrt{b}$, $\tau(\sqrt[p]{a + \sqrt{b}}) = \zeta \sqrt[p]{a + \sqrt{b}}$, then we get

$$\sigma\tau\sigma^{-1} \sqrt[p]{a + \sqrt{b}} = \sigma\tau \sqrt[p]{a - \sqrt{b}} = \zeta^{-1} \sqrt[p]{a - \sqrt{b}} = \zeta^{-1} \sqrt[p]{a + \sqrt{b}} = \tau^{-1} \sqrt[p]{a + \sqrt{b}}.$$

This is the relation for D_p. 5, M

Remark: for (d) we did not need to assume that $M \supseteq K$ was Galois, as long as the characteristic is not 2 or p, since it follows from the formula for M and the fact that $a^2 - b$ is a p-th power in K that M is normal, and from the assumption on characteristic the extension is separable.

Review of mark distribution:
Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 100 of 80 marks
Total Mastery marks: 20 of 20 marks

MATH60037 Galois Theory

Question	Marker's comment
1	Students scored well on this, with almost all students having at least seven of the ten true/false questions correct.
2	This question was one of the easier ones, with some students just having difficulty with proving that the decompositions they obtained in (a) are correct, and with the second part of (b), many did not think to consider the splitting field and try to show that it equals L under the hypotheses.nbsp; Also, for (c) some forgot about the Kummer theorem.
3	This question was a little more challenging. The hardest aspect was finding, in part (a), all the intermediate fields (for which one has to employ a deep understanding of the fundamental theorem of Galois theory).
4	This was the most difficult question of Q1--Q4. Challenging aspects included, in (b), employing (a) to show that the extension in question is of degree a power of p; in (c), to understand well enough the facts in the hint to give a generalistion of (a) to the case where extensions need not be separable; and in (d), to make use of the explicit description of the Galois group of finite fields as generated by the Frobenius automorphism.

MATH70037 Galois Theory

Question	Marker's comment
1	Students scored well on this, with almost all students having at least seven of the ten true/false questions correct.
2	This question was one of the easier ones, with some students just having difficulty with proving that the decompositions they obtained in (a) are correct, and with the second part of (b), many did not think to consider the splitting field and try to show that it equals L under the hypotheses.nbsp; Also, for (c) some forgot about the Kummer theorem.
3	This question was a little more challenging. The hardest aspect was finding, in part (a), all the intermediate fields (for which one has to employ a deep understanding of the fundamental theorem of Galois theory).
4	This was the most difficult question of Q1--Q4. Challenging aspects included, in (b), employing (a) to show that the extension in question is of degree a power of p; in (c), to understand well enough the facts in the hint to give a generalistion of (a) to the case where extensions need not be separable; and in (d), to make use of the explicit description of the Galois group of finite fields as generated by the Frobenius automorphism.
5	This question was challenging, and it also seemed that most students had little time left to attempt it.nbsp; Difficulties included: in part (a), the idea (briefly mentioned in lectures) of taking the minimal polynomial of M over L, and multiplying it by its conjugate under the Galois group of L over K; in part (b), the use of Kummer theory; and in part (d), explicitly considering the action of the dihedral group via automorphisms of the field.