Imperial College
London

MATH97034 MATH70037

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2022

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

Galois Theory

Date: 16 May 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 hours

Upload Time Allowed: 30 minutes

This paper has 5 Questions.

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

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS AS ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

N.B.

(1) Throughout this paper, all extensions of fields are assumed to be finite.

(2) This is an open-book exam. You are allowed to quote any of the results stated in the GALOIS THEORY notes, for example by number as in "[...] by Lemma 16(A) in the notes [...]."

(3) When answering a question, or part of a question, you are allowed to quote statements from other questions or parts even if you have not answered them.

1. For each of the following assertions, state whether it is true (T) or false (F). No justification is needed. You will be given a mark of $+2$ for every correct answer, -2 **for every incorrect answer**, and 0 for every answer that you leave blank. (If your total mark is negative you will be awarded 0 marks for the question.)

   (i) If $K \subset L$ is a field extension, then $[L : K] = 1$ if and only if K is isomorphic to L. (2 marks)

   (ii) If $K \subset L$ is a field extension where both K and L are finite fields, then $K \subset L$ is normal and separable. (2 marks)

   (iii) Let K be a field, $f(X) = X^4 + AX^2 + B \in K[X]$ a separable irreducible polynomial, $K \subset L$ its splitting field, and G the Galois group. Denote by D_8 the dihedral group of order 8. Then $G \cong D_8$ if and only the discriminant $\delta = \mathrm{disc}(f) \in K$ is not a square in K. (2 marks)

   (iv) Let K be a field of characteristic zero, $K \subset L$ a normal extension and Ge the Galois group. Then G is a cyclic group if and only if for some $a \in K$ $L = K(\sqrt[n]{a})$. (2 marks)

   (v) Let K be the splitting field over $\mathbb{Q}$ of the polynomial $X^4 + 8X^2 + 9$. The Galois group of $\mathbb{Q} \subset K$ is the cyclic group C_4. (2 marks)

   (vi) The polynomial $X^5 + 5X^2 + 125 \in \mathbb{Q}[X]$ is irreducible. (2 marks)

   (vii) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. There are 16 distinct subfields $F \subset K$ with $[F : \mathbb{Q}] = 4$. (2 marks)

   (viii) Let $K \subset L$ be a normal extension and write $G = \mathrm{Emb}_K(L, L)$. Then $K \subset L$ is a separable extension if and only if $K = \{a \in L \mid \text{for all } g \in G,\ g(a) = a\}$. (2 marks)

   (ix) Let $K \subset L$ be a normal and separable field extension with Galois group G. If a polynomial $f(X) \in K[X]$ splits completely over L, then G acts transitively on the set of roots of $f(X)$. (2 marks)

   (x) Let $f(X) \in \mathbb{Z}[X]$ be a polynomial. If $f(X)$ is separable over $\mathbb{Q}$, then there exists a prime number p such that the reduction of $f(X)$ mod p is separable over $\mathbb{F}_p$. (2 marks)

(Total: 20 marks)

2. In this question, consider a field extension $K \subset L$ and intermediate fields $K \subset F_1 \subset L$, $K \subset F_2 \subset L$ such that $F_1 \cdot F_2 = L$.

(a) Prove that $[L : K] \leq [F_1 : K][F_2 : K]$. (5 marks)

(b) Either prove or disprove: If $[F_1 : K]$, $[F_2 : K]$ are coprime, then $[L : K] = [F_1 : K][F_2 : K]$. (5 marks)

(c) For all positive integers n, write $K_n = \mathbb{Q}(e^{\frac{2\pi \mathrm{i}}{n}})$. Prove that if n, m are coprime, then $K_n \cap K_m = \mathbb{Q}$. (5 marks)

(d) Either prove or disprove: If $F_1 \cap F_2 = K$, then $[L : K] = [F_1 : K][F_2 : K]$. (5 marks)

(Total: 20 marks)

3. In this question, $K \subset L$ is a normal and separable extension with Galois group G, F is a given intermediate field $K \subset F \subset L$, and $H = F^\dagger \leq G$. The group G acts on the set $X = \mathrm{Emb}_K(F, L)$ via

$$G \times X \to X \quad \text{such that} \quad (g, x) \mapsto g \circ x$$

In answering the question, you are allowed to use the fact, proven in class, that this action is transitive.

(a) For $x \in X$, denote by G_x its stabiliser. Prove that $x(F)^\dagger = G_x$. (5 marks)

(b) Prove that for all $g \in G$, $g(F) = F$ as subfields of L if and only if $gHg^{-1} = H$. (5 marks)

(c) Prove that the extension $K \subset F$ is normal if and only if H is a normal subgroup of G. (5 marks)

(d) Let $N = \{g \in G \mid gHg^{-1} = H\}$. Show that N is a subgroup of G and that H is a normal subgroup of N. Prove that

$$\mathrm{Emb}_K(F, F) = N/H$$

(5 marks)

(Total: 20 marks)

4. In this question, denote by K the splitting field of the polynomial

$$f(X) = X^6 + 4X^3 + 1 \in \mathbb{Q}[X]$$

and by G the Galois group of the extension $\mathbb{Q} \subset K$. You may assume without proof that $f(X)$ is irreducible over $\mathbb{Q}$.

(a) Find all the roots of $f(X)$ and plot them on the complex plane. Show that $\sqrt{3} \in K$, and $\mathtt{i} \in K$. (5 marks)

(b) Use Part (a) to determine $[K : \mathbb{Q}]$. (5 marks)

(c) Describe the action of the group $H = \mathbb{Q}(\sqrt{3}, \mathtt{i})^\dagger$ on the roots of $f(X)$. (5 marks)

(d) Describe explicitly the action on the roots of $f(X)$ of all $g \in G$ such that $g(\mathtt{i}) = \mathtt{i}$ and $g(\sqrt{3}) = -\sqrt{3}$. (5 marks)

(Total: 20 marks)

5. In this question, $K = \mathbb{F}_2(t)$. Consider the tower of Artin–Schreier extensions $K \subset F \subset L$ where:

- $F = K(u)$ and $u^2 + u = t \in K$;
- $L = F(w)$ and $w^2 + w = tu \in F$.

You may assume without proof that both these extensions have degree 2.

(a) Find the minimal polynomial of $w + u$ in $F[X]$. (5 marks)

(b) Find the minimal polynomial $f(X)$ of w in $K[X]$. (5 marks)

(c) Find all the roots of $f(X)$ in L and hence show that $f(X)$ splits completely as a polynomial in $L[X]$. (5 marks)

(d) Let G be the Galois group of the extension $K \subset L$. Describe explicitly the action of an element $g \in G$ such that $g(u) = 1 + u$ and hence determine the structure of G. (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2022

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

MATH60037/70037/97034

Galois Theory (Solutions)

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

1. (i) False
   (ii) True
   (iii) False
   (iv) False
   (v) False
   (vi) True
   (vii) False
   (viii) True
   (ix) False
   (x) True

seen ⇓

2, A

seen ⇓

2, A

unseen ⇓

2, D

unseen ⇓

2, C

sim. seen ⇓

2, B

sim. seen ⇓

2, A

seen ⇓

2, B

unseen ⇓

2, C

sim. seen ⇓

2, B

seen ⇓

2, B

2. (a) We know that

unseen ⇓

$$F_1 \cdot F_2 = \Big\{ \sum_{i \in I \text{ finite}} a_i b_i \mid a_i \in F_1,\ b_i \in F_2 \Big\}$$

This implies: If $b_1, \ldots, b_n$ is a basis of F_2 as a vector space over K, then it is a generating set of $F_1 \cdot F_2$ over F_1. This in turn implies that $[F_1 \cdot F_2 : F_1] \leq [F_2 : K]$. The result follows from the tower law:

$$[L : K] = [F_1 \cdot F_2 : F_1][F_1 : K] \leq [F_2 : K][F_1 : K]$$

5, D

(b) By the tower law both $[F_1 : K]$ and $[F_2 : K]$ divide $[L : K]$ hence their product $[F_1 : K][F_2 : K]$ also divides $[L : K]$ hence by Part (a)

unseen ⇓

$$[F_1 : K][F_2 : K] \leq [L : K] \leq [F_1 : K][F_2 : K]$$

implying equality.

5, B

(c) It is clear that $K_n \cdot K_m = K_{nm}$. Write $F = K_n \cap K_m$ and let $c = [F : \mathbb{Q}]$: we want to show that $c = 1$, implying $F = \mathbb{Q}$. Write $c_1 = [K_n : F]$, $c_2 = [K_m : F]$ so that by the tower law $\varphi(n) = cc_1$ and $\varphi(m) = cc_2$. By Part (a) we have:

unseen ⇓

$$[K_{nm} : \mathbb{Q}] = \varphi(nm) = \varphi(n)\varphi(m) \leq cc_1c_2 = \varphi(n)c_2$$

hence $cc_2 = \varphi(m) \leq c_2$ implying $c = 1$.

5, C

(d) The statement is false. For example, if L is the splitting field of $X^3 - 2$ over $K = \mathbb{Q}$, then consider $F_1 = K(\sqrt[3]{2})$ and $F_2 = K(\omega\sqrt[3]{2})$. It is clear that $F_1 \cap F_2 = \mathbb{Q}$ (for example because $F_1 \cap F_2 \neq F_2$ e.g. because it is contained in $\mathbb{R}$, and then by the tower law $F_1 \cap F_2 = \mathbb{Q}$.) Also $F_1 \cdot F_2 = L$, for example because $\omega \in F_1 \cdot F_2$. However $[L : \mathbb{Q}] = 6$ is not $3 \times 3 = 9$.

seen ⇓

5, A

3. (a) $g \circ x = x$ if and only if for all $a \in F$ $g(x(a)) = x(a)$ if and only if (because $x\colon F \to x(F)$ is bijective) for all $b \in x(F)$ $g(b) = b$, if and only if $g \in x(F)^\dagger$. seen ⇓ 5, A

(b) By the Galois correspondence, $g(F) = F$ as subfields if and only if $g(F)^\dagger = F^\dagger$ as subgroups, if and only if (by Part (a) and the general fact that $G_{gx} = gG_xg^{-1}$) $gHg^{-1} = H$. seen ⇓ 5, A

(c) By definition $K \subset F$ is normal if and only if for all $F \subset \Omega$, and all $x \in \mathrm{Emb}_K(F, \Omega)$, $x(F) = F$. By Remark 17(i) in the GALOIS THEORY notes, it is enough to check this for a single given tower $K \subset F \subset \Omega$ where $K \subset \Omega$ is normal. We apply this with $L = \Omega$: $K \subset F$ is normal if and only if for all $x \in X$ $x(F) = F$, if and only if (because the action is transitive) for all $g \in G$ $g(F) = F$, if and only if (by Part (b)) for all $g \in G$ $gHg^{-1} = H$, if and only if H is normal. seen ⇓ 5, D

(d) Suppose $g, h \in N$, then first $hHh^{-1} = H$ implies $H = h^{-1}(hHh^{-1})h = h^{-1}Hh$, that is $h^{-1} \in N$. Then also $(gh^{-1})H(gh^{-1})^{-1} = g(h^{-1}Hh)g^{-1} = H$, that is, $gh^{-1} \in N$ and this shows that N is a subgroup, and it is obvious from the definition that $H \leq N$ is a normal subbroup. seen ⇓

Define $\psi\colon N \to \mathrm{Emb}_K(F, F)$ by $r(g) = g_{|F}$. By Part (b), if $g \in N$ then $g(F) = F$ as subfields, that is, $\psi(N) \in \mathrm{Emb}_K(F, F)$.

Consider any $x \in \mathrm{Emb}_K(F, F) \subset X$. Because the action is transitive, there is $g \in G$ such that $g_{|F} = x$, and by Part (b) (reverse implication) $g \in N$. By construction $\psi(g) = x$, that is, ψ is surjective.

$\mathrm{Ker}(\psi)$ consists of those $h \in N$ that act trivially on F, that is, $\mathrm{Ker}(\psi) = H$. 5, C

4. (a) Write as usual $\omega = \frac{-1+\mathtt{i}\sqrt{3}}{2}$. By the quadratic formula the roots are

sim. seen ⇓

$$a_i = \omega^i \sqrt[3]{-2-\sqrt{3}} \quad (i=0,1,2) \quad \text{and} \quad b_i = \omega^i \sqrt[3]{-2+\sqrt{3}} \quad (i=0,1,2)$$

In the plot the b_i are on triangle inscribed in a circle of radius < 1, and the a_i on a triangle inscribed in a circle of radius > 1. It is clear that $\sqrt{3} \in K$ (for example it is easily computable from a_i^3) and then, because $\omega = \frac{-1+\mathtt{i}\sqrt{3}}{2} \in K$, also $\mathtt{i} \in K$.

5, A

(b) $K = \mathbb{Q}(a_0, \mathtt{i})$ and, because $f(X)$ is irreducible and by the tower law: $[K:\mathbb{Q}] = [\mathbb{Q}(a_0,\mathtt{i}):\mathbb{Q}(a_0)][\mathbb{Q}(a_0):\mathbb{Q}] = 2\times 6 = 12$ (the first degree is 2 because $\mathtt{i} \notin \mathbb{Q}(a_0)$, given that $\mathbb{Q}(a_0) \subset \mathbb{R}$).

sim. seen ⇓

5, A

(c) Write $F = \mathbb{Q}(\sqrt{3}, \mathtt{i})$. The extension $F \subset K$ is the splitting field of the polynomial

$$f(X) = X^3 - 2 - \sqrt{3} \in F[X]$$

Moreover this polynomial is irreducible because otherwise $F = K$ contradicting $[K:\mathbb{Q}] = 12$ for example. Now F contains the 3rd roots of unity, thus $H = C_3$ is a cyclic group of order 3 where a generator acts as $a_i \mapsto \omega a_i$, $b_i \mapsto \omega b_i$. On the plot, this is a counterclockwise rotation with angle $\frac{2\pi}{3}$. (This can all be taken for granted from Kummer theory.)

5, B

(d) It is clear that $g(a_0) \in \{b_0, b_1, b_2\}$: indeed a_0 is a cube root of $-2-\sqrt{3}$ and hence g maps a_0 to one of the three cube roots of $g(-2-\sqrt{3}) = -2+\sqrt{3}$. Since G is transitive on the roots, we know that all must occur so there is a g such that $g(a_0) = b_0$. It follows from this that $g(a_i) = g(\omega^i a_i) = g(\omega)^i b_0 = \omega^{-i} b_0$: to be explicit, $g(a_1) = b_2$ and $g(a_2) = b_1$. I claim that $g(b_0) = a_0$: indeed, $a_0 b_0 = 1$ implies $g(a_0)g(b_0) = 1$. Then as before $g(b_1) = a_2$ and $g(b_2) = a_1$.

sim. seen ⇓

We have described one of the $g \in G$ in question. The other two are ωg and $\omega^2 g$.

5, D

5. (a) We compute: unseen ⇓

$$(w+u)^2+(w+u)=w^2+w+u^2+u=t+tu=t(1+u)$$

hence — because $w\notin F$ — the minimal polynomial is $X^2+X+t(1+u)\in F[X]$. 5, M

(b) By Artin–Schreier, the Galois group of the extension $K\subset F$ is cyclic of order two generated by the involution σ such that $\sigma(u)=u+1$. The minimal polynomial is unseen ⇓

$$\Big(X^2+X+tu\Big)\Big(X^2+X+\sigma(tu)\Big)=\Big(X^2+X+tu\Big)\Big(X^2+X+t(1+u)\Big)=$$
$$=X^4+(1+tu+t+tu)X^2+t^2(u^2+u)=X^4+(1+t)X^2+t^3$$

5, M

(c) By Part (b) the roots are $w,1+w,w+u,w+u+1$. unseen ⇓

(d) g maps w to either $w+u$ or $w+u+1$ (if $g(w)=w+1$, then $g(w+1)=w$ and then $g(w^2+w)=w^2+w$, so $g(u)=u$, a contradiction). Because G is transitive both are possible so let's assume that $g(w)=w+u$. Then $g(w+u)=g(w)+g(u)=w+u+u+1=w+1$, and $g(w+1)=g(w)+1=w+u+1$ and then also $g(w+u+1)=w$. It follows that g is a cycle of order 4. Because $|G|=[L:K]=4$ it follows that G is a cyclic group of order 4. 5, M unseen ⇓ 5, M

Review of mark distribution:
Total A marks: 31 of 32 marks
Total B marks: 18 of 20 marks
Total C marks: 14 of 12 marks
Total D marks: 17 of 16 marks
Total marks: 100 of 80 marks
Total Mastery marks: 20 of 20 marks

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.
Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a separate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
Galois Theory_MATH60037 MATH97034 MATH70037	1	There were many tricky bits into this question but several of the students did well.
Galois Theory_MATH60037 MATH97034 MATH70037	2	There is not much to say here. I thought that this was a difficult question but students did rather well.
Galois Theory_MATH60037 MATH97034 MATH70037	3	This question was done rather well by the students. It is an abstract question but the material was sufficiently emphasised during the lectures that many students did rather well.
Galois Theory_MATH60037 MATH97034 MATH70037	4	It seems that students found this question particularly difficult. I am not sure quite why that is since this is a variation on a well-understood, standar type of question. The "variation" was maybe rather elaborate.
Galois Theory_MATH60037 MATH97034 MATH70037	5	None of the students completed this question. The key point is that Artin-Schreier theory is about extensions of prime order p, but this extension has order 4, not a prime. The point of the question was to go beyond p=2. In my view the question was NOT too hard, but in retrospect perhaps students were confused by the exotic world of characteristic 2