Imperial College
London

MATH70037

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2023

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

## Galois Theory

Date: 15 May 2023

Time: 10:00 – 12:30 (BST)

Time Allowed: 2.5hrs

**This paper has 5 Questions.**

**Please Answer All Questions in 1 Answer Booklet**

Candidates should start their answers 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**

**N.B.**

(1) Throughout this paper all field extensions are finite.

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

(3) You are permitted to use without proof any statement that is proved in the written notes, provided that you make it clear which statement you are using. Unless instructed otherwise, you must justify all other statements that you make.

1. (a) Determine whether the polynomial $f(X) = X^5 + 3X^2 + 9 \in \mathbb{Q}[X]$ is irreducible. (4 marks)

   (b) Determine the number of monic irreducible polynomials of degree $10$ in $\mathbb{F}_2[X]$ (4 marks)

   (c) For $K$ a field and $f \in K[X]$ a separable polynomial, denote by $G(f)$ the Galois group of a splitting field of $f$. Either prove or disprove: If $f_1, f_2$ are separable, irreducible and coprime, then $G(f_1 f_2) = G(f_1) \times G(f_2)$. (4 marks)

   (d) Let $K$ be a splitting field of the polynomial $f(X) = X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$. Determine the Galois group of the extension $\mathbb{Q} \subset K$. (4 marks)

   (e) For a positive integer $n$, write $\zeta_n = e^{\frac{2\pi i}{n}}$ and $K_n = \mathbb{Q}(\zeta_n) \subset \mathbb{C}$. Either prove or disprove: If $n, m$ are coprime, then $K_n \cap K_m = \mathbb{Q}$. (4 marks)

(Total: 20 marks)

2. In this question $K$ is a field of characteristic $\neq 2$.

   (a) Let $K \subset F$ be a field extension. Prove that if $[F : K] = 2$ then there exists $a \in K$ such that $F = K(\sqrt{a})$. (2 marks)

   (b) For $a, b \in K$ consider the field extension $L = K(\sqrt{a}, \sqrt{b})$. Assume that $[L : K] = 4$.

      (i) Prove that the extension is normal and separable; (2 marks)

      (ii) determine the Galois group $G$ of the extension; (2 marks)

      (iii) draw a picture of the Galois correspondence showing all the subgroups of $G$ and the intermediate fields $K \subset F \subset L$ that they correspond to. (6 marks)

   (c) In the situation of Part (b), prove that $K(\sqrt{a} + \sqrt{b}) = L$.

   [*Hint. Use Part (b). Alternatively, consider the orbit of the element* $\sqrt{a} + \sqrt{b} \in L$ *under the Galois group.*]

   (4 marks)

   (d) In the situation of Part (b), find the minimal polynomial of $\alpha = \sqrt{a} + \sqrt{b}$ over $K$.

   (4 marks)

(Total: 20 marks)

3. Let $K \subset L$ be a field extension, and $K \subset E \subset L$, $K \subset F \subset L$ intermediate fields such that $L = EF$. For each of the following statements, either prove it or disprove it.

(a) If $K \subset E$ is normal, then $F \subset L$ is normal. (4 marks)

(b) If $F \subset L$ is normal, then $K \subset E$ is normal. (4 marks)

(c) If both $K \subset E$ and $K \subset F$ are normal, then $K \subset E \cap F$ is normal. (4 marks)

(d) If both $K \subset E$ and $K \subset F$ are normal, then $K \subset L$ is normal. (4 marks)

(e) If both $K \subset E$ and $E \subset L$ are normal, then $K \subset L$ is normal. (4 marks)

(Total: 20 marks)

4. In this question you may assume that the polynomial

$$f(X) = X^6 - 2X^3 - 1 \in \mathbb{Q}[X]$$

is irreducible. Denote by $K$ a splitting field of $f(X)$ and by $G$ the Galois group of the extension $\mathbb{Q} \subset K$.

For a subfield $\mathbb{Q} \subset F \subset K$, denote by $F^\dagger \leq G$ the subgroup that corresponds to $F$ under the Galois correspondence. For a subgroup $H \leq G$, denote by $H^\star$ the corresponding subfield.

(a) (i) Find expressions for the six roots of the polynomial $f(X)$; (2 marks)

(ii) plot the roots in the complex plane and label them in some way; (2 marks)

(iii) use the information to show that $K = \mathbb{Q}(\sqrt{-3}, \alpha)$ where $\alpha = \sqrt[3]{1+\sqrt{2}}$, and hence compute $[K : \mathbb{Q}]$. (4 marks)

(b) Let $H = \mathbb{Q}(\sqrt{2})^\dagger \leq G$: describe the structure of $H$ and describe explicitly how $H$ acts on the set of roots. (No justification necessary for this Part.) (4 marks)

(c) Write as in Part (a) $\alpha = \sqrt[3]{1+\sqrt{2}}$, and write $\beta = \sqrt[3]{1-\sqrt{2}}$. Consider the subset

$$Z = \Big\{\sigma \in G \mid \sigma(\alpha) = \beta\Big\} \subset G$$

how many elements does $Z$ have? Describe explicitly how each element of $Z$ acts on the set of roots. (6 marks)

(d) Draw a triangular based prism $P$, with vertices labelled by the roots, such that $G$ is the group of symmetries of $P$. (No justification necessary for this Part.) (2 marks)

(Total: 20 marks)

5. In this question $K$ is a field of characteristic $2$, $a, b \in K$ and

$$f(X) = X^2 + X + a, \quad g(X) = X^2 + X + b \in K[X] \,.$$

(a) Assume that $f(X)$ is irreducible and consider the extension $K \subset K(\alpha)$ where $f(\alpha) = 0$. Prove that $g(X)$ has a root in $K(\alpha)$ if and only if: either $g(X)$ has a root in $K$, or the polynomial:

$$X^2 + X + a + b$$

has a root in $K$. (6 marks)

(b) In the same situation as in Part (a), assume that $g(X)$ does not have a root in $K(\alpha)$. Consider the extension $K \subset L = K(\alpha, \beta)$ where $g(\beta) = 0$.

(i) Prove that the extension is normal and separable; (2 marks)

(ii) determine the Galois group $G$ of the extension; (2 marks)

(iii) determine the action of each element of $G$ on the set of roots of the polynomial $h(X) = f(X)g(X)$; and draw a picture of the Galois correspondence showing all the subgroups of $G$ and the intermediate fields $K \subset F \subset L$ that they correspond to. (5 marks)

(c) In the situation of Part (b), prove that $K(\alpha\beta) = L$.
[*Hint. Use Part (b). Alternatively, consider the orbit of $\alpha\beta \in L$ under the Galois group.*] (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2023

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

# MATH MATH60037/70037

# Galois Theory (Solutions)

| Setter's signature | Checker's signature | Editor's signature |
|---|---|---|
| . . . . . . . . . . . . . . . . | . . . . . . . . . . . . . . . . | . . . . . . . . . . . . . . . . |

1. (a) The polynomial is irreducible. Indeed the reduction mod 2 $\boxed{\text{sim. seen} \Downarrow}$

$$X^5 + X^2 + 1 \in \mathbb{F}_2[X]$$

is irreducible, as it has no roots and it is not divisible by the only degree 2 irreducible $X^2 + X + 1 \in \mathbb{F}_2[X]$ (as can be checked by performing long division. Performing the long division is mandatory in order to earn full marks). $\boxed{4, \text{A}}$

(b) We work in $\mathbb{F}_{2^{10}}$; the only intermediate fields $\mathbb{F}_2 \subsetneq F \subsetneq \mathbb{F}_{2^{10}}$ are $F = \mathbb{F}_4$ and $F = \mathbb{F}_{2^5}$; by inclusion-exclusion the sought for number is $\boxed{\text{sim. seen} \Downarrow}$

$$N = \frac{2^{10} - 2^5 - 2^2 + 2}{5} = \frac{1024 - 32 - 4 + 2}{5} = \frac{990}{5} = 198$$

$\boxed{4, \text{B}}$

(c) The statement is false. Consider $f_1(X) = X^2 - 2$ and $f_2(X) = X^2 - 2X - 1$ in $\mathbb{Q}[X]$: the polynomials are manifestly irreducible and coprime. The splitting field of both, and of the product, is $K = \mathbb{Q}(\sqrt{2})$. The Galois group is $C_2$, manifestly not $C_2 \times C_2$. $\boxed{\text{unseen} \Downarrow}$ $\boxed{4, \text{B}}$

(d) In the notation of the course notes, $c = 2$ is not a square; $b = a^2 - 2 = 2$ so $bc = 4$ is a square; hence $G = C_4$. $\boxed{\text{meth seen} \Downarrow}$ $\boxed{4, \text{A}}$

(e) First of all $K_n K_m = K_{nm}$.[1] Now write $K = K_n \cap K_m$: it is clear that $[K_n : K] \geq [K_n K_m : K_m] = [K_{nm} : K_m] = \varphi(n)$. But then by the tower law $\varphi(n) = [K_n : \mathbb{Q}] = [K_n : K][K : \mathbb{Q}] \geq \varphi(n)[K : \mathbb{Q}]$. It follows that $[K : \mathbb{Q}] = 1$ hence $K = \mathbb{Q}$. $\boxed{\text{unseen} \Downarrow}$ $\boxed{4, \text{D}}$

[1] In principle this should be proved, for example there exist $p, q \in \mathbb{Z}$ such that $\frac{p}{n} + \frac{q}{m} = \frac{1}{nm}$, so $\zeta_{nm} = \zeta_n^p \zeta_m^q$, hence the nontrivial inclusion $K_{nm} \subset K_n K_m$. I will deduct a point for claiming the fact without proof, unless at least one student gets it.

2. (a) Pick $\alpha \in F \setminus K$: it is clear that the minimal polynomial of $\alpha$ has degree 2. Writing this polynomial as

$$X^2 + AX + B$$

we see from the quadratic formula that $F = K(\sqrt{A^2 - B})$.

seen ⇓

2, A

(b) $L$ is the splitting field of the polynomial $f(X) = (X^2 - a)(X^2 - b) \in K[X]$ and hence the extension is normal. In characteristic 2 the four roots $\pm\sqrt{a}, \pm\sqrt{b}$ are all distinct hence the extension is separable. The Galois group $G$ has order 4 and it is a subgroup of $C_2 \times C_2$ (permutations that preserve the roots of the two factors of $f(X)$) so $G = C_2 \times C_2$. Since $[L : K(\sqrt{a})] = 2$, there is an involution $\sigma \in G$ such that $\sigma(\sqrt{b}) = -\sqrt{b}$ and $\sigma(\sqrt{a}) = \sqrt{a}$. Similarly there is an involution $\tau \in G$ such that $\tau(\sqrt{a}) = -\sqrt{a}$ and $\tau(\sqrt{b}) = \sqrt{b}$. By a Lemma seen in class, $ab$ is not a square in $K$, and hence the field fixed by $\sigma\tau$ is $K(\sqrt{ab})$,[2] hence a picture of the Galois correspondence is:

seen ⇓

$$\begin{tikzcd}
 & K(\sqrt{a}, \sqrt{b}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(\sqrt{a}) \arrow[dr, dash] & K(\sqrt{b}) \arrow[d, dash] & K(\sqrt{ab}) \arrow[dl, dash] \\
 & K &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{e\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\tau\rangle \arrow[d, dash] & \langle\sigma\tau\rangle \arrow[dl, dash] \\
 & C_2 \times C_2 &
\end{tikzcd}$$

8, B

(c) In the first place $\sqrt{a} + \sqrt{b}$ is not in any of the fields $K(\sqrt{a})$, $K(\sqrt{b})$, $K(\sqrt{ab})$: it is not in $K(\sqrt{a})$ because otherwise for example $\sqrt{b} \in K(\sqrt{a})$; similarly it is not in $K(\sqrt{b})$; and it is not in $K(\sqrt{ab})$ because, if it were, then also

2, D

$$a\sqrt{b} + b\sqrt{a} = (\sqrt{a} + \sqrt{b})\sqrt{ab} \in K(\sqrt{ab})$$

from which we would conclude (since $a \neq b$) that $\sqrt{a}, \sqrt{b} \in K(\sqrt{ab})$. It follows from this that $K(\sqrt{a} + \sqrt{b}) = L$.

2, A

(d) From Part (c), we know that the minimal polynomial of $\sqrt{a} + \sqrt{b}$ has degree 4. It remains to find a degree 4 polynomial of which $\alpha = \sqrt{a} + \sqrt{b}$ is a root. We compute:

2, C

$$\alpha^4 = (a^2 + 6ab + b^2) + 4(a + b)\sqrt{ab}, \quad \text{and} \quad \alpha^2 = a + b + 2\sqrt{ab}$$

and from this we conclude that

$$f(X) = X^4 - 2(a + b)X^2 + (a + b)^2$$

is the minimal polynomial of $\alpha$.

4, A

[2] If $ab$ were a square in $K$ then $b$ would be a square in $K(\sqrt{a})$. I provisionally assign 2 ”D” marks for realising that this is key to identifying the third field. If none of the students gets this, then I will condone it.

3. (a) The statement is true: if $E$ is the splitting field of $f(X) \in K[X]$, then $EF$ is the splitting field of $f(X)$, now seen as a polynomial with coefficients in $F$.

unseen $\Downarrow$

4, B

(b) The statement is false: take $K = \mathbb{Q}$, $F = E = L = \mathbb{Q}(\sqrt{3})$.

unseen $\Downarrow$

4, A

(c) The statement is true. Consider a polynomial $f(X) \in K[X]$ and assume that it has a root in $E \cap F$. Since $K \subset E$ is normal, $f(X)$ has all its roots in $E$. Similarly $f(X)$ has all its roots in $F$, and hence it has all its roots in $E \cap F$. By a result proven in the notes (three characterisations of normal extensions) $K \subset E \cap F$ is normal.

seen $\Downarrow$

4, C

(d) The statement is true: if $K \subset F$ is the splitting field of $f(X) \in K[X]$, and $K \subset E$ is the splitting field of $g(X) \in K[X]$, then $K \subset EF = L$ is the splitting field of the polynomial $h(X) = f(X)g(X) \in K[X]$.

seen $\Downarrow$

4, C

(e) The statement is false: take $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, $F = L = \mathbb{Q}(\sqrt[4]{2})$.

unseen $\Downarrow$

4, A

4. (a) The roots of the quadratic $Y^2 - 2Y - 1$ are $1 \pm \sqrt{2}$; hence, the roots of the polynomial $f(X)$ are:[3] unseen ⇓

$$\alpha_1 = \alpha = \sqrt[3]{1+\sqrt{2}},\ \alpha_2 = \omega\alpha,\ \alpha_3 = \omega^2\alpha, \quad \text{and}$$
$$\beta_1 = \beta = -\sqrt[3]{-1+\sqrt{2}} = -\frac{1}{\alpha_1},\ \beta_2 = \omega^2\beta = -\frac{1}{\alpha_2},\ \beta_3 = \omega\beta = -\frac{1}{\alpha_3}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of $1$. (The plot shows the vertices of two equilateral triangles inscribed in two circles; it does not need to look nice.) From the formulas it is clear that $K = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$. Now $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 6 = 12$ (the first because $\sqrt{-3}$ is not in $\mathbb{Q}(\alpha) \subset \mathbb{R}$, the second because we are assuming that $f(X)$ is irreducible). 8, A

(b) It follows from what was said in Part (a) that $\mathbb{Q}(\sqrt{2}) \subset K$ is the splitting field of the cubic polynomial meth seen ⇓

$$Y^3 - 1 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$$

Moreover by the tower law $[K : \mathbb{Q}(\sqrt{2})] = 6$ and hence $H = \mathfrak{S}_3$, the full symmetric group on the three roots $\alpha_1, \alpha_2, \alpha_3$. To describe the action of $H$, it is sufficient to note that, with the labelling given in Part (a), the same permutation acts on the $\beta$s as on the $\alpha$s. (This follows from the relation $\alpha_i\beta_i = -1$ but the students don't need to justify it.) 2, C

(c) By the orbit-stabiliser theorem, the stabiliser $G_\alpha$ is a group with two elements. $Z$ is a coset of $G_\alpha$ and hence it too has two elements. 2, D

Suppose that $\sigma \in Z$, that is, $\sigma(\alpha) = \beta$. It follows from this that $\sigma(1 + \sqrt{2}) = \sigma(\alpha^3) = \beta^3 = 1 - \sqrt{2}$ and hence $\sigma(\sqrt{2}) = -\sqrt{2}$, and from this we conclude that $\sigma$ must move every "$\alpha$" into a "$\beta$," and viceversa. meth seen ⇓

Let us consider $\sigma(\alpha_2)$. There are two cases:

CASE 1 $\sigma(\alpha_2) = \beta_2$. In this case we must have that $\sigma(\alpha_3) = \beta_3$, because $\beta_3$ is the last available "$\beta$." From $\sigma(\alpha) = \beta$ and $\sigma(\omega\alpha) = \sigma(\omega)\sigma(\alpha) = \omega^2\sigma(\alpha)$ we conclude that in this case we must have that $\sigma(\omega) = \omega^2$. From $-1 = \sigma(\alpha)\sigma(\beta) = \beta\sigma(\beta)$ we conclude that $\sigma(\beta) = -\frac{1}{\beta} = \alpha$, and then $\sigma(\beta_3) = \sigma(\omega\beta) = \omega^2\alpha = \alpha_3$. To summarise, there is only one possibility for this case and it works like this:

$$\sigma\colon \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \mapsto \beta_1, \beta_2, \beta_3, \alpha_1, \alpha_2, \alpha_3$$

CASE 2 $\sigma(\alpha_2) = \beta_3$. Reasoning as in the previous case, there is only one possibility for this case, too, and it works like this:

$$\sigma\colon \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \mapsto \beta_1, \beta_3, \beta_2, \alpha_1, \alpha_3, \alpha_2$$

Now we know from Part (c) that $Z$ is a two-element set; hence both cases must occur and this completely determines $Z \subset G$. 6, D

(d) A triangular-base prism with the vertices of the bottom triangle labelled $\alpha_1, \alpha_2, \alpha_3$ and the corresponding vertices of the top triangle labelled $\beta_1, \beta_2, \beta_3$. (From the description of $H$ and $Z$ it is obvious that $G$ preserves the prism; on the other hand by the orbit-stabiliser theorem the group of symmetries of the prism has $12$ elements. It follows that $G$ is the group of symmetries of the prism, but students are not asked to justify any of this.) 2, D

[3] at some point the student must realise that $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$; it is not necessary for them to realise this now. Several labelling strategies are possible of course.

5. (a) Assume that $g$ has a root $\beta \in K(\alpha)$. There exist $x, y \in K$ such that $\beta = x + y\alpha$ is a root of $g$, that is

$$(x+y\alpha)^2 + (x+y\alpha) = x^2 + x + y^2\alpha^2 + y\alpha = x^2 + x + y^2 a + (y^2+y)\alpha = b$$

We must have $y^2 + y = y(y+1) = 0$. If $y = 0$ then $x^2 + x = b$, that is, $g$ has a root already in $K$. Otherwise $y + 1 = 0$ and then $x^2 + x = a + b$, that is, the polynomial $X^2 + X + a + b$ has a root in $K$ as was to be shown. $\boxed{6, \mathrm{M}}$

(b) The Galois group $G$ has order $4$ and it is a subgroup of $C_2 \times C_2$ (permutations that preserve the roots of the two factors of $h(X)$) so $G = C_2 \times C_2$. Since $[L : K(\alpha)] = 2$, by Artin–Schreier there is an involution $\sigma \in G$ such that $\sigma(\beta) = \beta + 1$ and $\sigma(\alpha) = \alpha$. Similarly there is an involution $\tau \in G$ such that $\tau(\alpha) = \alpha + 1$ and $\tau(\beta) = \beta$. By Part (a), the polynomial $X^2 + X + a + b$ does not have a root in $K$, in other words $\alpha + \beta \notin K$ and hence the field fixed by $\sigma\tau$ is $K(\alpha + \beta)$, hence a picture of the Galois correspondence is:

$$\begin{tikzcd}
 & K(\alpha,\beta) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K(\alpha) \arrow[dr, dash] & K(\beta) \arrow[d, dash] & K(\alpha+\beta) \arrow[dl, dash] \\
 & K &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{e\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\tau\rangle \arrow[d, dash] & \langle\sigma\tau\rangle \arrow[dl, dash] \\
 & C_2 \times C_2 &
\end{tikzcd}$$

$\boxed{9, \mathrm{M}}$

(c) The orbit is $\{\alpha\beta, \alpha(\beta+1), (\alpha+1)\beta, (\alpha+1)(\beta+1)\}$. These $4$ pairwise distinct elements of $L$ are the roots of the minimal polynomial of $\alpha\beta$, hence $K(\alpha\beta)$ has degree $4$ over $K$ and therefore it must be all of $L$. $\boxed{5, \mathrm{M}}$

**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

**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.**

| **ExamModuleCode** | **QuestionNumber** | **Comments for Students** |
|---|---|---|
| MATH60037/70037 | 1 | This was intended to be a straightforward question and indeed many students did well on it. |
| MATH60037/70037 | 2 | Mostly well done by the students.Part (a) is *really* easy. The only proof that I know of starts as follows: "choose a in F\K; then a must satisfy a quadratic equation..." It is really perverse how MANY students dislike making a choice (some mathematicians are like that, too, and that tends to lead them in higher homotopy theory): so many miss out on two really easy marks.In part (b) NOBODY told me that the extension is separable because, in characteristic not 2, if a is nonzero then a is never equal to -a.In part (c) NOBODY pointed out that ab is not a square in K hence K(sqrt{ab}) is a nontrivial extension. |
| MATH60037/70037 | 3 | This question is not easy but standard. |
| MATH60037/70037 | 4 | This was the hardest question. On the other hand it is well known that I like this kind of question so it could have been expected. It is difficult for students to provide much detail on this type of question hence I was lenient in awarding partial credit |
| MATH70037 | 5 | This was not an easy question.It is the characteristic 2 analogue of Q2; and the additive and multiplicative group roles are reversed. Even for somebody who has internalised the main idea of Artin-Schreier extensions, the question requires good concentration and stamina.So I was pleased that the students actually did reasonably well. |