Imperial College
London

MATH97034 MATH97142

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

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

Galois Theory

Date: Friday, 14 May 2021

Time: 09:00 to 11:30

Time Allowed: 2.5 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 ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET 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 [...]."

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) Consider a monic polynomial $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$. For p a prime, denote by $f_p(X) \in \mathbb{F}_p[X]$ the reduction of $f(X)$ modulo p. If $f_p(X) \in \mathbb{F}_p[X]$ is irreducible, then $f(X) \in \mathbb{Q}[X]$ is also irreducible. (2 marks)

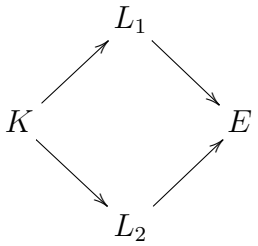
   (ii) Let p be a prime and let $K = \mathbb{F}_p(T)$. The polynomial $f(X) = X^{2p} + TX^p + T \in K[X]$ is irreducible. (2 marks)

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

   (iv) Let $K \subset L$ be the splitting field of a polynomial $f(X) \in K[X]$. The group $G = \mathrm{Emb}_K(L, L)$ acts transitively on the roots of $f(X)$ in L. (2 marks)

   (v) Let $f(X) \in K[X]$ be irreducible, and let $K \subset L$ be any normal field extension. The group $G = \mathrm{Emb}_K(L, L)$ acts transitively on the set $R = \{a \in L \mid f(a) = 0\}$. (2 marks)

   (vi) Consider a diagram of field extensions



   where $E = L_1L_2$. Then $[E : L_1] \leq [L_2 : K]$. (2 marks)

   (vii) Same setup as the previous part: $K \subset L_1$ separable implies $L_2 \subset E$ separable. (2 marks)

   (viii) Same setup as the previous part: $K \subset L_1$ normal implies $L_2 \subset E$ normal. (2 marks)

   (ix) A normal extension $K \subset L$ is separable if and only if the group $G = \mathrm{Emb}_K(L, L)$ has $[L : K]$ elements. (2 marks)

   (x) For n, m integers let ζ_n, $\zeta_m \in \mathbb{C}$ be primitive n^{th} and m^{th} roots of unity. If $\mathrm{hcf}(n, m) = 1$, then $\zeta_n\zeta_m$ is a primitive nm^{th} root of unity. (2 marks)

(Total: 20 marks)

2. The two parts of this question are not related.

(a) What is the degree $[\mathbb{F}_{1024} : \mathbb{F}_2]$? Draw a diagram showing all the intermediate fields $\mathbb{F}_2 \subset F \subset \mathbb{F}_{1024}$ and the inclusions between them. Compute the number of degree 10 irreducible monic polynomials $f(X) \in \mathbb{F}_2[X]$. (10 marks)

(b) Consider the polynomial

$$f(X) = X^5 - 3X^4 + X^3 + 2X^2 + 3X + 1 \in \mathbb{Q}[X]$$

By studying how $f(X)$ splits modulo 2 and modulo 5, determine the structure of the Galois group of its splitting field over $\mathbb{Q}$. (10 marks)

(Total: 20 marks)

3. Let $K \subset F$ be a field extension. In this question, we say that $F \subset L$ is a *normal closure* of $K \subset F$ if the following two conditions are satisfied:

(i) For all extensions $L \subset \Omega$ and for all K-embeddings $\sigma\colon F \to \Omega$, $\sigma(F) \subset L$;

(ii) L is generated by the images $\sigma(F)$, as $\sigma \in \mathrm{Emb}_K(F, L)$.

[**N.B.** *This is not the definition used in the course, but it is equivalent to it. When answering the question you must use this definition.*]

(a) Let $F \subset L$ be a normal closure of $K \subset F$. Prove that $K \subset L$ is a normal extension. (10 marks)

(b) Let $F \subset L_1$ and $F \subset L_2$ be two normal closures of $K \subset F$. Prove that there is an F-isomorphism $\sigma\colon L_1 \to L_2$. (10 marks)

(Total: 20 marks)

4. (a) Let $\zeta = e^{\frac{\pi \mathrm{i}}{9}}$. Prove that $\lambda = \zeta + \zeta^{-1}$ is a root of the polynomial

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

Determine the structure of the Galois group of the splitting field K of $f(X)$ over $\mathbb{Q}$. Setting $\lambda_1 = \lambda$, find expressions for the remaining two roots λ_2, λ_3 of $f(X)$ and show that they are both real and < 0. (10 marks)

(b) Consider now the polynomial

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

In this part you may assume without proof that $g(Y) \in \mathbb{Q}[Y]$ is irreducible. Denote by $\mathbb{Q} \subset L$ the splitting field of $g(Y)$, and let G be the Galois group of this extension.

Let $K \subset L$ be the same field as in Part (a). Show that $K^\dagger \leq G$ is a normal subgroup isomorphic to $C_2 \times C_2$ and compute the degree $[L : \mathbb{Q}]$.

[*Hint. Work with the tower* $\mathbb{Q} \subset K \subset L$ where K is as in Part (a) of the question; the roots of $g(Y)$ are $\pm\mu_i$ where $\mu_i^2 = \lambda_i$: prove that λ_1 is not a square in K and that λ_2 is not a square in $\mathbb{Q}(\mu_1)$. On the other hand $\lambda_1\lambda_2\lambda_3 = 1$ so go ahead and choose, as you may, $\mu_3 = \frac{1}{\mu_1\mu_2}$.] (10 marks)

(Total: 20 marks)

5. In this question you are permitted to quote any result in Keith Conrad's paper *Galois groups of cubics and quartics (not in characteristic 2)*.

Let $p > 0$ be an integer prime. Consider the polynomial

$$f(X) = X^4 + pX + p \in \mathbb{Q}[X]$$

Show that f is irreducible. Write down the cubic resolvent $r(X) \in \mathbb{Q}[X]$ and prove that $r(X)$ is irreducible if and only if $p \neq 3, 5$. Write down the discriminant and show that it is never a square in $\mathbb{Q}$. For all $p \neq 3, 5$ determine the Galois group of the splitting field of $f(X)$ over $\mathbb{Q}$. Carefully justify each step. (20 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2021

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

MATH96025/MATH97034/MATH97142

Galois Theory (Solutions)

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

1. (i) T
(ii) T
(iii) F
(iv) F
(v) T
(vi) T
(vii) T
(viii) T
(ix) T
(x) T

seen $\Downarrow$

2, A

meth seen $\Downarrow$

2, A

seen $\Downarrow$

2, B

seen $\Downarrow$

2, B

seen $\Downarrow$

2, B

unseen $\Downarrow$

2, B

unseen $\Downarrow$

2, A

unseen $\Downarrow$

2, A

seen $\Downarrow$

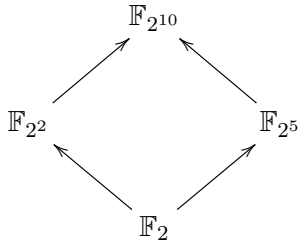
2, A

unseen $\Downarrow$

2, A

2. (a) $[\mathbb{F}_{1024} : \mathbb{F}_2] = 10$ since $1024 = 2^{10}$. meth seen ⇓

The diagram of intermediate fields with inclusion is the same as the diagram of divisors of 10:



By inclusion-exclusion the number of elements of $\mathbb{F}_{2^{10}}$ that are neither in $\mathbb{F}_{2^5}$ nor in $\mathbb{F}_{2^2}$ is $1024 - 32 - 4 + 2 = 990$. These are precisely the elements of degree 10 hence there are $\frac{990}{10} = 99$ degree 10 monic polynomials $f(X) \in \mathbb{F}_2[X]$. 10, A

(b) First working mod 2 we see that meth seen ⇓

$$f(X) = X^5 - 3X^4 + X^3 + 2X^2 + 3X + 1 = X^5 + X^4 + X^3 + X + 1 = \\ = (X^2 + X + 1)X^3 + (X + 1) \in \mathbb{F}_2[X]$$

hence $f(X) \in \mathbb{F}_2[X]$ is irreducible because it has no roots and it is not divisible by $X^2 + X + 1$ (the only degree 2 monic irreducible in $\mathbb{F}_2[X]$).

Working mod 5 we see that ± 1 are both roots; long division gives

$$X^5 + 2X^4 + X^3 + 2X^2 - 2X + 1 = (X^2 - 1)(X^3 + 2X^2 + 2X - 1) \in \mathbb{F}_5[X]$$

Next we spot that $X = -2$ is also a root and long division again gives:

$$X^3 + 2X^2 + 2X - 1 = (X + 2)(X^2 + 2) \in \mathbb{F}_5[X]$$

By Corollary 57 in the notes we conclude that G has a 5-cycle and a transposition, and by Lemma 59 we conclude that $G = \mathfrak{S}_5$. 10, B

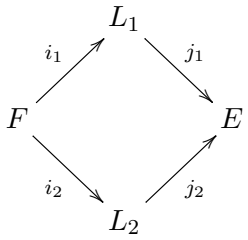
3. (a) Fix an inclusion $L \subset \Omega$ and let $j\colon L \to \Omega$ be a K-embedding. By property (ii) in the definition of normal closure, as σ varies in $\mathrm{Emb}_K(L, L)$ the $\sigma(F)$ generate L; it follows that the $j\sigma(F)$ generate $j(L)$; but by property (i) all $j\sigma(F)$ are contained in L, hence the field that they generate, namely $j(L)$, is also contained in L; that is $j(L) \subset L$ and this shows that $K \subset L$ is a normal extension.

seen/sim.seen ⇓

10, C

(b) By Axiom 4 we can construct a diagram:

seen/sim.seen ⇓



where $j_1 i_1 = j_2 i_2$. All we need to show is that $j_1(L_1) = j_2(L_2)$. In fact all we need to show is that $j_1(L_1) \subset j_2(L_2)$, as the other inclusion follows from the same argument.

By property (ii) (for $F \subset L_1$), L_1 is generated by the union of the $\sigma(F)$ over $\sigma \in \mathrm{Emb}_K(F, L_1)$; hence $j_1(L_1)$ is generated by the union of the $j_1\sigma(F)$; by property (i) (for $F \subset L_2 \subset E$) these $j_1\sigma(F)$ are all contained in $j_2(L_2)$, hence the field that they generate $j_1(L_1)$ is also contained in $j_2(L_2)$.

10, D

4. (a) The first assertion is the calculation: seen/sim.seen ⇓

$$\lambda^3 = \left(\zeta + \frac{1}{\zeta}\right)^3 = \zeta^3 + \frac{1}{\zeta^3} + 3\left(\zeta + \frac{1}{\zeta}\right) = \frac{1+\mathtt{i}\sqrt{3}}{2} + \frac{1-\mathtt{i}\sqrt{3}}{2} + 3\lambda = 3\lambda + 1$$

The discriminant $4 \times 27 - 27 = 3^4$ is a square in $\mathbb{Q}$ hence the Galois group is a cyclic group C_3.

The other two roots are:

$$\lambda_2 = \zeta^5 + \zeta^{-5}, \quad \lambda_3 = \zeta^7 + \zeta^{-7}$$

(e.g. by direct computation same as for λ_1.) It is clear from this formula that both λ_2, λ_3 are negative. 10, A

(b) It is clear that $L = K(\mu_1, \mu_2)$ where $\mu_1^2 = \lambda_1$, $\mu_2^2 = \lambda_2$ and the roots are $\pm\mu_1$, $\pm\mu_2$, and — setting $\mu_3 = \frac{1}{\mu_1\mu_2}$ — $\pm\mu_3$. meth seen ⇓

Now, λ_1 is not a square in K — for otherwise $g(Y)$ has a root in an extension K of degree $[K : \mathbb{Q}] = 3$ and hence it is not irreducible — hence $[K(\mu_1) : K] = 2$. 2, B
Also λ_2 is not a square in $K(\mu_1)$ because if it were then (by Lemma 36): either λ_2 or $\lambda_1\lambda_2 = \frac{1}{\lambda_3}$ would be a square in K, but neither is a square in K because of the same reason that λ_1 is not. It follows that $L = K(\mu_1, \mu_2)$ and that the Galois group of the extension $K \subset L$ is $C_2 \times C_2$. By the fundamental theorem this Galois group is $K^\dagger$ so we have shown that $K^\dagger = C_2 \times C_2$. Because $\mathbb{Q} \subset K$ is normal, $K^\dagger \leq G$ is normal (and, in fact, $G/V = C_3$, the Galois group of the extension $\mathbb{Q} \subset K$).

We compute $[L : \mathbb{Q}]$ by applying the tower law to the tower $\mathbb{Q} \subset K \subset L$:

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 4 \times 3 = 12$$

8, D

5. The polynomial $f(X)$ is irreducible by the Eisenstein criterion at p. unseen ⇓

The cubic resultant is 2, M

$$r(Y) = Y^3 - 4pY + p^2 \in \mathbb{Q}[Y]$$

Because $r(Y)$ has degree 3, it is irreducible over the rationals if and only if it has no rational roots. Possible rational roots are $\pm 1, \pm p, \pm p^2$. 4, M

One checks by elementary arguments that

$$r(1) = p^2 - 4p + 1,\ r(-1) = p^2 + 4p - 1,\ r(p^2) = p^6 - 4p^3 + p^2 = (p^4 - 4p + 1)p^2,$$
$$\text{and } r(-p^2) = -(p^4 - 4p - 1)p^2$$

can never vanish. 4, M

On the other hand, $r(p) = p^2(p-3) = 0$ if and only if $p = 3$ and $r(-p) = -p^2(p-5) = 0$ if and only if $p = 3$. We conclude that $(Y + 5)$ is a factor if $p = 5$ and $(Y - 3)$ is a factor if $p = 3$, and $r(Y)$ is irreducible for all other p. 3, M

The discriminant $p^3(-27p + 256)$ is never a perfect square (p must divide 256 hence $p = 2$, but then we need $-27 + 128 = 101$ to be square, which it is not.) 5, M

It follows from this that for $p \neq 3, 5$ $G = \mathfrak{S}_4$. 2, M

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 sperate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH96025 MATH97034 MATH97142	1	I tend to have a question like this in all my exams. Students rarely appreciate how tricky this type of question can be and how much I can learn from it. This year was perhaps a little harder than usual and students did not do super-well.
MATH96025 MATH97034 MATH97142	2	Every bit of this question was straightforward/standard and most students did very well on this question.
MATH96025 MATH97034 MATH97142	3	This was a serious question and many students did it well. The best starategy by far for solving it was to 'never lose altitude' namely remain squarely in the categorical plane. Several students instead tried to do part (a) by checking that L was the slpitting field of a polynomial; it is not impossible to do it this way but it is very difficult and only one student managed to pull it off.
MATH96025 MATH97034 MATH97142	4	By contrast this question was serious but very concrete/explicit. Many students did well. It is interesting to see that some students did better on Q3, and some other students did better on Q4: roughly this would be the divide between those who like theory and those who like computation.
MATH96025 MATH97034 MATH97142	5	This question was rather elementary for those who knew the basic processes.