



Coláiste na Tríonóide, Baile Átha Cliath  
Trinity College Dublin

Ollscoil Átha Cliath | The University of Dublin

**Faculty of Science, Technology, Engineering and Mathematics**

**School of Mathematics**

JS/SS Maths/TP/TJH

Michaelmas 2025–26

**MAU34101 Galois theory — Revision paper (NOT REAL EXAM)**

Never

Nowhere

Ever

**Dr. Nicolas Mascot**

---

**Instructions to candidates:**

This is a mock exam paper for revision purposes only.

Question 1 is for warmup. Questions 2–8 are more or less representative of what to expect at the exam. Questions 5 and 9–11 are more difficult and are included here for practice.

**You may not start this examination until you are instructed to do so by the Invigilator.**

**Question 1** *Subgroups for appetiser*

Sketch a diagram showing all the subgroups of  $G$  when:

1.  $G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ ,
2.  $G = V_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23)\} < S_4$ ,
3.  $G = S_3$ ,
4.  $G = \mathbb{Z}/n\mathbb{Z}$ , for  $n$  up to 12.

**Question 2** *Bookwork*

Let  $K \subset L$  be a finite extension, and let  $\Omega \supset K$  be algebraically closed. Which inequalities do we always have between  $[L : K]$ ,  $\# \text{Aut}_K(L)$ ,  $\# \text{Hom}_K(L, \Omega)$ ? When are they equalities? State equivalent conditions.

**Question 3** *Yoga with the Galois correspondence*

Let  $L/K$  be a finite Galois extension with Galois group  $G = \text{Gal}(L/K)$ . Let  $K \subseteq E_1, E_2 \subseteq L$  be intermediate extensions, and let  $H_1, H_2 \leq G$  be the corresponding subgroups.

We denote by  $E_1 E_2$  the subfield of  $L$  generated by  $E_1$  and  $E_2$ , and by  $H_1 H_2$  the subgroup of  $G$  spanned by  $H_1$  and  $H_2$ .

Find the intermediate extensions corresponding to  $H_1 H_2$  and to  $H_1 \cap H_2$ , and the subgroups corresponding to  $E_1 E_2$  and to  $E_1 \cap E_2$ .

**Question 4** *Galois group computations*

Determine the Galois group over  $\mathbb{Q}$  of the polynomials below, and say if they are solvable by radicals over  $\mathbb{Q}$ :  $x^3 - x^2 - x - 2$ ,  $x^3 - 3x - 1$ ,  $x^3 - 7$ ,  $x^5 + 21x^2 + 35x + 420$ ,  
 $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ .

**Question 5** *From the 2019 exam*

Let  $K$  be a field, let  $F(x) \in K[x]$  be separable and irreducible over  $K$ , and let  $\alpha$  be a root of  $F(x)$  (in some extension of  $K$ ). Suppose that  $\text{Gal}_K(F)$  is Abelian. Prove that  $K(\alpha)$  is a splitting field of  $F(x)$  over  $K$ .

Show that all the hypotheses are necessary (give counter-examples).

**Question 6** *Correspondence in degree 3*

*Note: This exercise has a lot of overlap with the next one.*

Let  $K$  be a field, and  $F(x) \in K[x]$  be separable and of degree 3. Denote its 3 roots in its splitting field  $L$  by  $\alpha_1, \alpha_2, \alpha_3$ .

1. What are the possibilities for  $\text{Gal}_K(F)$ ? How can you tell them apart?
2. For each of the cases found in the previous question, sketch the diagram showing all the fields  $K \subset E \subset L$  and identifying these fields. In particular, locate  $K(\alpha_1)$ ,  $K(\alpha_2)$ ,  $K(\alpha_3)$ ,  $K(\alpha_1, \alpha_2)$ , etc.
3. In which of the cases above is the stem field of  $F$  isomorphic to its splitting field?  
(Warning: there is a catch in this question.)

**Question 7** *Cube roots (From the 2021 exam)*

*Note: This exercise has a lot of overlap with the previous one.*

Let  $K$  be a subfield of  $\mathbb{C}$ . Let  $0 \neq a \in K$ , and let  $\alpha \in \mathbb{C}$  be such that  $\alpha^3 = a$ . Let

$$f(x) = x^3 - a \in K[x],$$

and let  $S \subset \mathbb{C}$  be the splitting field of  $f(x)$  over  $K$ .

Finally, let  $\zeta = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ .

*Note that  $a$  may or may not be a cube in  $K$ , and that  $\zeta$  may or may not lie in  $K$ .*

1. (a) Prove that if  $a$  is not a cube in  $K$ , then  $f(x)$  is irreducible over  $K$ .
- (b) Prove that  $[K(\zeta) : K] \leq 2$ .
- (c) Express the complex roots of  $f(x)$  in terms of  $\alpha$  and  $\zeta$ .

*In what follows, we denote these roots by  $\alpha_0 = \alpha$ ,  $\alpha_1$ , and  $\alpha_2$ .*

- (d) Prove that  $S \ni \zeta$ .
- (e) Prove that  $S$  is a Galois extension of  $K$ .

*In what follows, we write  $G$  for  $\text{Gal}(S/K)$ , and we view  $G$  as a subgroup of  $S_3$  acting on  $\alpha_0, \alpha_1, \alpha_2$ .*

2. In each of the following situations:

- (a)  $a$  is not a cube in  $K$  and  $\zeta \notin K$ ,
- (b)  $a$  is not a cube in  $K$  but  $\zeta \in K$ ,
- (c)  $a$  is a cube in  $K$  but  $\zeta \notin K$ ,
- (d)  $a$  is a cube in  $K$  and  $\zeta \in K$ ,

determine  $[S : K]$ , explain how  $G$  acts on  $\alpha_0, \alpha_1, \alpha_2$ , explain how  $G$  acts on  $\zeta$ , draw a diagram showing all the intermediate fields  $K \subseteq E \subseteq S$ , and say which of these  $E$  are Galois over  $K$ . Justify your answers.

### Question 8 *The fundamental theorem of algebra*

The goal of this Question is to use Galois theory to prove by contradiction that  $\mathbb{C}$  is algebraically closed.

You may use without proof the following facts:

- If  $F(x) \in \mathbb{R}[x]$  is a polynomial of *odd degree*, then  $F(x)$  has at least one root in  $\mathbb{R}$ .
- If  $G(x) \in \mathbb{C}[x]$  is a polynomial of *degree 2*, then  $G(x)$  has at least one root in  $\mathbb{C}$ .
- If  $G$  is a finite group of cardinal  $\#G = 2^a b$  with  $b$  odd, then  $G$  has at least one subgroup of cardinal  $2^a$ .
- If  $H$  is a finite group whose cardinal  $\#H = 2^a$  is a power of 2, then for each integer  $0 \leq n \leq a$ ,  $H$  has at least one subgroup of cardinal  $2^n$ .

1. Prove that if  $\mathbb{C}$  were not algebraically closed, then there would exist a finite nontrivial extension  $K$  of  $\mathbb{C}$  (that is to say  $K \supsetneq \mathbb{C}$  and  $1 < [K : \mathbb{C}] < \infty$ ).
2. Deduce that there would exist a finite nontrivial extension  $\mathbb{C} \subsetneq L$  such that the extension  $\mathbb{R} \subsetneq L$  is Galois.
3. Prove that  $[L : \mathbb{R}]$  would necessarily be a power of 2.
4. Prove that there would exist an intermediate field  $\mathbb{C} \subsetneq F \subseteq L$  such that  $[F : \mathbb{C}] = 2$ .
5. Derive a contradiction.

*Note: the admitted facts at the top of the Question follow respectively from elementary calculus (limits at  $\pm\infty$  and then intermediate value theorem), the formula to solve quadratic equations and the fact that every element of  $\mathbb{C}$  admits a square root in  $\mathbb{C}$ , Sylow's theorem, and Sylow's theorem again.*

**Question 9** *A cosine formula*

1. Prove that the group  $(\mathbb{Z}/17\mathbb{Z})^\times$  is cyclic, and find a generator for it.
2. Let  $c = \cos(2\pi/17)$ . Prove that  $c$  is algebraic over  $\mathbb{Q}$ .
3. Determine the conjugates of  $c$  over  $\mathbb{Q}$ , and its degree as an algebraic number over  $\mathbb{Q}$ .
4. Explain how one could in principle use Galois theory (and a calculator / computer) to find an explicit formula for  $c$ .

**Question 10** *Another cosine formula*

Let  $L = \mathbb{Q}(z)$  where  $z = e^{i\pi/10}$  which is a primitive 20-th root of unity, and let  $c = z + z^{-1} = 2 \cos(\pi/10)$ . We admit without proof that  $(\mathbb{Z}/20\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ , the first factor being generated by  $-9 \bmod 20$ , and the second factor being generated by  $-3 \bmod 20$ .

1. What is the minimal polynomial of  $z$  over  $\mathbb{Q}$ ?
2. Figure out the diagram of subgroups of  $(\mathbb{Z}/20\mathbb{Z})^\times$ .

*You may use without proof the fact that any group of order 4 is isomorphic either to  $\mathbb{Z}/4\mathbb{Z}$  or to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . You should find 8 subgroups in total.*

3. Deduce the diagram of intermediate fields between  $\mathbb{Q}$  and  $L$ .

*You may want to use a calculator / computer.*

4. Find a radical expression for  $c$ .

**Question 11** *Extensions of finite fields are Galois*

Let  $p \in \mathbb{N}$  be prime,  $n \in \mathbb{N}$ , and  $q = p^n$ .

1. Give two proofs of the fact that the extension  $\mathbb{F}_p \subset \mathbb{F}_q$  is Galois: one by viewing  $\mathbb{F}_q$  as a splitting field, and the other by considering the order of  $\text{Frob} \in \text{Aut}(\mathbb{F}_q)$ .
2. What does the Galois correspondence tell us for  $\mathbb{F}_p \subset \mathbb{F}_q$ ?
3. Generalise to an arbitrary extension of finite fields  $\mathbb{F}_q \subset \mathbb{F}_{q'}$ .

**Question 12** *A quaternionic Galois group*

Let  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , and let  $\alpha = (2 + \sqrt{2})(3 + \sqrt{3}) \in L$ ,  $\beta = (2 - \sqrt{2})(3 + \sqrt{3}) \in L$ ,  $\gamma = (2 + \sqrt{2})(3 - \sqrt{3}) \in L$ , and  $\delta = (2 - \sqrt{2})(3 - \sqrt{3}) \in L$ .

Observe that  $\alpha$ ,  $\beta$ ,  $\gamma$ , and  $\delta$  are all positive; thus each of them has a unique *positive* square root, which we denote by  $\sqrt{\alpha}$ ,  $\sqrt{\beta}$ ,  $\sqrt{\gamma}$ , and  $\sqrt{\delta}$ .

Finally, let  $M = \mathbb{Q}(\sqrt{\alpha})$ .

1. Make sure you remember how to prove that  $L/\mathbb{Q}$  is Galois, what  $\text{Gal}(L/\mathbb{Q})$  looks like, and what the intermediate fields  $\mathbb{Q} \subseteq E \subseteq L$  are.
2. Determine the action of all the elements of  $\text{Gal}(L/\mathbb{Q})$  on  $\alpha$ . Deduce that  $L = \mathbb{Q}(\alpha)$ .
3. Let  $\sigma \in \text{Gal}(L/\mathbb{Q})$  flip  $\sqrt{2}$  and fix  $\sqrt{3}$ . Prove that  $\sigma(\alpha) = (\sqrt{2} - 1)^2\alpha$ . Deduce that  $\sqrt{\alpha} \notin L$ .

*Hint: Determine  $\sigma(\sqrt{\alpha})$  and  $\sigma^2(\sqrt{\alpha})$ .*

4. Determine the Galois conjugates of  $\sqrt{\alpha}$  over  $\mathbb{Q}$ .

*Hint: Consider the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ .*

5. Deduce that  $M$  is Galois over  $\mathbb{Q}$ .
6. Prove that  $\text{Gal}(M/\mathbb{Q})$  is a solvable group.
7. Prove that  $\text{Gal}(M/L) = \{\text{Id}, \varepsilon\}$  for some  $\varepsilon \in \text{Gal}(M/\mathbb{Q})$  of order 2, and that  $\text{Gal}(M/L)$  is normal in  $\text{Gal}(M/\mathbb{Q})$ .
8. Deduce that  $\varepsilon$  commutes with all the elements of  $\text{Gal}(M/\mathbb{Q})$ .
9. Determine the action of  $\varepsilon$  on the  $\mathbb{Q}$ -conjugates of  $\sqrt{\alpha}$ .
10. Determine the action of all the elements of  $\text{Gal}(M/\mathbb{Q})$  on the  $\mathbb{Q}$ -conjugates of  $\sqrt{\alpha}$ .

*Hint: Start with the  $\mathbb{Q}$ -conjugates of  $\alpha$  (as opposed to  $\sqrt{\alpha}$ ).*