Galois theory — Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2023/MAU34101/index.html

Version: November 6, 2023

Submit[1] your answers by Monday November 6th, 4PM.

Exercise 1 *From the 2021 exam (100 pts)*

Let $f(x) = x^4 - 5x^2 + 1 \in \mathbb{Q}[x]$. We admit without proof that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Let $\alpha \in \mathbb{C}$ be a root of $f(x)$, and let $K = \mathbb{Q}(\alpha)$.

Note: This is the exercise form the 2021 exam I warned you about in the lectures. So even if it is possible to find an expression for α in terms of nested square roots, you are strongly advised to refrain from doing so, and to merely rely on the relation $f(\alpha) = 0$ instead.

1. (5 pts) Express the complex roots of $f(x)$ in terms of α.

   Hint: Check out $1/\alpha$.

2. (20 pts) Prove that K is a Galois extension of $\mathbb{Q}$.

3. (25 pts) Prove that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and explain how its elements act on the conjugates of α.

4. (40 pts) Draw a diagram showing all the intermediate fields $\mathbb{Q} \subseteq E \subseteq K$, and identifying these intermediate fields explicitly. Justify your answer.

5. (10 pts) Prove that $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

Solution 1

1. We observe directly that $1/\alpha$ is also a root of $f(x)$. Since $f(x)$ is even it follows that $\pm\alpha$ and $\pm 1/\alpha$ are roots of $f(x)$. These are all distinct, because $\alpha = -\alpha$, $\alpha = 1/\alpha$, and $\alpha = -1/\alpha$ would respectively force $\alpha = 0$, $\alpha = \pm 1$, $\alpha = \pm i$, none of which are roots of $f(x)$. Since $f(x)$ has at most $\deg f = 4$ roots, we have found all of them.

2. Clearly, the field $K = \mathbb{Q}(\alpha)$ agrees with $\mathbb{Q}(\alpha, -\alpha, 1/\alpha, -1/\alpha)$, which is the spitting field of $f(x)$ over $\mathbb{Q}$ by the previous question. Besides, $f(x)$ is separable since its 4 roots are distinct as explained in the previous question. In conclusion, K, which is the splitting field over $\mathbb{Q}$ of a separable polynomial, is Galois over $\mathbb{Q}$.

[1] Preferably in paper form, or by emailing LaTeXdocuments to mismet@tcd.ie

3. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Since $f(x)$ is irreducible and monic, it is the minimal polynomial of α over $\mathbb{Q}$. It follows that $[K : \mathbb{Q}] = 4$, and that the $\mathbb{Q}$-conjugates of α are $\pm\alpha$ and $\pm 1/\alpha$ in view of the first question. Since $K/\mathbb{Q}$ is Galois, there exists σ_1 (resp. σ_2, σ_3) in G which takes α to $-\alpha$ (resp. $1/\alpha$, $-1/\alpha$). These are clearly distinct from each other and from the identity, whence 4 elements of G. On the other hand, again because K/Q is Galois, $\#G = [K : \mathbb{Q}] = 4$, whence $G = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_3\}$, where

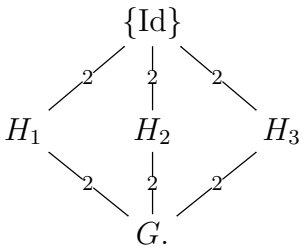
$$\sigma_1(\alpha) = -\alpha \rightsquigarrow \sigma_1(-\alpha) = -\sigma_1(\alpha) = \alpha, \sigma_1(1/\alpha) = 1/\sigma_1(\alpha) = -1/\alpha, \sigma_1(-1/\alpha) = -1/\sigma_1(\alpha) = 1/\alpha;$$

$$\sigma_2(\alpha) = 1/\alpha \rightsquigarrow \sigma_2(-\alpha) = -\sigma_2(\alpha) = -1/\alpha, \sigma_2(1/\alpha) = 1/\sigma_2(\alpha) = \alpha, \sigma_2(-1/\alpha) = -1/\sigma_2(\alpha) = -\alpha;$$

$$\sigma_3(\alpha) = -1/\alpha \rightsquigarrow \sigma_3(-\alpha) = -\sigma_3(\alpha) = 1/\alpha, \sigma_3(1/\alpha) = 1/\sigma_3(\alpha) = -\alpha, \sigma_3(-1/\alpha) = -1/\sigma_3(\alpha) = \alpha.$$

Since $K/\mathbb{Q}$ is the splitting field of $f(x)$, we can visualise G as a subgroup of S_4 acting on the 4 conjugates of α; and these identities shows that G consists precisely of the double transpositions and of the identity. Therefore $G \simeq V_4 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

4. We know from class that the subgroup lattice of $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is



where $H_j = \{\mathrm{Id}, \sigma_j\}$. Clearly G corresponds to $\mathbb{Q}$, and $\{\mathrm{Id}\}$ corresponds to K. Let $E_j = K^{H_j}$.

The element $\beta_1 = -\alpha\sigma_1(\alpha) = \alpha^2$ lies in E_1, and is a root of $x^2 - 5x + 1$. Therefore $\beta_1 = \frac{5\pm\sqrt{21}}{2} \in E_1$, so $\mathbb{Q}(\sqrt{21}) \subseteq E_1$. Since both have degree 2 over $\mathbb{Q}$ (because $x^2 - 21$ is Eisenstein at 3 and $[G : H_1] = 2$), we actually have $E_1 = \mathbb{Q}(\sqrt{21})$.

The element $\beta_2 = \alpha + \sigma_2(\alpha) = \alpha + 1/\alpha$ lies in E_2, and satisfies

$$\beta_2^2 = \frac{\alpha^4 + 2\alpha^2 + 1}{\alpha^2} = \frac{5\alpha^2 - 1 + 2\alpha^2 + 1}{\alpha^2} = 7.$$

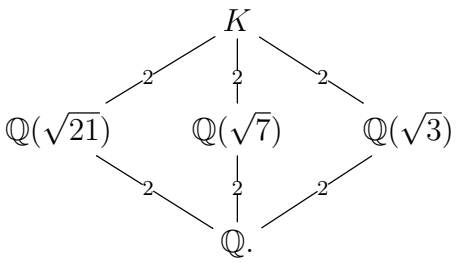
Therefore $\mathbb{Q}(\sqrt{7}) \subseteq E_2$, and that's actually an equality by degrees.

The element $\beta_3 = \alpha + \sigma_3(\alpha) = \alpha - 1/\alpha$ lies in E_3, and satisfies

$$\beta_3^2 = \frac{\alpha^4 - 2\alpha^2 + 1}{\alpha^2} = \frac{5\alpha^2 - 1 - 2\alpha^2 + 1}{\alpha^2} = 3.$$

Therefore $\mathbb{Q}(\sqrt{3}) \subseteq E_3$, and that's actually an equality by degrees.

Conclusion:



5. Since $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ are subfields of K, we have $\sqrt{3}, \sqrt{7} \in K$ (as demonstrated in the previous question), so $\mathbb{Q}(\sqrt{3}, \sqrt{7}) \subseteq K$. If this inclusion were strict, then $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ would be an intermediate field containing both $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$; but the above diagram shows that no such intermediate field exists.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *Yes or no?*

Let $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ (you may assume without proof that f is irreducible over $\mathbb{Q}$), and let $L = \mathbb{Q}[x]/(f)$.

1. Is L a separable extension of $\mathbb{Q}$? Explain.
2. Is L a normal extension of $\mathbb{Q}$? Explain.

   Hint: What does the fact that $f : \mathbb{R} \longrightarrow \mathbb{R}$ is strictly increasing tell you about the complex roots of f?
3. Is L a Galois extension of $\mathbb{Q}$? Explain.

Solution 2

1. Yes, since all fields of characteristic 0 are perfect.
2. Since $f : \mathbb{R} \longrightarrow \mathbb{R}$ is strictly increasing, f has exactly one real root α (intermediate value theorem) and thus one complex-conjugate pair of roots β, $\bar{\beta}$. The images of L by its $[L : \mathbb{Q}] = 3$ $\mathbb{Q}$-embeddings into $\mathbb{C}$ are $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\mathbb{Q}(\beta) \not\subset \mathbb{R}$, and $\mathbb{Q}(\overline{\beta}) \not\subset \mathbb{R}$. Since some are $\subset \mathbb{R}$ but others are not, they do not all agree, so L is not normal over $\mathbb{Q}$.
3. No, since it is not normal over $\mathbb{Q}$.

Exercise 3 *A cyclic biquadratic extension*

Let $\alpha = \sqrt{13}$, $K = \mathbb{Q}(\alpha)$, $\beta = i\sqrt{65 + 18\sqrt{13}}$ (where $i^2 = -1$), $\beta' = i\sqrt{65 - 18\sqrt{13}}$ (note that $65 > 18\sqrt{13}$), and $L = \mathbb{Q}(\beta)$.

1. Prove that the minimal polynomial of β over $\mathbb{Q}$ is
$$M(x) = (x^2 + 65)^2 - 18^2 \cdot 13 = x^4 + 130x^2 + 13.$$
2. What are the Galois conjugates of β over $\mathbb{Q}$?
3. Prove that L is a Galois extension of $\mathbb{Q}$.
Hint: Check that $\beta\beta' = -\alpha$.
4. Explain why there exists an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\beta) = \beta'$.
5. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be such that $\sigma(\beta) = \beta'$ as above. Explain why $\sigma(\alpha)$ makes sense, and determine $\sigma(\alpha)$.
6. Let again $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be such that $\sigma(\beta) = \beta'$ as above. Determine the action of σ on the conjugates of β.
Hint: Again, $\beta\beta' = -\alpha$.
7. Deduce that $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$.
8. Sketch a diagram showing all the fields $\mathbb{Q} \subseteq E \subseteq L$, ordered by inclusion.
9. Does $i\sqrt{13} \in L$?

Solution 3

1. First of all, we have $\beta^2 = -(65 + 18\sqrt{13})$ so $(\beta^2 + 65)^2 = (18\sqrt{13})^2$, so β is indeed a root of $M(x)$. Besides, the expanded form of $M(x)$ reveals that it is Eisenstein at 13, so it is irreducible over $\mathbb{Q}$; since it is also monic, it is the minimal polynomial of β over $\mathbb{Q}$.
2. The Galois conjugates of β over $\mathbb{Q}$ are by definition the roots of its minimal polynomial over $\mathbb{Q}$, namely $M(x)$. Since it is of degree 4, there are at most 4 of them (in fact exactly 4, because we are in characteristic 0 so this irreducible polynomial must be separable). But one checks as above that $\pm\beta$ and $\pm\beta'$ are roots of $M(x)$; since these 4 numbers are distinct, they are the Galois conjugates of β.
3. We find indeed that
$$\beta\beta' = -\sqrt{(65 + 18\sqrt{13})(65 - 18\sqrt{13})} = \sqrt{65^2 - 18^2 \cdot 13} = -\sqrt{13}.$$
Besides, $L \ni \beta^2 = -(65+18\sqrt{13})$, so $\sqrt{13} \in L$ since $65, 18 \in L \supset \mathbb{Q}$. Therefore $\beta' = -\sqrt{13}/\beta \in L$. It follows that the conjugates of β lie in L, so $L = \mathbb{Q}(\beta)$ is the splitting field of $M(x)$ over $\mathbb{Q}$, and is therefore a normal extension of $\mathbb{Q}$. It must also be separable, since the characteristic of $\mathbb{Q}$ is 0.

4. Since $L/\mathbb{Q}$ is Galois, given any conjugate γ of β, there exists at least one $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\beta) = \gamma$.

5. σ is a function from L to L, so $\sigma(\alpha)$ makes sense since we have shown that $\alpha \in L$. More specifically, we have that

$$\alpha = -\frac{\beta^2 + 65}{18},$$

so

$$\sigma(\alpha) = \sigma\left(-\frac{\beta^2 + 65}{18}\right) = -\frac{\sigma(\beta^2) + 65}{18} = -\frac{\beta'^2 + 65}{18} = -\alpha$$

since $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is a field automorphism which fixes the rationals.

6. These conjugates are $\pm\beta$ and $\pm\beta'$, and we already know that $\sigma(\beta) = \beta'$, which immediately implies that $\sigma(-\beta) = -\beta'$. Besides, since $\beta' = -\alpha/\beta$, we have

$$\sigma(\beta') = -\sigma(\alpha)/\sigma(\beta) = \alpha/\beta' = -\beta,$$

which immediately implies that $\sigma(-\beta') = \beta$.

7. We know that $\#\,\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg M(x) = 4$. Lagrange therefore implies that the order of σ is 1 or 2 or 4. But the above question shows that neither σ nor σ^2 is the identity, so σ has order 4. As result, $\mathrm{Gal}(L/\mathbb{Q})$, which is a group of order 4 which contains an element of order 4, must be cyclic (and generated by this element σ; more specifically, we see that σ acts on the conjugates of β by the 4-cycle $\beta \mapsto \beta' \mapsto -\beta \mapsto -\beta' \mapsto \beta$).

8. Since $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$ is cyclic, its only nontrivial subgroup is $H = \langle\sigma^2\rangle$, which has cardinal 2 and therefore index 2. The Galois correspondence thus shows that

$$\mathbb{Q} \subset L^H \subset L$$

is the complete list of intermediate fields, where both inclusions are of degree 2. On the other hand, we know that $\alpha \in L$, so $K = \mathbb{Q}(\alpha)$ is a subfield of L. The minimal polynomial of α over $\mathbb{Q}$ is $x^2 - 13$ (Eisenstein at 13), so $[K : \mathbb{Q}] = 2$; therefore $K = L^H$. Final answer:

$$\mathbb{Q} \subset K \subset L.$$

9. If $i\sqrt{13} \in L$, then $E = \mathbb{Q}(i\sqrt{13})$ is a subfield of L, of degree 2 over $\mathbb{Q}$ (same argument: the minimal polynomial of $i\sqrt{13}$ is x^2+13), so by the above question we must have $E = K$. But this is absurd, for instance because $K \subset \mathbb{R}$ whereas $E \not\subset \mathbb{R}$. So $i\sqrt{13} \notin L$.

Exercise 4 *More square roots*

You may want to use the results established in Exercise 5 of the previous assignment to solve this exercise.

Let $L = \mathbb{Q}(\sqrt{10}, \sqrt{42})$.

1. Prove that L is a Galois extension of $\mathbb{Q}$.

2. Prove that $[L : \mathbb{Q}] = 4$.

3. Describe all the elements of $\mathrm{Gal}(L/\mathbb{Q})$. What is $\mathrm{Gal}(L/\mathbb{Q})$ isomorphic to?

4. Sketch the diagram showing all intermediate extensions $\mathbb{Q} \subseteq E \subseteq L$, ordered by inclusion. Explain clearly which field corresponds to which subgroup.

5. Does $\sqrt{15} \in L$? Use the previous question to answer.

Solution 4

1. L is the splitting field over $\mathbb{Q}$ of $(x^2 - 10)(x^2 - 42) \in \mathbb{Q}[x]$ which is separable (not multiple root), so it is Galois over $\mathbb{Q}$.

2. Since 10 is not a square, $\mathbb{Q}(\sqrt{10}) \neq \mathbb{Q}$, so $[\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = 2$. In order to conclude that $[L : \mathbb{Q}] = 4$, we need to prove that $[L : \mathbb{Q}(\sqrt{10})]$ is 2 and not 1, i.e. that $\sqrt{42} \notin \mathbb{Q}(\sqrt{10})$. This follows from the previous exercise, since $\frac{42}{10} = \frac{21}{5}$ is not a square in $\mathbb{Q}$ as 21 is not a square in $\mathbb{N}$.

3. We already know that $\#\,\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$ since L is Galois over $\mathbb{Q}$. Besides, an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ must take $\sqrt{10} \in L$ to a root of $x^2 - 10 \in \mathbb{Q}[x]$, i.e. to $\pm\sqrt{10}$; and similarly $\sigma(\sqrt{42}) = \pm\sqrt{42}$. Since σ is completely determined by what it does to $\sqrt{10}$ and to $\sqrt{42}$, this leaves us with only 4 possibilities for σ. But since $\#\,\mathrm{Gal}(L/\mathbb{Q}) = 4$, all these possibilities must occur. Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ is made up of

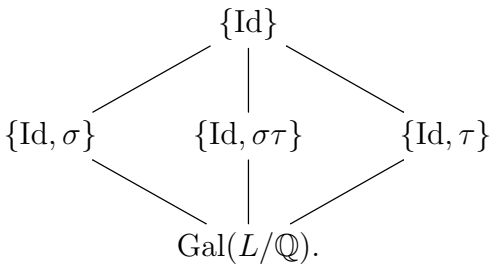
   - Id,
   - $\sigma : \sqrt{10} \mapsto -\sqrt{10},\ \sqrt{42} \mapsto \sqrt{42}$,
   - $\tau : \sqrt{10} \mapsto \sqrt{10},\ \sqrt{42} \mapsto -\sqrt{42}$,
   - $\sigma\tau : \sqrt{10} \mapsto -\sqrt{10},\ \sqrt{42} \mapsto -\sqrt{42}$.

   We see that $\sigma\tau = \tau\sigma$, and that $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{Id}$. Therefore

   $$\begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ (a, b) & \longmapsto & \sigma^a\tau^b \end{array}$$

   is a group isomorphism.

4. We know from class that since $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, its subgroup diagram is

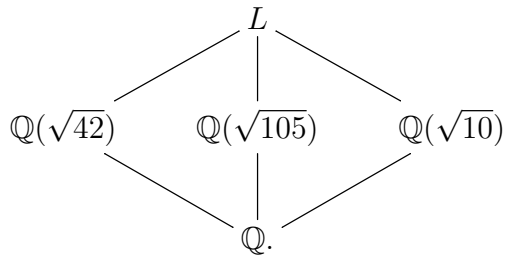
   Let us now find the corresponding fields.

- Clearly, $L^{\{\mathrm{Id}\}} = L$.
- We also have $L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$ since L is Galois over $\mathbb{Q}$.
- We know that $L^{\{\mathrm{Id},\sigma\}}$ is an extension of $\mathbb{Q}$ of degree $[\mathrm{Gal}(L/\mathbb{Q}) : \{\mathrm{Id}, \sigma\}] = 2$. It is the subfield of L formed of the elements fixed by σ, so it contains $\sqrt{42}$ and thus $\mathbb{Q}(\sqrt{42})$. Since the latter is already an extension of $\mathbb{Q}$ of degree 2, it must agree with $L^{\{\mathrm{Id},\sigma\}}$.
- Similarly, $L^{\{\mathrm{Id},\tau\}}$ is an extension of degree 2 of $\mathbb{Q}$, which contains $\sqrt{10}$ as it is fixed by τ, so $L^{\{\mathrm{Id},\tau\}} = \mathbb{Q}(\sqrt{10})$.
- Finally, $L^{\{\mathrm{Id},\sigma\tau\}}$ is an extension of degree 2 of $\mathbb{Q}$, but it contains neither $\sqrt{10}$ nor $\sqrt{42}$ since they are not fixed by $\sigma\tau$. However, $\sqrt{10}\sqrt{42} = \sqrt{420}$ is fixed by $\sigma\tau$ since

$$\sigma\tau(\sqrt{10}\sqrt{42}) = (-\sqrt{10})(-\sqrt{42}),$$

so $L^{\{\mathrm{Id},\sigma\tau\}} = \mathbb{Q}(\sqrt{420}) = \mathbb{Q}(\sqrt{105})$.

The field diagram is thus



5. No. Indeed, if $\sqrt{15} \in L$, then $\mathbb{Q}(\sqrt{15})$ is an intermediate field, but that contradicts the previous question: in view of Exercise 5 of assignment 1, $\mathbb{Q}(\sqrt{15})$ is neither of $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{42})$, $\mathbb{Q}(\sqrt{105})$ as neither $\frac{15}{10} = \frac{3}{2}$, $\frac{15}{42} = \frac{5}{14}$, $\frac{15}{105} = \frac{1}{7}$ are squares in $\mathbb{Q}$.

Exercise 5 *The fifth cyclotomic field*

In this exercise, we consider the primitive 5th root $\zeta = e^{2\pi i/5}$, and we set $L = \mathbb{Q}(\zeta)$. We know that L is Galois over $\mathbb{Q}$, so we define $G = \mathrm{Gal}(L/\mathbb{Q})$. We also let

$$c = \frac{\zeta + \zeta^{-1}}{2} = \cos(2\pi/5) = 0.309\cdots,$$

$$C = \mathbb{Q}(c),$$

and finally

$$c' = \frac{\zeta^2 + \zeta^{-2}}{2} = \cos(4\pi/5) = -0.809\cdots.$$

1. Write down explicitly the minimal polynomial of ζ over $\mathbb{Q}$, and express its complex roots in terms of ζ.
2. Deduce that $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$.

3. Prove that G is a cyclic group. What is its order? Find an explicit generator of G.

4. Deduce that $c \notin \mathbb{Q}$.

5. Make the list of all subgroups of G.

6. Draw a diagram showing all the fields E such that $\mathbb{Q} \subset E \subset L$, ordered by inclusion.

7. What are the conjugates of c over $\mathbb{Q}$? Determine explicitly the minimal polynomial of c over $\mathbb{Q}$ (exact computations only, computations with the approximate value of c are forbidden).

8. Deduce that
$$c = \frac{-1+\sqrt{5}}{4}.$$

9. What are the conjugates of ζ over C (as opposed to over $\mathbb{Q}$)?

10. Deduce that
$$\zeta = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Solution 5

1. The minimal polynomial of ζ over $\mathbb{Q}$ is the 5th cyclotomic polynomial
$$\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1.$$
Its complex roots are the primitive 5-th roots of 1, namely
$$\mu_5^\times = \{\zeta^k \mid k \in (\mathbb{Z}/5\mathbb{Z})^\times\} = \{\zeta, \zeta^2, \zeta^3, \zeta^4\}.$$

2. By Vieta and the previous question,
$$\zeta+\zeta^2+\zeta^3+\zeta^4 = \sum \text{Roots of } \Phi_5(x) = -\text{Coeff. of } x^3 = -1.$$
Alternatively,
$$1+\zeta+\zeta^2+\zeta^3+\zeta^4 = \sum \text{Roots of } x^5-1 = -\text{Coeff. of } x^4 = 0.$$

3. We know that G can be identified to $(\mathbb{Z}/5\mathbb{Z})^\times$ by matching $x \in (\mathbb{Z}/5\mathbb{Z})^\times$ to $\sigma_x : z \mapsto z^x \in G$ for all $z \in \mu_5$. In particular, $G \simeq (\mathbb{Z}/5\mathbb{Z})^\times$ is an Abelian group of order $\phi(5) = 4$. To prove that it is cyclic, we can notice that $2 \in (\mathbb{Z}/5\mathbb{Z})^\times$ is a generator since
$$2 \neq 1, \quad 2^2 = 4 \neq 1, \quad 2^3 = 3 \neq 1, \quad 2^4 = 1,$$
so that $\sigma_2 \in G$ is a generator. We can also argue that since 5 is prime, $\mathbb{Z}/5\mathbb{Z}$ is a finite field, so its multiplicative group is cyclic; but then we still need to find an explicit generator.

4. The element $\sigma_2 \in G$ acts on L by $\zeta \mapsto \zeta^2$, and thus takes $c = \frac{\zeta+\zeta^{-1}}{2}$ to $\frac{\zeta^2+\zeta^{-2}}{2} = c'$. Since $c' \neq c$ (clear from their numerical values), we have $c \notin L^G$; but $L^G = \mathbb{Q}$ since L is Galois over $\mathbb{Q}$.

5. Since $G \simeq \mathbb{Z}/4\mathbb{Z}$ is cyclic of order 4, its only nontrivial subgroup is $2\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, and is generated by $\sigma_2^2 = \sigma_4 = \sigma_{-1}$. Our list is thus

$$\begin{array}{c} \{1\} \\ | \\ H = \{\sigma_{\pm 1}\} \\ | \\ G. \end{array}$$

6. We already know that under the Galois correspondence, $\{\sigma_1\}$ corresponds to L, and G to $\mathbb{Q}$. It remains to identify L^H.

   We know that $[L^H : \mathbb{Q}] = [G : H] = 2$; besides $\sigma_{-1} \in H$ acts by $\zeta \mapsto \zeta^{-1}$ (i.e. is the complex conjugation) and therefore fixes c, so that $c \in L^H$, whence

$$C = \mathbb{Q}(c) \subseteq L^H.$$

   Since $c \notin \mathbb{Q}$, we have $C \supsetneq \mathbb{Q}$ and so $[C : \mathbb{Q}] \geqslant 2$, so finally

$$L^H = C.$$

   Our diagram is thus

$$\begin{array}{c} L \\ | \\ C \\ | \\ \mathbb{Q}. \end{array}$$

7. The conjugates of c over $\mathbb{Q}$ are the $\sigma(c)$ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ (and also for $\sigma \in \mathrm{Gal}(C/\mathbb{Q})$), i.e.

   - c itself for $\sigma = 1$,
   - $\frac{\zeta^2+\zeta^{-2}}{2} = c'$ for $\sigma = 2$,
   - $\frac{\zeta^{-2}+\zeta^2}{2} = c'$ for $\sigma = 3 = -2$,
   - and $\frac{\zeta^{-1}+\zeta}{2} = c$ for $\sigma = 4 = -1$,

   so finally, just c itself and c'. (We can get the same conclusion faster by taking σ in the smaller quotient $\mathrm{Gal}(C/\mathbb{Q}) = G/H = \{\sigma_{\pm 1}, \sigma_{\pm 2}\} \simeq (\mathbb{Z}/5\mathbb{Z})^\times/\pm 1$ of $\mathrm{Gal}(L/\mathbb{Q})$, if we are not afraid to work with this quotient). The minimal

polynomial of c over $\mathbb{Q}$ is thus

$$\begin{aligned}\prod_{\beta \text{ conjugate to } c}(x-\beta) &= (x-c)(x-c') \\ &= x^2-(c+c')x+cc' \\ &= x^2-\frac{\zeta+\zeta^{-1}+\zeta^2+\zeta^{-2}}{2}x+\frac{(\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})}{4} \\ &= x^2-\frac{\zeta+\zeta^4+\zeta^2+\zeta^3}{2}x+\frac{\zeta^3+\zeta^4+\zeta+\zeta^2}{4} \\ &= x^2+\frac{1}{2}x-\frac{1}{4}.\end{aligned}$$

8. By solving $x^2+\frac{1}{2}x-\frac{1}{4}=0$, we find that $\Delta=5/4$, whence

$$c,c'=\frac{-1\pm\sqrt{5}}{4}.$$

   Since $c>c'$, we deduce that $c=\frac{-1+\sqrt{5}}{4}$ (and also that $c'=\frac{-1-\sqrt{5}}{4}$).

9. The conjugates of ζ over C are the elements of the orbit of ζ under $H=\mathrm{Gal}(L/C)$, that is to say the $\sigma(\zeta)$ for $\sigma\in\mathrm{Gal}(L/C)=H=\{\sigma_{\pm 1}\}$. So they are ζ and ζ^{-1}.

10. Similarly to the previous questions, the minimal polynomial of ζ over C is

$$\prod_{\substack{\beta \text{ conjugate}\\ \text{of } \zeta \text{ over } C}}(x-\beta)=(x-\zeta)(x-\zeta^{-1})=x^2-(\zeta+\zeta^{-1})x+\zeta\zeta^{-1}=x^2-2cx+1\in C[x],$$

    whose roots are

$$\frac{2c\pm\sqrt{4c^2-4}}{2}=c\pm\sqrt{c^2-1}=\frac{-1+\sqrt{5}\pm i\sqrt{10+2\sqrt{5}}}{4}$$

    using $c=\frac{-1+\sqrt{5}}{4}$. Since ζ (as opposed to ζ^{-1}) is the root with positive imaginary part (draw a regular pentagon; alternatively $\mathrm{Im}\,\zeta=\sin(2\pi/5)>0$ as $2\pi/5<\pi$), we conclude that

$$\zeta=\frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Exercise 6 *Bioche vs. Galois*

This exercise has an unusual flavour, and is not representative of what you should expect for the final exam. The goal of this exercise is to give a Galois-theoretic interpretation of Bioche's rules (cf. `https://en.wikipedia.org/wiki/Bioche%27s_rules`*), which are rules suggesting appropriate substitutions to turn integrals involving trigonometric functions into integrals of rational fractions. Knowledge of Bioche's rules is not required to solve this exercise.*

In this exercise, we use the shorthands s for the sine function and c for the cosine function, and we denote by $\mathbb{C}(s,c)$ the set of rational fractions in $\sin x$ and $\cos x$ with complex coefficients, meaning of expressions such as

$$\frac{2sc^3 - i}{c - 7s + 3} = \frac{2\sin x \cos^3 x - i}{\cos x - 7\sin x + 3}.$$

Observe that $\mathbb{C}(s,c)$ is a field with respect to point-wise addition and multiplication.

We write $\mathbb{C}(c)$ for the subfield of $\mathbb{C}(s,c)$ consisting of rational fractions which can be expressed in terms of c only, and similarly $\mathbb{C}(s)$ for rational fractions in s only. For example, $\frac{c^3-2c^2+2i}{ic-1} \in \mathbb{C}(c)$, but $s \notin \mathbb{C}(c)$ since all the elements of $\mathbb{C}(c)$ are even functions whereas s is not; observe however that $s^2 \in \mathbb{C}(c)$ since $s^2 = 1 - c^2$.

We also define $K = \mathbb{C}(s) \cap \mathbb{C}(c) \subset \mathbb{C}(s,c)$, so that for instance the function $c_2 = \cos(2x)$ lies in K since $c_2 = 2c^2 - 1 = 1 - 2s^2$.

Finally, we define

$$\begin{array}{rcl} \mu : \mathbb{C}(s,c) & \to & \mathbb{C}(s,c) \\ f(x) & \mapsto & f(-x), \end{array} \qquad \begin{array}{rcl} \tau : \mathbb{C}(s,c) & \to & \mathbb{C}(s,c) \\ f(x) & \mapsto & f(x+\pi), \end{array} \qquad \begin{array}{rcl} \sigma : \mathbb{C}(s,c) & \to & \mathbb{C}(s,c) \\ f(x) & \mapsto & f(\pi - x); \end{array}$$

observe that these are field automorphisms of $\mathbb{C}(s,c)$ which are involutive and commute with each other, so they generate the subgroup

$$G = \{\mathrm{Id},\, \mu = \sigma\tau,\, \tau = \mu\sigma,\, \sigma = \mu\tau\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

of $\mathrm{Aut}\big(\mathbb{C}(s,c)\big)$.

1. Prove that the four inclusions $K \subset \mathbb{C}(s) \subset \mathbb{C}(s,c)$ and $K \subset \mathbb{C}(s) \subset \mathbb{C}(s,c)$ are all strict.

2. Prove that $[\mathbb{C}(s) : K] = [\mathbb{C}(s,c) : \mathbb{C}(s)] = [\mathbb{C}(c), K] = [\mathbb{C}(s,c) : \mathbb{C}(c)] = 2$.

3. Prove that $K = \mathbb{C}(c_2)$, where $\mathbb{C}(c_2)$ is the field of rational fractions expressible in terms of c_2 only.

4. Prove that the extension $\mathbb{C}(s,c)/K$ is Galois, and describe its Galois group.

5. Let $f \in \mathbb{C}(s,c)$. Prove that if f is invariant by any two of μ, τ, σ, then it is also invariant by the third one, and that in this case $f \in \mathbb{C}(c_2)$.

6. Determine the minimal polynomials over K of the elements $t = \tan x = s/c$ and $s_2 = \sin(2x) = 2sc$ of $\mathbb{C}(s,c)$.

7. Draw a diagram showing all the subgroups of $\mathrm{Gal}(\mathbb{C}(s,c)/K)$.

8. Draw a diagram showing all the intermediate fields E between K and $\mathbb{C}(s,c)$. Where are the fields $\mathbb{C}(t)$, $\mathbb{C}(s_2, c_2)$, and $\mathbb{C}(s_2)$ on this diagram?

Make sure find an explanation for all the surprising conclusions you may be led to!

Solution 6

1. Every element of $\mathbb{C}(c)$ is even since c is; therefore $s \notin \mathbb{C}(c)$, so $\mathbb{C}(s,c) = \mathbb{C}(c)(s) \supsetneq \mathbb{C}(s)$. The same argument shows that $s \notin K \subset \mathbb{C}(c)$, so $\mathbb{C}(s) \supsetneq K$. Besides, s is invariant by σ whereas c is not, so $c \notin \mathbb{C}(s)$ so $\mathbb{C}(s,c) \supsetneq \mathbb{C}(s)$, and similarly $c \notin K$ so $\mathbb{C}(c) \supsetneq K$.

2. Since $s^2+c^2 = 1$, s is a root of the polynomial $x^2-(1-c^2) \in \mathbb{C}(c)[x]$; therefore, s is algebraic over $\mathbb{C}(c)$ over degree at most 2; since $\mathbb{C}(s,c) = \mathbb{C}(c)(s)$, this shows that $[\mathbb{C}(s,c) : \mathbb{C}(c)] \leq 2$. Since this degree cannot be 1 by the previous question, it must be 2. Similarly, $[\mathbb{C}(s,c) : \mathbb{C}(s)] = 2$.

   The identity $c_2 = 2c^2 - 1$ proves that c is a root of $2x^2 - 1 - c_2 \in K[x]$, so c is algebraic of degree at most 2 over K. We have $\mathbb{C}(c) \subseteq K(c)$ since $\mathbb{C} \subset K$, and $K(c) \subseteq \mathbb{C}(c)$ since $K \subset \mathbb{C}(c)$, so $\mathbb{C}(c) = K(c)$ is an extension of K of degree at most 2, hence exactly 2 by the previous question. Similarly, $\mathbb{C}(s) = K(s)$ is an extension of K of degree at most 2, and hence 2, since s is a root of $2x^2 + c_2 - 1 \in K[x]$.

3. We know that $\mathbb{C}(c_2) \subseteq K \subsetneq \mathbb{C}(c)$; besides, since $\mathbb{C}(c) = \mathbb{C}(c, c_2) = \mathbb{C}(c_2)(c)$ as $c_2 = 2c^2-1 \in \mathbb{C}(c)$, the fact that the polynomial $2x^2-1-c_2$ used in the previous question actually lies in $\mathbb{C}(c_2)[x]$ shows that we have $[\mathbb{C}(c) : \mathbb{C}(c_2)] \leq 2$. The tower law allows us to conclude that $[K : \mathbb{C}(c_2)] \leq 1$.

4. The tower law shows that $[\mathbb{C}(s,c) : \mathbb{C}(c_2)] = [\mathbb{C}(s,c) : \mathbb{C}(c)][\mathbb{C}(c) : K] = 2 \times 2 = 4$, so $\#\operatorname{Aut}_K\big(\mathbb{C}(s,c)\big) \leq 4$, with equality iff. $\mathbb{C}(s,c)$ is Galois over K. But since c_2 is fixed by Id, μ, τ, and σ, these 4 automorphisms induce the identity on $\mathbb{C}(c_2) = K$; therefore $\#\operatorname{Aut}_K\big(\mathbb{C}(s,c)\big) \geq 4$. In conclusion, $\#\operatorname{Aut}_K\big(\mathbb{C}(s,c)\big) = 4 = [\mathbb{C}(s,c) : K]$, so $\mathbb{C}(s,c)$ is Galois over K with Galois group $\operatorname{Gal}(\mathbb{C}(s,c)/K) = \{\mathrm{Id}, \mu, \sigma, \tau\} = G$.

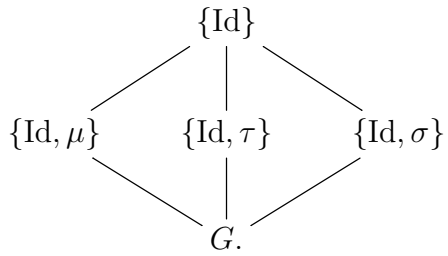
5. Since any two of μ, τ, σ generate G, any element of $\mathbb{C}(s,c)$ fixed by two of those is actually fixed by the whole of $G = \operatorname{Gal}(\mathbb{C}(s,c)/K)$, and therefore lies in $\mathbb{C}(s,c)^{\operatorname{Gal}(\mathbb{C}(s,c)/K)} = K = \mathbb{C}(c_2)$.

6. Since $\mathbb{C}(s,c)$ is Galois over K, the minimal polynomial of any $\alpha \in \mathbb{C}(s,c)$ is the polynomial whose roots are the orbit of α under $\operatorname{Gal}(\mathbb{C}(s,c)) = G$.

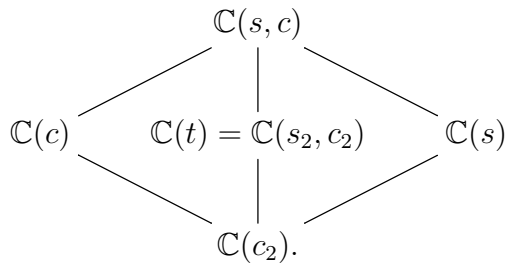
   In the case $\alpha = t$, this orbit is $\{\mathrm{Id}\, t = t, \mu t = -t, \tau t = t, \sigma t = -t\} = \{t, -t\}$, so the minimal polynomial of t over K is $(x-t)(x+t) = x^2 - t^2$. It must lie in $K[x]$, so we necessarily have $t^2 \in K = \mathbb{C}(c_2)$; indeed, we find that $t^2 = \frac{s^2}{c^2} = \frac{1-c_2}{1+c_2} \in \mathbb{C}(c_2)$.

   Similarly, since the orbit of s_2 under G is $\{s_2, -s_2\}$, the minimal polynomial of s_2 over K is $(x-s_2)(x+s_2) = x^2 - s_2^2$, so we must have $s_2^2 \in K = \mathbb{C}(c_2)$; and indeed $s_2^2 = (2sc)^2 = (2s^2)(2c^2) = (1+c_2)(1-c_2) = 1 - c_2 \in \mathbb{C}(c_2)$ — that is simply $s_2^2 + c_2^2 = 1$.

7. Since $\mathrm{Gal}(\mathbb{C}(s,c)/K) = G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, its subgroup lattice is



8. We apply the Galois correspondence. The subfields corresponding to $\{\mathrm{Id}\}$ and G are of course $\mathbb{C}(s,c)$ and $K = \mathbb{C}(c_2)$, respectively. The subfield corresponding to $\{\mathrm{Id}, \mu\}$ contains c since μ fixes c, and is an extension of K of degree $[G : \{\mathrm{Id}, \mu\}] = 4/2 = 2$, so it is $\mathbb{C}(c)$ by the second question. Similarly, the subfield corresponding to $\{\mathrm{Id}, \sigma\}$ is $\mathbb{C}(s)$. Finally, the subfield corresponding to $\{\mathrm{Id}, \tau\}$ is also an extension of K of degree 2; besides, it contains t since t is invariant by τ. By the previous question, $\mathbb{C}(t)$ is an extension of K of degree at most 2; but $t \notin K$ since t is not fixed by μ, so this extension has degree exactly 2, so it is the subfield corresponding to $\{\mathrm{Id}, \tau\}$. The same thing can be said about $K(s_2)$, so we are led to the curious conclusion that $\mathbb{C}(t) = K(s_2) = \mathbb{C}(s_2, c_2)$; and indeed $t = \frac{s}{c} = \frac{2sc}{2c^2} = \frac{s_2}{1+c_2} \in \mathbb{C}(s_2, c_2)$ whereas $s_2 = 2sc = 2tc^2 = \frac{2tc^2}{s^2+c^2} = \frac{2t}{t^2+1} \in \mathbb{C}(t)$.



As for $\mathbb{C}(s_2)$, it does not appear on this diagram, simply because $\mathbb{C}(c_2) \not\subset \mathbb{C}(s_2)$! (so yes, that was a trap.) Indeed, every element of $\mathbb{C}(s_2)$ is invariant by $x \mapsto \pi/2 - x$ since s_2 is; but c_2 is not.