Galois theory — Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU34101/index.html

Version: November 22, 2021

Email your answers to mascotn@tcd.ie by Monday 22nd November, 4PM.

Exercise 1 *A polynomial with Galois group A_4 (100 pts)*

Let $F(x) = x^4 - 2x^3 + 2x^2 + 2 \in \mathbb{Q}[x]$. We denote the roots of $F(x)$ in $\mathbb{C}$ by α_1, α_2, α_3, and α_4.

In this exercise, you may use without proof the following facts:

- *The discriminant of f is $\Delta_f = 3136 = 2^6 \cdot 7^2$.*
- *The transitive subgroups of the symmetric group S_4 are*
  - *S_4 itself,*
  - *the alternating group A_4,*
  - *the dihedral group D_8 of symmetries of the square acting on the vertices of the square,*
  - *the Klein group $V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,*
  - *and the cyclic group $\mathbb{Z}/4\mathbb{Z}$.*

1. *(15 pts)* Prove that $F(x)$ is separable and irreducible over $\mathbb{Q}$.
2. *(20 pts)* Prove that $F(x)$ factors mod 3 as a linear factor times an irreducible factor of degree 3.
3. *(25 pts)* Prove that the Galois group of $F(x)$ is A_4.
4. *(20 pts)* Prove that $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2)$.
5. *(20 pts)* Determine the degrees of the irreducible factors of $F(x)$ over $\mathbb{Q}(\alpha_1)$.

Solution 1

1. This follows from the fact that f is Eisenstein at 2.
2. First of all, f has a root mod 3, namely $x = 1$ mod 3. In particular, $F(x)/(x - 1) \in \mathbb{F}_3[x]$; we compute that actually $F(x) \equiv (x-1)(x^3 - x^2 + x + 1)$ mod 3. Besides $g(x) = x^3 - x^2 + x + 1$ has no roots in $\mathbb{F}_3$, so it is irreducible since it has degree 3.

3. Let $G = \mathrm{Gal}_{\mathbb{Q}}(f)$. Then G is a subgroup of S_4. By the first question, G is transitive, so it is one of the groups on the list given at the beginning of the exercise. By the previous question, G contains a 3-cycle; this eliminates all possibilities except S_4 and A_4. Finally, since Δ_f is a square in $\mathbb{Q}$, G is contained in A_4.

4. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $E = \mathbb{Q}(\alpha_1, \alpha_2)$. We know that L is Galois over $\mathbb{Q}$, with Galois group A_4. The subgroup H corresponding to E is the subgroup of A_4 consisting of permutations that leave both α_1 and α_2 fixed. In S_4, the only such permutations are Id and (34), but $(34) \notin S_4$, so $H = \{\mathrm{Id}\}$. Therefore $E = L$.

5. Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ above, and $E' = \mathbb{Q}(\alpha_1)$. Clearly, we have the (possibly incomplete) factorisation $F(x) = (x - \alpha_1)h(x)$ over E', where $h(x) = (x-\alpha_2)(x-\alpha_3)(x-\alpha_4) = F(x)/(x-\alpha_1) \in E'[x]$. The subgroup H' corresponding to E' is the stabiliser of α_1. In particular, it contains the 3-cycle $\sigma = (234)$. Since $\sigma \in H' = \mathrm{Gal}(L/E')$ permutes the roots of $h(x)$ transitively, $h(x)$ is irreducible over E'. We thus have two irreducible factors, one of degree 1 and one of degree 3.

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

Exercise 2 *More Galois groups over $\mathbb{Q}$*

Prove that the following polynomials have no repeated root in $\mathbb{C}$, and determine their Galois group over $\mathbb{Q}$. *Warning: Some polynomials may be reducible!*

1. $F_1(x) = x^3 - 4x + 6$,

2. $F_2(x) = x^3 - 7x + 6$,

3. $F_3(x) = x^3 - 21x - 28$,

4. $F_4(x) = x^3 - x^2 + x - 1$,

5. $F_5(x) = x^5 - 6x + 3$, *using without proof the fact that this polynomial has exactly* 3 *real roots.*

Solution 2

1. Since $\mathrm{disc}(F_1) = -4 \cdot (-4)^3 - 27 \cdot 6^2 = -716$ is nonzero, $F_1(x)$ has no repeated root, and since $-716 < 0$ is clearly not a square in $\mathbb{Q}$, $\mathrm{Gal}_{\mathbb{Q}}(F_1) \not\subset A_3$. Besides $F_1(x)$ is Eisenstein at $p = 2$, so it is irreducible over $\mathbb{Q}$, so its Galois group is either S_3 or A_3. Conclusion:
$$\mathrm{Gal}_{\mathbb{Q}}(F_1) = S_3.$$

2. The possible rational roots of $F_2(x)$ are $\pm 1, \pm 2, \pm 3, \pm 6$. Checking these, we find that 1, 2, and -3 are roots of $F_2(x)$. Since $F_2(x) = (x-1)(x-2)(x+3)$ splits completely over $\mathbb{Q}$,
$$\mathrm{Gal}_{\mathbb{Q}}(F_2) = \{\mathrm{Id}\}.$$

3. Since $\mathrm{disc}(F_3) = -4 \cdot (-21)^3 - 27 \cdot (-28)^2 = 15876 = 126^2$ is a nonzero square in $\mathbb{Q}$, $F_3(x)$ has no repeated root, and its Galois group is contained in A_3. Besides $F_3(x)$ is Eisenstein at $p = 7$, so it is irreducible over $\mathbb{Q}$, so its Galois group is either S_3 or A_3. Conclusion:
$$\mathrm{Gal}_{\mathbb{Q}}(F_3) = A_3 \simeq \mathbb{Z}/3\mathbb{Z}.$$

4. The possible roots of $F_4(x)$ are ± 1. Of these, we check that only $+1$ is a root. Dividing $F_4(x)$ by $(x-1)$ reveals that $F_4(x) = (x-1)(x^2+1)$; in particular, $F_4(x)$ has no repeated root. Since the factor x^2+1 is clearly irreducible over $\mathbb{Q}$, we get
$$\mathrm{Gal}_{\mathbb{Q}}(F_4) = \mathbb{Z}/2\mathbb{Z}$$
(generated by complex conjugation swapping i and $-i$).

5. Thanks to the formula
$$\mathrm{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big),$$
we compute that
$$\mathrm{disc}(F_5) = (-1)^{5\cdot 4/2}\big((-4)^4 \cdot (-6)^5 + 5^5 \cdot 3^4\big) = -1737531.$$
Since $\mathrm{disc}(F_5) \neq 0$, F_5 has no repeated root, so it has 3 real roots and 2 complex-conjugate nonreal roots. We may also say that since $\mathrm{disc}(F_5) < 0$, F_5 has an odd number of complex conjugate pairs of roots, which forces it to have 2 complex roots and 3 real roots, but this was not required by the question. Finally, since $\mathrm{disc}(F_5) < 0$ is not a square in $\mathbb{Q}$, $\mathrm{Gal}_{\mathbb{Q}}(F_5) \not\subset A_5$, but this does not help us identify $\mathrm{Gal}_{\mathbb{Q}}(F_5)$.

   Mod 2, we have $F_5(x) \equiv x^5 - 1$, which has $x = 1$ s a root. Dividing by $x - 1$ shows that $F_5(x) \equiv (x-1)G(x)$, where $G(x) = x^4 + x^3 + x^2 + x + 1$. We check that $G(x)$ has no root in $\mathbb{F}_2$, so it has no linear factor. Besides, we compute that $\gcd(G, x^4 - x) = 1$ (we could see this directly: $\gcd(G, x^4 - x) = \gcd(G - (x^4 - x), x^4 - x) = \gcd(x^3 + x^2 + 1, x^4 - x) = 1$ since $x^3 + x^2 + 1$, having degree 3 and no root in $\mathbb{F}_2$, is irreducible, and thus has no factor of degree 1 or 2), so G has no factor of degree 2 either (alternatively we know that the only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $x^2 + x + 1$, and

$G \neq (x^2+x+1)^2 = x^4+x^2+1)$. As a conclusion, G is irreducible, so the complete factorisation of F_5 mod 2 is

$$(x-1)(x^4+x^3+x^2+x+1),$$

which shows that $\mathrm{Gal}_{\mathbb{Q}}(F_5)$ contains a 4-cycle (which confirms that $\mathrm{Gal}_{\mathbb{Q}}(F_5) \not\subset A_5$).

Besides, complex conjugation is an element of $\mathrm{Gal}_{\mathbb{Q}}(F_5)$ which fixes the 3 real roots and swaps the 2 complex roots, so it is a 2-cycle.

Finally, F_5 is irreducible over $\mathbb{Q}$ as it is Eisenstein at $p=3$, so $\mathrm{Gal}_{\mathbb{Q}}(F_5)$ is a transitive subgroup of S_5.

Since any transitive subgroup of S_n containing an $(n-1)$-cycle and a 2-cycle must be the whole of S_n, we conclude that

$$\mathrm{Gal}_{\mathbb{Q}}(F_5) = S_5.$$