Galois theory — Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2019/MAU34101/index.html

Version: November 18, 2019

Answers are due for Tuesday November 19th, 3PM.

Exercise 1 *Galois groups over $\mathbb{Q}$ (100 pts)*

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. (10 pts) $F_1(x) = x^3 - 4x + 6$,
2. (10 pts) $F_2(x) = x^3 - 7x + 6$,
3. (10 pts) $F_3(x) = x^3 - 21x - 28$,
4. (10 pts) $F_4(x) = x^3 - x^2 + x - 1$,
5. (60 pts) $F_5(x) = x^5 - 6x + 3$, *using without proof the fact that this polynomial has exactly* 3 *real roots.*

Solution 1

1. Since $\operatorname{disc}(F_1) = -4 \cdot (-4)^3 - 27 \cdot 6^2 = -716$ is nonzero, $F_1(x)$ has no repeated root, and since $-716 < 0$ is clearly not a square in $\mathbb{Q}$, $\operatorname{Gal}_{\mathbb{Q}}(F_1) \not\subset A_3$. 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:
$$\operatorname{Gal}_{\mathbb{Q}}(F_1) = S_3.$$

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 $\mathbb{Q}$,
$$\operatorname{Gal}_{\mathbb{Q}}(F_2) = \{\mathrm{Id}\}.$$

3. Since $\operatorname{disc}(F_3) = -4 \cdot (-21)^3 - 27 \cdot (-28)^2 = 15876 = 126^2$ 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:
$$\operatorname{Gal}_{\mathbb{Q}}(F_3) = A_3 \simeq \mathbb{Z}/3\mathbb{Z}.$$

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