Galois theory — Exercise sheet 3

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

Version: November 23, 2023

Submit[1] your answers by Monday November 20th, 5PM.

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 $\mathrm{disc}(F_1) = -4 \cdot (-4)^3 - 27 \cdot 6^2 = -716$ 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:
$$\mathrm{Gal}_{\mathbb{Q}}(F_3) = A_3 \simeq \mathbb{Z}/3\mathbb{Z}.$$

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

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

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 *The sign of the discriminant*

Let $F(x) \in \mathbb{R}[x]$ be a separable polynomial. Suppose $F(x)$ has r roots in $\mathbb{R}$, and s complex-conjugate pairs of roots in $\mathbb{C} \setminus \mathbb{R}$ (so that $\deg F = r + 2s$).

1. Let $G = \mathrm{Gal}_{\mathbb{R}}(F)$. Describe G: how many elements does it have, and how do these elements act on the roots of F?

   Hint: Distinguish the cases $s = 0$ and $s \neq 0$.

2. Prove that the sign of $\operatorname{disc} F$ is $(-1)^s$.

   Hint: What are the squares in $\mathbb{R}$?

Solution 2

1. By definition $G = \mathrm{Gal}(S/\mathbb{R})$ where $S = \mathbb{R}(\text{roots of } F)$ is the splitting field of $F(x)$ over $\mathbb{R}$.

   If $s = 0$, then all the roots of F are real, so $S = \mathbb{R}$, so $G = \mathrm{Gal}(\mathbb{R}/\mathbb{R}) = \{\mathrm{Id}\}$.

   If $s > 0$, then at least some of the roots of F are not real, so $\mathbb{R} \subsetneq S \subseteq \mathbb{C}$. As $[\mathbb{C} : \mathbb{R}] = 2$, the only possibility is that $S = \mathbb{C}$. Therefore $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, c\}$ where c is the complex conjugation, which fixes all real roots and swaps all non-real roots with their complex conjugates.

2. First of all, $\operatorname{disc} F \neq 0$ since we assume that F is separable. Next, a nonzero real number is positive iff. it is a square in $\mathbb{R}$, so the hint points to the criterion for G being contained in the alternating group.

   If $s = 0$ then $G = \{\mathrm{Id}\}$ is obviously contained in the alternating group, so $\operatorname{disc} F$ is a square and is therefore positive, so the formula is satisfied in this case.

   Suppose now that $s > 0$. Then $G = \{\mathrm{Id}, c\}$ where c acts on the roots of F as the product of s disjoint 2-cycles. Since 2-cycles are odd, we therefore have $\varepsilon(c) = (-1)^s$. As a result, $\operatorname{disc} F$ is positive iff. $\operatorname{disc} F$ is a square in $\mathbb{R}$ iff. G is contained in the alternating group iff. $\varepsilon(c) = +1$ iff. s is even, so the result follows.

Exercise 3 *The Trinks polynomial*

Reminder: $\operatorname{disc}(x^n + ax + b) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big)$.

Let $F(x) = x^7 - 7x + 3 \in \mathbb{Q}[x]$.

1. Prove that $F(x)$ is separable over $\mathbb{Q}$.

   From now on, we denote by G the Galois group of $F(x)$ over $\mathbb{Q}$, and we see it as a subgroup of S_7.

2. For which prime number(s) p is $F(x)$ not separable mod p?

3. Prove that G is contained in A_7.

   We admit without proof[2] *that there are exactly 664,579 prime numbers up to* 10^7*, and that when* $F(x)$ *is factored mod these primes, we obtain the following factorisations:*

Factorisation	#Occurrences
Tot. split	$3,906$
$1+1+1+2+2$	$83,126$
$1+3+3$	$221,776$
$1+2+4$	$165,851$
Irreducible	$189,918$
Other	2.

4. Give a coarse estimate of $\#G$.

5. Prove that $\#G$ is divisible by 3, by 4, and by 7. Use this to refine your estimate of $\#G$.

Solution 3

Let $F(x) = x^7 - 7x + 3 \in \mathbb{Q}[x]$.
Reminder: $\operatorname{disc}(x^n + ax + b) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}a^n + n^n b^{n-1}\big)$.

1. We have $F'(x) = 7x - 7 = 7(x-1)$; as $F(1) \neq 0$, F and F' are coprime, so F is separable.

2. We know that these are exactly the prime factors of $\operatorname{disc} F$, which by the formula given at the beginning of the exercises evaluates to

   $$(-1)^{7\cdot 6/2}\big((-6)^6\cdot(-7)^7 + 7^7\cdot 3^6\big) = 7^7(6^6 - 3^6) = 3^6\cdot 7^7(2^6-1) = 3^6\cdot 7^7\cdot 63 = 3^8 7^8.$$

   (Incidentally, the fact that this is nonzero is another proof of the separability of F.)

   Therefore, these primes are precisely 3 and 7.

3. This follows from the fact that $\operatorname{disc} F = (3^4 \cdot 7^4)^2$ is a square in $\mathbb{Q}$.

4. The two "other" prime numbers are of course 3 and 7, for which we cannot extract any information since $F(x)$ is not separable mod these primes.

   By the Cebotarev density theorem, the probability[3] that F mod p splits completely is $1/\#G$. Therefore

   $$\#G \approx \frac{664,579}{3,906} \approx 170.$$

[2] With a good computer program, it is actually not very difficult to determine this.

[3] To make this rigorous, we should give a proper definition of this probability; see `https://en.wikipedia.org/wiki/Dirichlet_density`

5. Since there exists a prime p (in fact, plenty of them) such that $F \bmod p$ factors as $1+2+4$, there exists an element of G of the form $(*)(**)(***)$. Such an element has order 4, so $4 \mid \#G$ by Lagrange. Similarly, the fact that a factorisation of the form $1+3+3$ shows up implies that $G \ni (*)(***)(***)$, so $3 \mid \#G$; and finally, the presence of p such that $F \bmod p$ is irreducible shows that G contains 7-cycles so that $7 \mid \#G$.

   Since $3, 4, 7$ are pairwise coprime, this means that $\#G$ is a multiple of $3 \cdot 4 \cdot 7 = 84$. We estimated $\#G \approx 170$, and $170/84 \approx 2$, so a better estimate is $\#G = 2 \cdot 84 = 168$.

   Remark: In the symmetric group S_n, conjugation can be calculated as

$$g(a,b,c,\cdots)(x,y,z,\cdots)\cdots g^{-1} = (g(a),g(b),g(c),\cdots)(g(x),g(y),g(z),\cdots)\cdots,$$

   so two permutations have the same cycle decomposition type iff. they are conjugate in S_n. In particular, if two elements of G are conjugate in G, then they have the same cycle decomposition type (but the converse may not hold, since they could be conjugates in S_7 but not in G). It follows that the set of elements of G of given cycle decomposition type is a union of conjugacy classes of G. Since conjugacy classes are disjoint and since the size of a conjugacy class divides $\#G$, the proportion of such elements is a sum of reciprocals of divisors of $\#G$. And indeed,

$$\frac{83,126}{664,579} \approx \frac{1}{8},\ \frac{221,776}{664,579} \approx \frac{1}{3},\ \frac{165,851}{664,579} \approx \frac{1}{4},\ \frac{189,918}{664,579} \approx \frac{2}{7}.$$

   Note: it can be proved that G is actually isomorphic to $\mathrm{PGL}_3(\mathbb{F}_2)$ of automorphisms of the projective plane over $\mathbb{F}_2$, which is a simple group of order 168; see for instance `https://www.sciencedirect.com/science/article/pii/0022314X79900209`. In fact, trinomials with exotic Galois groups are extremely rare (see `https://people.math.harvard.edu/~elkies/trinomial.html`); this particular polynomial $F(x)$ was discovered by Trinks in 1968. Nowadays, efficient algorithms are known to determine the Galois group over $\mathbb{Q}$ of any polynomial of any degree; see `https://doi.org/10.1112/S1461157013000302`.