Galois theory — Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2025/MAU34101/index.html

Version: November 11, 2025

Submit your answers (preferably by LaTeX),
either by bringing them to class or by emailing them to the T.A.,
by Friday November 21st, 4PM.

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

Note: This exercise was part of the 2023 exam.

Let $F(x) = x^4 + 2x^2 + 4x + 10 \in \mathbb{Q}[x]$. 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 $\Delta_F = 246016 = 2^8 \cdot 31^2$.**
- **Up to conjugacy, the transitive subgroups of the symmetric group S_4 are**
  - S_4 **itself,**
  - **the alternate group A_4,**
  - **the dihedral group D_8 of symmetries 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 $\{(1234)^n \mid 0 \leqslant n < 4\} \simeq \mathbb{Z}/4\mathbb{Z}$.**

1. *(5 pts)* Show that $F(x)$ is irreducible over $\mathbb{Q}$.
2. *(10 pts)* Show that $F(x)$ separable.
3. *(20 pts)* Prove that $\mathrm{Gal}_{\mathbb{Q}}(F)$ contains a 3-cycle.

   Hint: Pick a prime for which calculations are easy.
4. *(20 pts)* Show that the $\mathrm{Gal}_{\mathbb{Q}}(F) \simeq A_4$.
5. *15 pts)* Prove that $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\alpha_1, \alpha_2)$.

   Hint: Apply the Galois correspondence.
6. *(20 pts)* Determine the degrees of the irreducible factors of $F(x)$ over $\mathbb{Q}(\alpha_1)$.

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 *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.*

Exercise 3 *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 $\mathbb{R}$?

3. Application: Determine the number of real roots of $x^3 - tx + 6 \in \mathbb{R}[x]$ in terms of the parameter $t \in \mathbb{R}$.

Exercise 4 *The Trinks polynomial*

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

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[1] *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 $\#G$.

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