Galois theory — Exercise sheet 3

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

Version: November 14, 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.*

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 $\mathbb{R}$?

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

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 $\#G$.

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