Math 414 Homework Assignment 12

DUE DATE: APR. 7, 2016

1. In this problem we will check that $x^n - x - 1$ has Galois group S_n (i.e, the splitting field of $x^n - x - 1$ has Galois group S_n over $\mathbb{Q}$) for $n = 2$, 3, and 4.

(a) Show the case $n = 2$.

For $n = 3$, 4 you may assume $x^n - x - 1$ is irreducible, without proving it. (Although proving it for $n = 3$ is something we know how to do.)

(b) Show the case $n = 3$.

(c) Show the case $n = 4$.

REMINDERS : (1) We have algorithms for computing the Galois groups of irreducible polynomials. (2) The formula for the discriminant of a cubic is in **H9** Q2. (3) given a quartic $f = x^4 + bx^3 + cx^2 + dx + e$ then the resolvent cubic of f is $p(t) = t^3 - ct^2 + (bd - 4e)t + (4ce - d^2 - b^2e)$. (4) The discriminant of a quartic polynomial is the same as the discriminant of its resolvent cubic.

2. In this question we will investigate the norm in quadratic extensions. Let d be an integer which isn't a square, and set $L = \mathbb{Q}(\sqrt{d})$.

(a) Let $\gamma = a + b\sqrt{d} \in \mathrm{L}$, with $a, b \in \mathbb{Q}$. Write out the 2×2 matrix for the map "multiplication by γ" and compute its determinant. I.e., compute $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma)$.

(b) $\mathrm{L}/\mathbb{Q}$ is a Galois extension of degree 2, with Galois group $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} = \mathrm{C}_2$. Let τ be the nontrivial element of G. How does τ act on L? (You don't have to prove your answer, we already did that in **H4** Q3, you just need to recall it for use below.)

(c) Given $\gamma = a + b\sqrt{d}$ as above, compute $\gamma \cdot \tau(\gamma)$, i.e., compute $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma)$ according to the alternate formula in Galois extensions.

For the rest of the question let us consider the case $d = 3$, and set $\gamma = 2 + \sqrt{3}$.

(d) Check that $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma) = 1$.

(e) Explain why $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma^n) = 1$ for all $n \geqslant 1$.

(f) Compute γ^2 and γ^3, and check directly that their norms are 1.

(g) Prove that the equation $x^2 - 3y^2 = 1$ has infinitely many solutions in positive integers x, y.

(h) Is there $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ such that $\gamma = (a + b\sqrt{3})/\tau(a + b\sqrt{3})$? (You don't have to find such a, b, but you do have to argue whether such a, b exist.)

3. Suppose that K is a field of characteristic zero, and that $f(x) \in K[x]$ is an irreducible polynomial of degree 4 with splitting field L. Further suppose that $G = \mathrm{Gal}(L/K) = A_4$. The purpose of this question is to write down all the intermediate fields of L/K, without having a concrete polynomial to work with. The idea is to demonstrate that the Galois group not only controls the "shape" of the diagram of intermediate fields (since this lattice is the reverse of the subgroup lattice), but that once the Galois group is fixed, there are "universal formulae" for these intermediate fields.

Let α_1, α_2, α_3, and α_4 be the four roots of f, and $\gamma_{12|34}$, $\gamma_{13|24}$, and $\gamma_{14|23}$ the three roots of the resolvent cubic g, as described in class.

(a) List and name the subgroups of A_4. You should have four subgroups of order 3, one subgroup of order 4, and three subgroups of order 2.

(By "name" I mean : if the subgroup has a well-known name that we've seen before, use that, if not give it your own name [e.g., "H_7"], whatever name you want, so that below when we match intermediate fields to subgroups you'll have a way to describe which subgroup, something better than "the third subgroup on the list from part (a)...".)

(b) Find the fixed fields associated to the subgroups of order 3 (this should be fairly easy).

(c) Find the fixed field of the subgroup of order 4.

(d) Explain why $K(\gamma_{12|34}) = K(\gamma_{13|24}) = K(\gamma_{14|23})$. (An indirect argument is best, and there is more than one possible such argument.)

(e) And now the challenge problem: find the fixed fields for the groups of order 2. Explain your answer, and your reasoning, as clearly as you can.