MATH5725: Galois Theory (2014, S2) Assignment 2

Due Date
This assignment is due at 5pm on Thursday 18 September.

Marks
The assignment is worth 20% of your total mark. It is marked out of 20.

Submission guidelines
You can submit the assignment by email to s.meagher@unsw.edu.au, or by giving me a hard copy, or by uploading to moodle.

Typed submissions are preferred, but if you do not have access to mathematical typesetting software (e.g. latex), or if you are not familiar with the use of such software, handwritten submissions are also acceptable.

Notes on references
If you use a theorem or a formula, you do not need to give a full reference if it is something mentioned in the lectures, but just a short reference will suffice.

Question 1
(12 Marks)
The point of this question is to show that it is (at least sometimes) possible to calculate a Galois group indirectly by deducing various facts about it in steps.
Let $f(X) = X^3 + 2X + 2 \in \mathbf{Q}[X]$.
(a) Let $a/b \in \mathbf{Q}$ with $a, b \in \mathbf{Z}$ and a and b coprime. Show that if $f(a/b) = 0$ then 2 divides a and b. Conclude that $f(X)$ has no root in $\mathbf{Q}$. (Hint: Multiply $f(a/b)$ by b^3 to show that $2 \mid a$. Then put $a = 2m$ to show that $2 \mid b$.)
(b) Show that if $f = gh$ then either g or h has degree 1. Conclude from (a) that f is irreducible.
(c) Show that as a function from $\mathbf{R}$ to $\mathbf{R}$ that f is strictly increasing. Deduce that f has exactly 1 real root.
Let $\beta_1, \beta_2, \beta_3 \in \mathbf{C}$ be the distinct roots of f, with β_1 the real root and β_2, β_3 the complex roots. Let $K = \mathbf{Q}(\beta_1, \beta_2, \beta_3)$. Then K is a splitting field for f and $K/\mathbf{Q}$ is Galois (you do not need to show this).
(d) Show that complex conjugation on $\mathbf{C}$ sends elements of K to K and swaps β_2 and β_3. Deduce that the Galois group $\mathrm{Aut}(K/\mathbf{Q})$ contains an element of order 2.
(e) By computing a basis of $\mathbf{Q}(\beta_1)$, show that $3 = [\mathbf{Q}(\beta_1) : \mathbf{Q}]$. Deduce that $3 \mid [K : \mathbf{Q}]$.
For the next part you may assume that if $\gamma \in K$ is a root of f and $\sigma \in \mathrm{Aut}(K/\mathbf{Q})$ then $\sigma(\gamma)$ is also a root of f. The notation S_3 is used to denote the symmetric group on 3 letters, which you may assume is a finite group of size 6.
(f) Use the fact that K is generated by β_1, β_2 and β_3 to show that there is an injection of groups $\mathrm{Aut}(K/\mathbf{Q}) \to S_3$. (Hint: For each $\sigma \in \mathrm{Aut}(K/\mathbf{Q})$ we have $\sigma(\beta_i) = \beta_{\tau_\sigma(i)}$. You need to show that $\sigma \mapsto \tau_\sigma$ is an injective group homomorphism).
(g) Use the fact that $[K : \mathbf{Q}] = |\mathrm{Aut}(K/\mathbf{Q})|$ to show that $3 \mid |\mathrm{Aut}(K/\mathbf{Q})|$. From (d) deduce that $2 \mid |\mathrm{Aut}(K/\mathbf{Q})|$. Conclude from (f) that $\mathrm{Aut}(K/\mathbf{Q}) \cong S_3$.

Question 2
(8 Marks)
Let $S_0 \subset \mathbf{R}^2$ be a finite subset with at least 2 elements. Recursively define new subsets S_n by the following method:
(1) A point $p \in \mathbf{R}^2$ is in $S_{n,1}$ if it is a point of intersection of two distinct lines l_1, l_2, where l_i is the unique line going through the distinct points $p_i, q_i \in S_{n-1}$.
(2) A point $p \in \mathbf{R}^2$ is in $S_{n,2}$ if it is a point of intersection of two distinct circles C_1, C_2 with centres $p_1, p_2 \in S_{n-1}$ and radii equal to a line segments joining any two pairs of points in S_{n-1}.
(3) A point $p \in \mathbf{R}^2$ is in $S_{n,3}$ if it is a point of intersection between a line segment joining any two distinct points of S_{n-1} circle C_1 with centre $p_1 \in S_{n-1}$ and radius equal to a line segment joint any two distinct points in S_{n-1}.
Let $S_n = S_{n,1} \bigcup S_{n,2} \bigcup S_{n,3}$.

The union of the S_n is called the set of points of the plane constructible by ruler and compass from S_0.

For each $n \geq 1$ let K_n be the field extension of K_{n-1} generated by the the coordinates of the points of S_n and the distances between points in S_n. Let K_0 be the field extension of $\mathbf{Q}$ generated by the co-ordinates of points in S_0 and the distances between points in S_0.

The union of the K_n is called the set of numbers constructible by ruler and compass from S_0.

(a) Show that if $n \geq 1$ then $K_n = K_{n-1}(\sqrt{a_1}, \cdots, \sqrt{a_t})$ for some $a_1, \cdots, a_t \in K_{n-1}$.

(b) Show that $[K_n : K_0] = 2^s$ for some integer $s \geq 1$.

(c) Show that if $S_0 = \{(0,0), (1,0)\}$ that there is no n such that K_n contains a solution of $X^3 - 2 = 0$.