Algebra I. Homework 9. Due on December, 4, 2020.

1. Let $K = \mathbb{Q}[\sqrt{2}]$ and $L = \mathbb{Q}[\sqrt{4+2\sqrt{2}}]$.
   (a) Show that $4+2\sqrt{2}$ is not a square in K.
   (b) Compute the degree $[L : \mathbb{Q}]$.
   (c) What is the minimal polynomial of $\sqrt{4+2\sqrt{2}}$ over $\mathbb{Q}$?
   (d) What is the minimal polynomial of $\sqrt{4+2\sqrt{2}}$ over K?
   (e) Show that $4-2\sqrt{2} \in L$. Deduce that $L/\mathbb{Q}$ is Galois.
   (f) Show that there is a unique element $g \in Gal(L/\mathbb{Q})$ such that $g(\sqrt{4+2\sqrt{2}}) = \sqrt{4-2\sqrt{2}}$.
   (g) What is the order of g?
   (h) Describe all the subfields of L.

2. Let k be a field and let $P \in k[x]$ be a polynomial of degree $n > 0$.
   (a) Show that if P is not irreducible, then P has a root in an extension of k of degree at most $n/2$.
   (b) Assume that $k = \mathbb{F}_p$ is the finite field with p elements. Show that P is irreducible if and only if P has no roots in $\mathbb{F}_{p^d}$ with $d \leq n/2$. Deduce that P is irreducible if and only if $(P, x^{p^d} - x) = 1 \quad \forall 1 \leq d \leq n/2$.

3. Let $P = x^5 - x + 3 \in \mathbb{Q}[x]$ and let G be the Galois group of P over $\mathbb{Q}$.
   (a) Show that P is separable. Deduce that G is isomorphic to a subgroup of S_5.
   (b) Let Q be the image of P under the reduction mod 3 map $\mathbb{Z}[x] \to \mathbb{F}_3[x]$. Factorize Q in $\mathbb{F}_3[x]$.
   (c) Let R be the image of P under the reduction mod 5 map $\mathbb{Z}[x] \to \mathbb{F}_5[x]$. Show that R is irreducible in $\mathbb{F}_5[x]$.
   (d) Show that G is isomorphic to S_5:
      - you can admit that a 5-cycle and a transposition generate S_5.
      - you can use the theorem announced in class: Let $P \in \mathbb{Z}[x]$ be a monic irreducible separable polynomial of degree n. Let p be a prime number and denote by $\bar{P}$ the image of P in $\mathbb{F}_p[x]$. Assume $\bar{P}$ is separable. Then $G = Gal(P, \mathbb{Q})$ has a subgroup isomorphic to $Gal(\bar{P}, \mathbb{F}_p)$. In particular, if $\bar{P}$ is irreducible, $G \subset S_n$ has a cycle of length n