Modern Algebra 2 – MA 542 – Spring 2019 – R. Pollack
HW #11

1. Let K denote the splitting field of $(x^2-5)(x^2-7)$ over $\mathbb{Q}$.
   (a) Compute $[K:\mathbb{Q}]$.
   (b) Write down generators of $\mathrm{Gal}(K/\mathbb{Q})$ and write down all elements of this group in terms of these generators.
   (c) Form a multiplication table for $\mathrm{Gal}(K/\mathbb{Q})$.
   (d) Which group is $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to?
   (e) Find all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$.
   (f) How many subfields are there between K and $\mathbb{Q}$ (inclusive)? What are their degrees?
   Extra credit: find these subfields explicitly and match them up with the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ via the Galois correspondence theorem.

2. Let K denote the splitting field of x^7-1 over $\mathbb{Q}$. Complete all parts of the previous question for this field K.

3. This question will lead you to a proof of the fact that all algebraic extensions of $\mathbb{Z}_p$ are separable.
   (a) Let $f(x)$ be a polynomial in $\mathbb{Z}_p[x]$. If $f'(x)=0$, prove that there is some polynomial $g(x)\in\mathbb{Z}_p[x]$ such that $f(x)=g(x)^p$.
   [Hint: First proof that if $f(x)=\sum_{i=0}^n c_i x^i$, then $c_i\neq 0$ iff i is a multiple of p. Then use the fact that $a^p=a$ for all $a\in\mathbb{Z}_p$ and the fact that $(a+b)^p=a^p+b^p$ in $\mathbb{Z}_p$.]
   (b) Let F be a field and let α be a root of $f(x)\in F[x]$ with multiplicity e. Show that α is a root of $f'(x)$ with multiplicity at least $e-1$. (We showed in class that the multiplicity was exactly $e-1$ if F has characteristic 0 — the same proof works here with the weaker conclusion.)
   (c) Prove that if $p(x)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, then $p(x)$ has no repeated roots.
   [Hint: If $p(x)$ has a repeated root, use part (b) to see that $p'(x)$ and $p(x)$ are not relatively prime. Since $p(x)$ is irreducible, this would force $p'(x)=0$. Now apply part (a) to deduce that $p(x)$ is not irreducible.]
   (d) Deduce that every algebraic extension of $\mathbb{Z}_p$ is separable.

4. (a) Let K be any finite field of characteristic p. Show that the map $\varphi(x)=x^p$ is an automorphism of K. (This is called the *Frobenius* automorphism.)
   (b) Let $K=\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ be a field with 4 elements. Show that $K/\mathbb{Z}_2$ is a Galois extension.
   [Hint: Show that K is the splitting field of x^3-1 over $\mathbb{Z}_2$.]
   (c) Show that $\mathrm{Gal}(K/\mathbb{Z}_2)$ is a cyclic group of size 2 generated by the Frobenius automorphism.