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

1. Let K denote the splitting field of $(x^2-5)(x^2-7)$ over $\mathbb{Q}$.

   (a) Compute $[K:\mathbb{Q}]$.

   Solution: We have $K=\mathbb{Q}(\sqrt{5},\sqrt{7})$. Clearly $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2$ as $x^2-5=\mathrm{irr}(\sqrt{5},\mathbb{Q})$. We now need to compute $[K:\mathbb{Q}(\sqrt{5})]$ and thus we need to compute $\mathrm{irr}(\sqrt{7},\mathbb{Q}(\sqrt{5}))$. We thus need to check that x^2-7 is irreducible over $\mathbb{Q}(\sqrt{5})$ for which it suffices to see that it has no roots in $\mathbb{Q}(\sqrt{5})$. To this end, assume $(a+b\sqrt{5})^2=7$. Then $a^2+5b^2+2ab\sqrt{5}=7$ and hence $a^2+5b^2=7$ and $2ab=0$. Thus $a=0$ or $b=0$. If $a=0$ then $5b^2=7$ which is not solvable in $\mathbb{Q}$, and if $b=0$ then $a^2=7$ which again is not solvable in $\mathbb{Q}$. Thus x^2-7 is irreducible over $\mathbb{Q}(\sqrt{5})$ which implies $[K:\mathbb{Q}(\sqrt{5})]=2$. Hence $[K:\mathbb{Q}]=[K:\mathbb{Q}(\sqrt{5})]\cdot[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2\cdot 2=4$.

   (b) Write down generators of $\mathrm{Gal}(K/\mathbb{Q})$ and write down all elements of this group in terms of these generators.

   Solution: Let ϕ be an element of $\mathrm{Gal}(K/\mathbb{Q})$. Then ϕ is determined by what it does to $\sqrt{5}$ and to $\sqrt{7}$. Moreover $\phi(\sqrt{5})\in\{\sqrt{5},-\sqrt{5}\}$ and $\phi(\sqrt{7})\in\{\sqrt{7},-\sqrt{7}\}$ as each element must be sent to a root of its minimal polynomial. We see then that the size of $\mathrm{Gal}(K/\mathbb{Q})$ is at most 4 and since this is a Galois extension the size is exactly $4=[K:\mathbb{Q}]$. Thus, everything possibility for ϕ works. To write down generators, let σ_5 be defined by $\sigma_5(\sqrt{5})=-\sqrt{5}$ and $\sigma_5(\sqrt{7})=\sqrt{7}$, and let σ_7 be defined by $\sigma_7(\sqrt{5})=\sqrt{5}$ and $\sigma_7(\sqrt{7})=-\sqrt{7}$. Note that $\sigma_5^2=\sigma_7^2=\mathbf{1}$ where $\mathbf{1}$ is the identity map and $\sigma_5\sigma_7=\sigma_7\sigma_5$. Then the elements of $\mathrm{Gal}(K/\mathbb{Q})$ are the $\mathbf{1}$, σ_5, σ_7 and $\sigma_5\sigma_7$.

   (c) Which group is $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to?

   Solution: This group is $C_2\times C_2$ as it has size 4 and every element has order 2.

   (d) Find all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$.

   Solution: The subgroups are $\{\mathbf{1}\}$, $\{\mathbf{1},\sigma_5\}$, $\{\mathbf{1},\sigma_7\}$, $\{\mathbf{1},\sigma_5\sigma_7\}$ and $\mathrm{Gal}(K/\mathbb{Q})$.

   (e) 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.

   Solution: Since there are 5 subgroups, there are 5 subfields. The degrees of these fields are 1, 2, 2, 2, and 4.

   Extra credit: The fixed field of $\{\mathbf{1}\}$ is K. The fixed field of $\{\mathbf{1},\sigma_5\}$ is $\mathbb{Q}(\sqrt{7})$. The fixed field of $\{\mathbf{1},\sigma_7\}$ is $\mathbb{Q}(\sqrt{5})$. The fixed field of $\{\mathbf{1},\sigma_5\sigma_7\}$ is $\mathbb{Q}(\sqrt{35})$. The fixed field of $\mathrm{Gal}(K/\mathbb{Q})$ is $\mathbb{Q}$.

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.

   (a) Compute $[K:\mathbb{Q}]$.

   Solution: We have $K=\mathbb{Q}(\zeta)$ where $\zeta=e^{2\pi i/7}$ as the roots of x^7-1 are all of the form $e^{2\pi ik/7}$ where $k=1,\dots,7$. We thus need to find the minimum polynomial of ζ. Note that $x^7-1=(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$ and since $\zeta\neq 1$ is a root of x^7-1 it must be a root of $f(x)=x^6+x^5+x^4+x^3+x^2+x+1$. To see that $f(x)$ is irreducible, we replace x by $x+1$ and get

$$\begin{aligned}f(x+1)&=\frac{(x+1)^7-1}{x+1-1}=\frac{x^7+\binom{7}{6}x^6+\binom{7}{5}x^5+\binom{7}{4}x^4+\binom{7}{3}x^3+\binom{7}{2}x^2+\binom{7}{1}x}{x}\\&=x^6+\binom{7}{6}x^5+\binom{7}{5}x^4+\binom{7}{4}x^3+\binom{7}{3}x^2+\binom{7}{2}x+\binom{7}{1}.\end{aligned}$$

Since $\binom{7}{i}$ is divisible by 7 for $i = 1, \ldots, 6$, we have that $f(x+1)$ is Eisenstein for $p = 7$ and thus irreducible. Thus, $f(x)$ is irreducible and $[K : \mathbb{Q}] = 6$. (This is the same trick we used for $p = 5$ earlier in the semester — it works for all primes.)

(b) Write down generators of $\mathrm{Gal}(K/\mathbb{Q})$ and write down all elements of this group in terms of these generators.

Solution: For $\phi \in \mathrm{Gal}(K/\mathbb{Q})$, we have that ϕ is uniquely determined by its value on ζ and moreover, $\phi(\zeta) \in \{\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\}$ as these are the roots of $f(x)$, the minimal polynomial of ζ. This gives 6 possible elements of $\mathrm{Gal}(K/\mathbb{Q})$ and thus they all work as $K/\mathbb{Q}$ is Galois with degree 6.
Define $\sigma(\zeta) = \zeta^3$. Then $\sigma^2(\zeta) = \zeta^9 = \zeta^2$, $\sigma^3(\zeta) = \sigma(\sigma^2(\zeta)) = \sigma(\zeta^2) = \zeta^6$, $\sigma^4(\zeta) = \sigma(\sigma^3(\zeta)) = \sigma(\zeta^6) = \zeta^{18} = \zeta^4$, $\sigma^5(\zeta) = \sigma(\sigma^4(\zeta)) = \sigma(\zeta^4) = \zeta^{12} = \zeta^5$, $\sigma^6(\zeta) = \sigma(\sigma^5(\zeta)) = \sigma(\zeta^5) = \zeta^{15} = \zeta$. Thus σ^6 is the identity and σ has order 6. Hence σ is a generator of this group.

(c) Which group is $\mathrm{Gal}(K/\mathbb{Q})$ isomorphic to?

Solution: $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group of size 6 generated by σ.

(d) Find all subgroups of $\mathrm{Gal}(K/\mathbb{Q})$.

Solution: The subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ are $\{\mathbf{1}\}$, $\{\mathbf{1}, \sigma^3\}$, $\{\mathbf{1}, \sigma^2, \sigma^4\}$ and all of $\mathrm{Gal}(K/\mathbb{Q})$.

(e) 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.

Solution: There are 4 subgroups and so there are 4 subfields. Their degrees are 1,2,3 and 6.

Extra credit: The fixed field of $\{\mathbf{1}\}$ is K. The fixed field of $\{\mathbf{1}, \sigma^3\}$ is $\mathbb{Q}(\zeta + \zeta^{-1})$. The fixed field of $\{\mathbf{1}, \sigma^2, \sigma^4\}$ is $\mathbb{Q}(\sqrt{-7})$ and the fixed field of $\mathrm{Gal}(K/\mathbb{Q})$ is $\mathbb{Q}$.

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 $\mathbb{Z}_p$.]

Solution: Let $f(x) = \sum_{i=0}^n c_i x^i$. Then $f'(x) = 0$ implies $ic_i = 0$ for all i. Thus if $i \neq 0$, we must have that $c_i = 0$. But $i = 0$ in $\mathbb{Z}_p$ iff i is a multiple of p. Thus

$$\begin{aligned} f(x) &= c_0 + c_p x^p + c_{2p} x^{2p} + \ldots \\ &= c_0^p + c_p^p x^p + c_{2p}^p x^{2p} + \ldots \\ &= (c_0 + c_p x + c_{2p} x^2 + \ldots)^p \end{aligned}$$

as desired. Here we are using the fact that $a^p = a \pmod{p}$.

(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.)

Solution: Write $f(x) = (x - \alpha)^e \cdot g(x)$ with $g(\alpha) \neq 0$. Then

$$f'(x) = e(x-\alpha)^{e-1} g(x) + (x-\alpha)^e g'(x) = (x-\alpha)^{e-1}(eg(x) + (x-\alpha)g'(x)).$$

and hence α has multiplicity at least $e - 1$.

(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.]

Solution: If $p(x)$ has a repeated root, then $p(x)$ and $p'(x)$ share a common factor by (b). But since $p(x)$ is irreducible and $\deg(p') < \deg(p)$, this is only possible if $p'(x) = 0$. But then by part (a), $p(x)$ is a p-th power and not irreducible.

(d) Deduce that every algebraic extension of $\mathbb{Z}_p$ is separable.

Solution: This is immediate from the previous part as all irreducible polynomials over $\mathbb{Z}_p$ have no repeated roots.

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.)

Solution: Since $(a + b)^p = a^p + b^p$ in characteristic p and $(ab)^p = a^p b^p$, φ is a homomorphism. It is clearly non-zero as $\varphi(1) = 1$. Thus, φ is injective (as non-zero maps between fields are always injective) and since K is finite, φ is automatically surjective. Thus, φ is an automophism.

(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 $y^3 - 1$ over $\mathbb{Z}_2$.]

Solution: The elements of K are given by the equivalence classes of 0, 1, x and $x + 1$. We claim that the 3 non-zero elements of K satisfy $y^3 - 1 = 0$. We have $1^3 = 1$. To compute x^3, note that $x^2 = x + 1$ in K and thus $x^3 = x^2 + x = 1$ in K. Finally, $(x + 1)^3 = x^3 + 1 = x + 1$. Hence, K is the splitting field of $y^3 - 1$ over $\mathbb{Z}_2$. By 3(d), $K/\mathbb{Z}_2$ is separable and thus is a Galois extension.

(c) Show that $\mathrm{Gal}(K/\mathbb{Z}_2)$ is a cyclic group of size 2 generated by the Frobenius automorphism.

Solution: Clearly $[K : \mathbb{Z}_2] = 2$ and thus $\mathrm{Gal}(K/\mathbb{Z}_2)$ has size 2. Since the Frobenius automorphism φ is in $\mathrm{Gal}(K/\mathbb{Z}_2)$ we just need to check that it is not the identity. But $\varphi(x) = x^2 = x + 1 \neq x$.