Homework 7

Kevin Guillen

MATH 202 — Algebra III — Spring 2021

Problem 14.7.4 Let $K = \mathbb{Q}(\sqrt[n]{a})$, where $a \in \mathbb{Q}$, $a > 0$ and suppose $[K : \mathbb{Q}] = n$ (i.e., $x^n - a$ is irreducible). Let E be any subfield of K and let $[E : \mathbb{Q}] = d$. Prove that $E = \mathbb{Q}(\sqrt[d]{a})$. [Consider $N_{K/E}(\sqrt[n]{a}) \in E$.]

Proof. First let $\delta = N_{K/E})\sqrt[n]{a} = \prod_{Gal(K/E)} \sigma(\sqrt[n]{a})$. For all $\sigma \in Gal(K/E)$ we have $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some root of unity ζ_σ, and therefore

$$\delta = \left(\prod_{Gal(K/E)} \zeta_\sigma \right) \sqrt[n]{a}^{\frac{n}{d}} = \left(\prod_{Gal(K/E)} \zeta_\sigma \right) \sqrt[d]{a}.$$

Since $\delta \in E \subseteq \mathbb{Q}(\sqrt[n]{a}) \subseteq \mathbb{R}$ and the only real roots of unity are ± 1 we have that $\delta = \pm \sqrt[d]{a}$. Therefore we have that $\mathbb{Q}(\sqrt[d]{a}) \subseteq E$ with $\sqrt[d]{a}$ of degree d over $\mathbb{Q}$. Thus $E = \mathbb{Q}(\sqrt[d]{a})$ as desired. □

Problem 14.7.5 Let K be as in the previous exercise. Prove that if n is odd then K has no nontrivial subfields which are Galois over $\mathbb{Q}$ and if n is even then the only nontrivial subfield of K which is Galois over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{a})$.

Proof. The minimal polynomial of $\sqrt[n]{a}$ is $x^n - a$, which has splitting field $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ for some primitive n^{th} root of unity ζ_n. For $n > 2$ we have $\mathbb{Q}(\sqrt[n]{a}) \neq \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$, so $\mathbb{Q}(\sqrt[n]{a})$ is Galois if and only if $n = 2$. Then by the previous exercise we have that K has a subfield E that is Galois only when n is even, in which case it is $\mathbb{Q}(\sqrt{a})$. □

Problem 14.7.6 Let L be the Galois closure of K in the previous two exercises (i.e., the splitting field of $n^n - a$). Prove that $[L : \mathbb{Q}] = n\varphi(n)$ or $\frac{1}{2}n\varphi(n)$. [Note that $\mathbb{Q}(\zeta_n) \cap K$ is a Galois extension of $\mathbb{Q}$.]

Proof. First we consider the splittinf field of $x^n - a$ which is just $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ where ζ_n is n^{th} primitive root of unity. We have then that,

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \mathbb{Q}] = \frac{[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[n]{a} \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}]} = \frac{n\varphi(n)}{[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}.$$

Using what we have seen in the previous exercise we have that if n is odd then $[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = n\varphi(n)$ or $[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \frac{1}{2}n\varphi(n)$ depending on if $\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{a})$. $\square$

Problem 14.7.8 Let p, q, and r be primes in $\mathbb{Z}$ with $q \neq r$. Let $\sqrt[p]{q}$ denote any root of $x^p - q$ and let $\sqrt[p]{r}$ denote any root of $x^p - r$. Prove that $\mathbb{Q}(\sqrt[p]{q}) \neq \mathbb{Q}(\sqrt[p]{r})$.

Proof. For this proof we can use the fact seen in exercise 7 part c, which in the context of this problem gives us that, $\mathbb{Q}(\sqrt[p]{q}) = \mathbb{Q}(\sqrt[p]{r})$ if and only if $k/l,\ m/n \in \mathbb{Q}$ with $i, j \in \mathbb{Z}$ such that

$$q = r^i \frac{k^p}{l^p} \qquad\qquad r = q^j \frac{m^p}{n^p}$$

Assuming though that k/l is in lowest terms we have that $l^p = r^i$ and $k^p = q$ which means that $p = 1$, but p is assumed to be prime in $\mathbb{Z}$, which is a contradiction! $\square$

Problem 14.7.9 (Artin-Schrier Extensions) Let F be a field of characteristic p and let K be a cyclic extension of F of degree p. Prove that $K = F(\alpha)$ where α is a root of the polynomial $x^p - x - a$ for some $a \in F$. [Note that $Tr_{K/F}(-1) = 0$ since F is characteristic p so that $-1 = \alpha - \sigma\alpha$ for some $\alpha \in K$ where σ is a generator of $Gal(K/F)$ by exercise 26 of section 2. Show that $a = \alpha^p - \alpha$ is an element of F.] Note that since F contains the p^{th} rot of unity (namely 1) that this completes the description of all cyclic extension of prime degree p over fields containing the p^{th} roots of unity in all characteristics.

Proof. Using the noted comment we have that $Tr_{K/F}(-1) = 0$, so there is some $\alpha \in K$ such that $\alpha - \sigma\alpha = -1$, therefore we have $\sigma\alpha = \alpha + 1$. Generalizing this we have that

$$\sigma^i \alpha = \alpha + i.$$

Because F is of characteristic p the elements $\sigma^i\alpha$ are distinct for $i = 0, \ldots, p-1$ and thus $[F(\alpha) : F] = p$ so $K = F(\alpha)$.

We have,

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha+1)^p - \alpha + 1 = \alpha^p - \alpha$$

so $\alpha^p - \alpha$ is in the fixed field of σ which is F. Let $a = \alpha^p - \alpha$ we have that α is a root of $x^p - x - a$ as desired. $\square$

Problem 14.7.12 Let L be the Galois closure of the finite extension of $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. For any prime p dividing the order of $\mathrm{Gal}(L/\mathbb{Q})$ prove there is a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$.

Proof. We have that p is prime dividing the order of $\mathrm{Gal}(L/\mathbb{Q})$. Then by Cauchy's theorem G has a subgroup H and through the fundamental theorem it corresponds to a subfield F' of L where $[L : F'] = p$. Suppose then that for all $\sigma \in G$ we have $\sigma(\alpha) \in F'$, then $F' = L$, which is a contradiction. So there must be a $\sigma \in G$ that satisfies $\sigma(\alpha) \notin F'$. Because p is prime and degree is multiplicative we have that $F'(\sigma(\alpha)) = L$. So if we set $F = \sigma^{-1}(F')$ we have $F(\alpha) = L$ and $[L : F] = p$ as desired. $\square$

Problem 14.7.13 Let F be subfield of the real numbers $\mathbb{R}$. let a be an element of F and let $K = F(\sqrt[n]{a})$ where $\sqrt[n]{a}$ denotes a real n^{th} root of a. Prove that if L is any Galois extension of F contained in K then $[L : F] \leqslant 2$.

Proof. Apply the arguments made in exercise 5, any Galois extension of F contained in K, as defined in the problem statement, is trivial if n is odd and if n is even the only non-trivial Galois extension will be $F(\sqrt{a})$. Thus the degree of any Galois extension of F contained in K is at most 2. $\square$

Problem 14.7.16 Let a be a nonzero rational number.

(a) Determine when the extension $\mathbb{Q}(\sqrt{ai})(i^2 = -1)$ is of degree 4 over $\mathbb{Q}$.

(b) When $K = \mathbb{Q}(\sqrt{ai})$ is of degree 4 over $\mathbb{Q}$ show that K is Galois over $\mathbb{Q}$ with the Klein 4-group as Galois group. In this case determine the quadratic extensions of $\mathbb{Q}$ contained in K.

(a) *Proof.* Note $\sqrt{ai} = \dfrac{\sqrt{2|a|}}{2} + \dfrac{\sqrt{2|a|}}{2}i$ is a root of,

$$x^4 + a^2 = \prod_{j=0}^{3}(x - i^j\sqrt{ai}).$$

This is an irreducible polynomial and is the minimal polynomial of $\sqrt{ai}$ if and only if $\sqrt{2|a|}$ is irrational. This is because if it is not,

$$(x - \sqrt{ai})(x + i\sqrt{ai}) = x^2 + \sqrt{2a} + a \in \mathbb{Q}[x]$$

divides $x^4 + a^2$. $\square$

(b) *Proof.* Using the same description of the roots above we have that the Galois group is generated by,

$$\sqrt{ai} \mapsto -\sqrt{ai} \qquad\qquad \sqrt{ai} \mapsto \overline{\sqrt{ai}}$$

which are both of order 2. Therefore the Galois group is the Klein 4-group, and by the observations made, the quadratic extension is $\mathbb{Q}(\sqrt{2a})$.

$\square$