

Math 200b Winter 2015 Homework 5

Due 3/13/2015

1. Let p be a prime. Let K be the splitting field of $f(x) = x^p - 3$ over $\mathbb{Q}$. Let ζ be any primitive p th root of 1 in $\mathbb{C}$, and let $\alpha = \sqrt[p]{3} \in \mathbb{C}$.

Show that $K = \mathbb{Q}(\zeta, \alpha)$ and that $[K : F] = p(p-1)$. Let $G = \text{Gal}(K/\mathbb{Q})$ be the Galois group. Show that G is isomorphic to the semidirect product $\mathbb{Z}_p \rtimes_{\phi} (\mathbb{Z}_p)^*$, where $\phi : (\mathbb{Z}_p)^* \rightarrow \text{Aut}(\mathbb{Z}_p)$ is the natural identification.

2. Let $F \subseteq K$ be a Galois extension and let $F \subseteq E \subseteq K$ and $F \subseteq L \subseteq K$ be intermediate fields. Show that there is an isomorphism $\theta : E \rightarrow L$ which restricts to the identity on F if and only if the subgroups $\text{Gal}(K/L)$ and $\text{Gal}(K/E)$ of $G = \text{Gal}(K/F)$ are conjugate subgroups in G .

3. (a). Suppose that K/F is a Galois extension with $[K : F] = p^n$ for some prime p and $n \geq 1$. Show that there are intermediate fields $F \subseteq E_1 \subseteq K$, $F \subseteq E_2 \subseteq K$ such that E_i/F is Galois for $i = 1, 2$ and $[E_1 : F] = p$, $[E_2 : F] = p^{n-1}$.

(b). Suppose that $f \in \mathbb{Q}[x]$ is irreducible of degree 4 over $\mathbb{Q}$, and that its splitting field K over $\mathbb{Q}$ satisfies $\text{Gal}(K/\mathbb{Q}) \cong S_4$. Show that there is a field $\mathbb{Q} \subseteq E \subseteq K$ such that $[E : \mathbb{Q}] = 4$ and there are no proper intermediate fields between $\mathbb{Q}$ and E .

4. Let $\pm\alpha, \pm\beta$ be the roots of the polynomial $f(x) = x^4 + ax^2 + b \in \mathbb{Z}[x]$.

(a). Prove that f is irreducible over $\mathbb{Q}$ if and only if $\alpha^2, \alpha + \beta, \alpha - \beta$ are not elements of $\mathbb{Q}$.

(b). Suppose that f is irreducible and let $G = \text{Gal}(K/\mathbb{Q})$ where K is the splitting field of f over $\mathbb{Q}$. Show that G is one of three possibilities, determined as follows:

1. $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ if and only if $\alpha\beta \in \mathbb{Q}$.

2. $G \cong \mathbb{Z}_4$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

3. $G \cong D_8$, the dihedral group of order 8, if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

(Hint: first show there are only 8 possible ways an element of G can permute the roots of f .)

(c). Give examples of polynomials f showing that each of the three cases in part (b) can occur.

5. Recall that for any field F of characteristic p , any irreducible polynomial $f \in F[x]$ is of the form $g(x^{p^k})$ for some irreducible, separable polynomial $g \in F[x]$ (Prop. 38 in the text). Recall also that an algebraic extension $F \subseteq K$ is called *purely inseparable* if for all $\alpha \in K \setminus F$, $\text{minpoly}_F(\alpha)$ is an inseparable polynomial.

(a). Suppose that $\text{char } F = p > 0$. Prove that $F \subseteq K$ is purely inseparable if and only if every $\alpha \in K$ satisfies $\alpha^{p^k} \in F$ for some $k \geq 0$.

(b). Every field F of characteristic p which is not perfect has some purely inseparable extension $F \subsetneq K$.

6. Let $F \subseteq K$ be an algebraic extension, not necessarily of finite degree.

(a). Let E be the set of elements $\alpha \in K$ such that α is separable over F . Show that E is a subfield of K containing F . (Hint: Show for any $\alpha, \beta \in E$ that $F \subseteq F(\alpha, \beta)$ is a separable extension. To do this, construct a Galois extension of F containing α and β .)

(b). With the same notation as in (a), show that K/E is purely inseparable. Thus any algebraic extension decomposes into a separable extension followed by a purely inseparable extension.

(c). Suppose that $F \subseteq L \subseteq K$ where K/F is an algebraic extension. Show that K/F is separable if and only if L/F and K/L are separable.

7. Let $q = p^m$ be a power of the prime p . Let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Let $\sigma_q : \mathbb{F}_q \rightarrow \mathbb{F}_q$ be the defined by $\sigma(a) = a^q$ for all $a \in \mathbb{F}_q$. This is the m th power of the Frobenius automorphism, so it is also an automorphism.

(a). Prove that every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, hence is unique up to isomorphism.

(b). Prove that if K is an extension of $\mathbb{F}_q$ with $[K : \mathbb{F}_q] = n$, then $\text{Gal}(K/\mathbb{F}_q)$ is cyclic with σ_q as a generator.

(c). With K as in (b), prove that the intermediate fields $\mathbb{F}_q \subseteq E \subseteq K$ are exactly the subfields $E_d = \{a \in K \mid a^{q^d} = a\}$ as d varies over the divisors of n .

8. Let $\zeta \in \mathbb{C}$ be a primitive p th root of 1 for some prime $p > 2$. Let $K = \mathbb{Q}(\zeta)$ be the splitting field of $x^p - 1$ inside $\mathbb{C}$.

(a). Let $\alpha = \sum_{i=0}^{p-1} \zeta^{i^2}$. This is called a *Gauss sum*. Prove that $E = \mathbb{Q}(\alpha)$ is the unique subfield of K such that $[E : \mathbb{Q}] = 2$.

(b). Show that $L = \mathbb{Q}(\zeta + \zeta^{-1})$ is the unique subfield of K such that $[K : L] = 2$. Show that in fact $L = K \cap \mathbb{R}$. (Hint: note that complex conjugation restricts to an automorphism of K).

Additional problems, not to be handed in:

Here are some more interesting problems, which do not need to be written up as part of the assignment.

A. Let $p_1, \dots, p_n$ be different prime numbers and let $E = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ as a subfield of $\mathbb{R}$.

(a). Show that $E/\mathbb{Q}$ is Galois and that $\text{Gal}(E/\mathbb{Q})$ is elementary Abelian of order 2^n . (Hint: Show that the fields $\mathbb{Q}(\sqrt{k})$ are all different as k runs over the $2^n - 1$ different products of distinct members of the set $\{p_1, \dots, p_n\}$.)

(b). Show that $E = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{p_1} + \sqrt{p_2} + \dots + \sqrt{p_n}$. (Hint: determine how the 2^n elements of the Galois group G act on the elements $\sqrt{p_1}, \dots, \sqrt{p_n}$. Then show that the orbit of α under G contains 2^n different elements.)

B. Let K be the splitting field of $f(x) = x^p - x - a$ over $\mathbb{F}_p$, where p is a prime and $0 \neq a \in \mathbb{F}_p$. Show that $G = \text{Gal}(K/\mathbb{F}_p)$ is cyclic. (Hint: Show that if α is a root of f in K then the roots of f are $\{\alpha + i \mid i \in \mathbb{Z}_p\}$.)

C. let p be a prime, $q = p^m$ for some m , and let $\mathbb{F}_q$ be the finite field of order q . Let $\sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q$ be the Frobenius automorphism $a \mapsto a^p$. View $\mathbb{F}_q$ as a vector space of dimension m over its prime subfield $\mathbb{F}_p$.

(a). Show that the minimal and characteristic polynomials of σ are both $x^m - 1$. (Hint: note that the powers $\{\sigma^i \mid 0 \leq i \leq m - 1\}$ are distinct and use the result on the linear independence of characters).

(b). Determine the rational canonical form of σ . Prove that σ is diagonalizable over $\mathbb{F}_p$ if and only if m divides $p - 1$.

(c). Determine the Jordan form of σ over an algebraic closure $\overline{\mathbb{F}_p}$. Prove that σ is diagonalizable over $\overline{\mathbb{F}_p}$ if and only if $\gcd(m, p) = 1$.

D. Let $K = \mathbb{F}_p(x, y)$ be rational functions in two variables over the field $\mathbb{F}_p$ of p elements. Let $F = \mathbb{F}_p(x^p, y^p)$.

(a). Show that K/F is purely inseparable, and that $[K : F] = p^2$.

(b). Show that there are infinitely many intermediate subfields between F and K .