Math 412 Final exam review questions

Paul Hacking

April 23, 2013

All fields are assumed to have characteristic 0.

(1) Let $K \subset L$ be a field extension. (That is, K and L are fields, and K is a subring of L.) Define the degree $[L : K]$ of the field extension $K \subset L$ Compute the degrees of the following field extensions.

(a) $K \subset K(\alpha)$, where $\alpha \in L$ for some field extension $K \subset L$, and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ is the irreducible polynomial of α over K.

(b) $K \subset L$, where there is an intermediate field $K \subset M \subset L$ such that $K \subset M$ has degree d and $M \subset L$ has degree e.

(c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{p})$ where $n \in \mathbb{N}$ and p is prime.

(d) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ and p is prime.

(e) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/4}$.

(f) $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/8}$.

(g) $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{5})$.

(h) $\mathbb{Q} \subset \mathbb{Q}(\alpha, \beta)$, where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 + 3x + 1$ and $\beta \in \mathbb{C}$ is a root of $g(x) = x^4 + 4x + 2$.

(i) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where $p, q \in \mathbb{N}$ are primes and $p \neq q$.

(2) Let K be a field and $f(x) \in K[x]$ a polynomial of degree $n \in \mathbb{N}$. What is the *splitting field* L for $f(x)$ over K? Describe the splitting field of the following polynomials over $\mathbb{Q}$ as simply as possible.

(a) $x^2 + 3x + 1$.

(b) $x^4 - 2x^2 - 3$.

(c) $x^4 - 5x^2 + 3$.

(d) $x^6 - 1$.

(e) $x^7 - 2$.

(f) $x^n - 1$, $n \in \mathbb{N}$.

(g) $x^n - a$, $n \in \mathbb{N}$, $a \in \mathbb{Q}$, $a > 0$.

(3) Let K be a field and $f(x) \in K[x]$ an irreducible monic polynomial of degree 2. Let L be a splitting field for $f(x)$ over K. So $f(x) = (x - \alpha_1)(x - \alpha_2)$ for some $\alpha_1, \alpha_2 \in L$, and $L = K(\alpha_1, \alpha_2)$.

(a) Explain why there is an isomorphism $\varphi \colon L \to L$ such that $\varphi(\alpha_1) = \alpha_2$ and $\varphi(a) = a$ for all $a \in K$.

(b) Use the quadratic formula to show that $L = K(\sqrt{d})$ for some $d \in K$.

(c) Use part (b) to give another description of the automorphism φ from part (a).

[Hint: (a) We have the following general result: If K is a field, $f(x) \in K[x]$ is an irreducible polynomial, $K \subset L$ is a field extension, and $\alpha, \beta \in L$ are roots of $f(x)$, then there is an isomorphism $\varphi \colon K(\alpha) \to K(\beta)$ given by $\varphi(\alpha) = \beta$ and $\varphi(a) = a$ for all $a \in K$.]

(4) Let $K \subset L$ be a field extension. Define the Galois group $G(L/K)$ of the field extension. What does it mean to say that the extension $K \subset L$ is a Galois extension? Compute the Galois groups of the following field extensions and determine whether the extension is Galois.

(a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3})$.

(b) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7})$.

(c) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{5})$.

(d) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(e) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/3}$.

(f) $K \subset L$ where $[L : K] = 2$.

(g) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{p})$ where p is prime and $n \in \mathbb{N}$ is odd.

(h) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{p})$ where p is prime and $n \in \mathbb{N}$ is even.

(i) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$.

[Hint: Recall that if $L = K(\alpha_1, \ldots, \alpha_n)$ and $\varphi\colon L \to L$ is an isomorphism such that $\varphi(a) = a$ for all $a \in K$, then (i) φ is determined by $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$, and (ii) if $\alpha \in L$ satisfies $f(\alpha) = 0$ for some $f(x) \in K[x]$, then also $f(\varphi(\alpha)) = 0$. See also the general result stated in the hint for Q3(a).]

(5) Let L be a field and H a finite group of automorphisms of L. Define the fixed field L^H. What is the degree $[L : L^H]$? Compute the fixed field explicitly in the following cases.

(a) $L = \mathbb{Q}(\sqrt{2})$, $H = \langle \varphi \rangle = \{e, \varphi\}$, where $\varphi(\sqrt{2}) = -\sqrt{2}$ and $\varphi(a) = a$ for all $a \in \mathbb{Q}$.

(b) $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ and $H = \langle \varphi \rangle = \{e, \varphi\}$ where $\varphi(\sqrt{3}) = -\sqrt{3}$, $\varphi(\sqrt{5}) = -\sqrt{5}$, and $\varphi(a) = a$ for all $a \in \mathbb{Q}$.

(c) L is the splitting field of the polynomial $f(x) = x^3 - 5$ over $\mathbb{Q}$ and $H = \langle \varphi \rangle = \{e, \varphi\}$ where $\varphi\colon L \to L$ is given by complex conjugation.

(d) L is the splitting field of $f(x) = x^4 - 2$ over $\mathbb{Q}$ and $H = \langle \varphi \rangle = \{e, \varphi, \varphi^2, \varphi^3\}$ where $\varphi\colon L \to L$ is the isomorphism given by $\varphi(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\varphi(i\sqrt[4]{2}) = -\sqrt[4]{2}$, and $\varphi(a) = a$ for all $a \in \mathbb{Q}$.

[Hint: To compute the fixed field explicitly, write down a basis of L as a vector space over $\mathbb{Q}$ and describe φ in terms of the basis. (Choose the basis carefully so that the computation of the fixed field is as simple as possible.) Alternatively, it is possible to give an indirect argument using the formula for the degree of the fixed field.]

(6) Let K be a field, $f(x) \in K[x]$ a monic polynomial of degree n, and L the splitting field of f over K. So

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

for some $\alpha_1, \ldots, \alpha_n \in L$, and $L = K(\alpha_1, \ldots, \alpha_n)$ is the field generated by $\alpha_1, \ldots, \alpha_n$ over K. Assume that f has no repeated roots in L, that is, $\alpha_i \neq \alpha_j$ for all $i \neq j$.

(a) What is the order $|G(L/K)|$ of the Galois group $G(L/K)$ of the extension $K \subset L$? Is the extension $K \subset L$ Galois?

(b) Explain how to define an injective group homomorphism

$$\theta \colon G(L/K) \to S_n$$

from the Galois group $G(L/K)$ of the extension $K \subset L$ to the symmetric group S_n on n letters.

(c) Show by example that the homomorphism θ is not necessarily surjective.

(7) In each of the following cases, identify the Galois group of the splitting field L of the given polynomial over $\mathbb{Q}$ with a subgroup of the symmetric group S_n (where n denotes the degree of the polynomial) using the homomorphism θ of Q6(b).

(a) $x^2 - 4x + 13$.

(b) $x^4 + x^2 - 6$.

(c) $x^3 + x + 1$.

(d) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

[Hint: (c) Show that the polynomial $f(x) = x^3+x+1$ is irreducible and has exactly one real root (by considering the derivative $f'(x)$). Deduce that $[L : \mathbb{Q}] = 6$ and use this to determine the Galois group.]

(8) In each of the following cases, for the given Galois extension $\mathbb{Q} \subset L$ and element $\alpha \in L$, compute the orbit of α under the Galois group $G(L/\mathbb{Q})$ and use it to determine the irreducible polynomial of α over $\mathbb{Q}$.

(a) $L = \mathbb{Q}(\sqrt{2})$, $\alpha = 3 + 4\sqrt{2}$.

(b) $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\alpha = \sqrt{3} + \sqrt{5} \in L$.

(c) $L = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/5}$, $\alpha = \zeta + \zeta^{-1} \in L$.

(9) State the main theorem of Galois theory. For each of the following Galois extensions, find the Galois group and describe the correspondence of the main theorem explicitly.

(a) $K \subset L$, $[L : K] = 2$.

(b) $K \subset L = K(\sqrt{d}, \sqrt{e})$, where $d, e \in K$ and $[L : K] = 4$.

(c) $\mathbb{Q} \subset L$, where L is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

(d) $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\sqrt[3]{5}, \zeta)$, where $\zeta = e^{2\pi i/3}$.

(e) $\mathbb{Q} \subset L$, where L is the splitting field of $x^8 - 1$.

(f) $\mathbb{Q} \subset L$, where L is the splitting field over $\mathbb{Q}$ of an irreducible cubic polynomial $f(x) \in \mathbb{Q}[x]$ and $[L : \mathbb{Q}] = 6$.

(g) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/5}$.

(h) $\mathbb{Q} \subset \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/7}$.

(10) Consider the Galois extension $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, where $\zeta = e^{2\pi i/3}$. Show that the element $\gamma = \sqrt[3]{2} + \zeta \in L$ satisfies $L = \mathbb{Q}(\gamma)$.

[Hint: List the intermediate fields M and verify that $\gamma \notin M$ for $M \neq L$. Use the basis $1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{2}^2$ for L as a vector space over $\mathbb{Q}$ and the relation $\zeta^2 = -1 - \zeta$ to express a basis for each intermediate field M in terms of this basis.]

(11) Prove that the polynomial $f(x) = x^5 + 5x + 1$ has no repeated roots in $\mathbb{C}$.

[Hint: Recall that a polynomial $f(x) \in K[x]$ has no repeated roots in its splitting field if and only if $\gcd(f, f') = 1$ where f' denotes the derivative of f.]

(12) Let $K \subset L$ be a field extension such that the degree $[L : K]$ is finite. Let $G = G(L/K)$ denote the Galois group of $K \subset L$. Prove that the extension $K \subset L$ is Galois if and only if the fixed field $L^G = K$.

(13) Let K be a field and $f(x) \in K[x]$ a polynomial of degree n. Let L be the splitting field of $f(x)$ over K, so $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in L$ and $L = K(\alpha_1, \ldots, \alpha_n)$.

(a) Show that $[L : K] \leq n!$.

(b) Show that we have equality in (a) if and only if the Galois group $G(L/K)$ is isomorphic to the symmetric group S_n on n letters.

(14) (Optional) Let $f(x) \in K[x]$ be a monic polynomial. Let L be the splitting field of L over K, so that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in L$ and $L = K(\alpha_1, \ldots, \alpha_n)$. Assume that $\alpha_i \neq \alpha_j$ for all $i \neq j$. Consider the element

$$\delta := \prod_{i<j} (\alpha_i - \alpha_j) \in L$$

(a) Show that, for $\tau \in S_n$ a transposition,

$$\prod_{i<j} (\alpha_{\tau(i)} - \alpha_{\tau(j)}) = -\delta.$$

(b) Deduce that, for $\sigma \in S_n$ a permutation,

$$\prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \begin{cases} +\delta & \text{if } \sigma \text{ is even,} \\ -\delta & \text{if } \sigma \text{ is odd.} \end{cases}$$

(c) Using part (b) and Q12 show that (i) $\delta^2 \in K$, and (ii) $\delta \in K$ if and only if the image of the homomorphism $\theta \colon G(L/K) \to S_n$ of Q6(b) is contained in the alternating group A_n (that is, the elements φ of the Galois group induce even permutations of the roots of f).