

Mathematics 100C Exam 2 Practice Problems

Instructions: Exam 2 is Friday May 19. It will be an in class exam, 50 minutes long. No notes or calculators are allowed. This practice worksheet is to help you study for Exam 2. Anything discussed up to and including the material in lecture on Friday May 12 is fair game for the exam. Note that inclusion of a topic on this sheet does not guarantee that a similar problem will appear on the exam, nor does exclusion of a topic from this sheet imply that that topic will not be on the exam.

1. Write down the statements of:
 - (a) The theorem that says when splitting fields contain all the roots of an irreducible polynomial.
 - (b) The two main theorems of Galois theory, including the part about normal subgroups of the Galois group of a finite extension.
 - (c) The theorem that computes the Galois group of $\mathbf{Q}(\mu_n)$ over $\mathbf{Q}$. (This was done on the Exam 1 practice worksheet. You should know the result, although you do not need to know the proof.)
 - (d) The main theorems from Kummer theory.
 - (e) The two theorems we proved for the Galois groups of composite extensions.
 - (f) The result that computes the irreducible polynomial of an algebraic element in terms of its Galois orbit.
2. Suppose F has characteristic 0, and K/F is a finite abelian extension, i.e., K/F is Galois with Galois group that is abelian. Observe that, in this case, every intermediate field extension $F \subseteq L \subseteq K$ is Galois over F . Now use this to prove that if p is prime, and $n > 2$ is an integer, then $p^{1/n}$ is not contained in $\mathbf{Q}(\mu_N)$ for any positive integer N . (By the way, it is a fact that if $p \equiv 1 \pmod{4}$, then $p^{1/2} \in \mathbf{Q}(\mu_p)$, so the condition $n > 2$ is necessary.)
3. Suppose p, q are distinct primes, and let $F = \mathbf{Q}(\mu_{pq})$. Suppose K_1 is a Galois extension of F of degree p inside $\mathbf{C}$ and K_2 is a Galois extension of F of degree q , again inside $\mathbf{C}$. Let L be the compositum of K_1 and K_2 in $\mathbf{C}$. Prove that there exists $v \in F^\times$ so that $K_1 = F(v^{1/p})$ and $K_2 = F(v^{1/q})$.
4. Let p and q be two prime numbers. Let K be the splitting field over $\mathbf{Q}$ of $f(x) = x^p - q$, and set $G = \text{Gal}(K/\mathbf{Q})$. Prove that $G \simeq C_p \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$, where C_p denotes the cyclic group of order p .
5. Suppose $a > 0$ is a rational number, and $x^n - a$ is irreducible in $\mathbf{Q}[x]$, so that $K = \mathbf{Q}(a^{1/n})$ has degree n over $\mathbf{Q}$. Suppose $E \subseteq K$ is a subfield, with $[E : \mathbf{Q}] = d$ (so $d|n$).
 - (a) Prove that $\mathbf{Q}(a^{1/d})$ has degree d over $\mathbf{Q}$.
 - (b) Prove that $N_{K/E}(a^{1/n}) = \pm a^{1/d}$.
 - (c) Deduce that $E = \mathbf{Q}(a^{1/d})$.
 - (d) Let $L = \mathbf{Q}(a^{1/n}, \mu_n)$ be the splitting field of $x^n - a$ over $\mathbf{Q}$. Suppose n is odd. Prove that $L/\mathbf{Q}$ has degree $n\varphi(n)$, and in fact, that $\text{Gal}(L/\mathbf{Q}) \simeq C_n \rtimes (\mathbf{Z}/n\mathbf{Z})^\times$.

6. Give an example of Galois extensions K/F and L/K so that L/F is not Galois.
7. Suppose $f(x) \in \mathbf{Q}[x]$ is a cubic irreducible polynomial, with one real root. Prove that the Galois group of $f(x)$ is the symmetric group S_3 .
8. Suppose F is a field of characteristic 0 that contains μ_n . Suppose $L = F(v^{1/n})$ for some $v \in F^\times$, and that L/F has degree n .
 - (a) Prove that the order of v in $F^\times/(F^\times)^n$ is n .
 - (b) Deduce that $\Delta(L/F) \subseteq F^\times/(F^\times)^n$ is the group generated by the class of v . **Note:** This is very similar to, but not exactly the same as, something we proved in class.
9. Let p, q, r be primes, with $q \neq r$. Prove that $\mathbf{Q}(q^{1/p}) \neq \mathbf{Q}(r^{1/p})$. Here is one way to proceed:
 - (a) Let $F = \mathbf{Q}(\mu_p)$, $L_1 = F(q^{1/p})$ and $L_2 = F(r^{1/p})$.
 - (b) If $\mathbf{Q}(q^{1/p}) = \mathbf{Q}(r^{1/p})$, then $L_1 = L_2$, and thus $\Delta(L_1/F) = \Delta(L_2/F)$.
 - (c) Using the previous problem, show that $\Delta(L_1/F) = \langle q \rangle$ and $\Delta(L_2/F) = \langle r \rangle$.
 - (d) If $q = r^m v^p$ for some integer $m = 1, 2, 3, \dots, p-1$ and $v \in F^\times$, take norms down to $\mathbf{Q}$ and get a contradiction.
10. Let $\mathbf{Q}(\alpha)$ be a finite extension of $\mathbf{Q}$, and L its Galois closure (in $\mathbf{C}$, say). Set $G = \text{Gal}(L/\mathbf{Q})$, and suppose p is a prime dividing the order of G . Prove that there exists a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$. **Hint:** Use the fact from finite group theory that G contains a subgroup H of order exactly p , let $H_1 = H, H_2, \dots, H_n$ be the conjugates of H in G , and set $F_j = L^{H_j}$. Observe that $[L : F_j] = p$. If $L \neq F_j(\alpha)$, then $\alpha \in F_j$. If this occurs for all j , then $\alpha \in \cap_j F_j$. But this intersection is Galois over $\mathbf{Q}$...
11. Determine the Galois group of $(x^3 - 2)(x^3 - 3) \in \mathbf{Q}[x]$.
12. Let K denote the splitting field of $(x^3 - 2)(x^3 - 2)$ over $\mathbf{Q}$. What are all the subfields of K that contain $\mathbf{Q}(\mu_3)$?
13. Suppose $v \in \mathbf{Q}(\mu_3) =: F$ is nonzero and is such that the complex conjugate $\bar{v}$ is equivalent to v^2 modulo $(F^\times)^3$, in other words, that $N(v) = v\bar{v} \equiv 1 \pmod{(F^\times)^3}$.
 - (a) Set $L = F(v^{1/3})$ as a subfield of $\mathbf{C}$. Prove that L is Galois over $\mathbf{Q}$.
 - (b) Prove that the Galois group $\text{Gal}(L/\mathbf{Q})$ is isomorphic to $C_3 \times C_2$.
 - (c) Let $K = L \cap \mathbf{R}$. Prove that K is Galois over $\mathbf{Q}$ with Galois group C_3 .
 - (d) Check that, for example, $v = 7(2 + \sqrt{-3})$ satisfies $N(v) \equiv 1 \pmod{(F^\times)^3}$.
14. Conversely, suppose $K/\mathbf{Q}$ is Galois extension with Galois group C_3 , with $K \subseteq \mathbf{C}$.
 - (a) First check that $K \subseteq \mathbf{R}$. (See question 7.)
 - (b) Let $F = \mathbf{Q}(\mu_3)$ and $L = K \cdot F = K(\mu_3)$. Confirm that L is Galois over $\mathbf{Q}$ with Galois group $C_2 \times C_3$, that L/F is Galois with group C_3 , and that L/K is Galois with group C_2 , generated by complex conjugation.
 - (c) Deduce that $L = F(v^{1/3})$ for some $v \in F^\times$. Check that we must have $\bar{v} \equiv v^2$ modulo $(F^\times)^3$.

15. Suppose F is a field of characteristic 0, and $K_1, \dots, K_n$ are finite Galois extensions of F in some large field E . Let the respective Galois groups be $G_1, \dots, G_n$. Set L to be the compositum of the K_j in E , i.e., the smallest subfield of E containing each of the K_j .
- (a) Prove that L is the set of finite sums of products of the form $x_1 \cdots x_n$, where $x_j \in K_j$.
 - (b) Prove that L is Galois over F , and $\text{Gal}(L/F)$ is isomorphic to a subgroup of $G_1 \times \cdots \times G_n$. (We did the case $n = 2$ in class.)
 - (c) Deduce that if all G_j are abelian, then $\text{Gal}(L/F)$ is again abelian.
16. Let ζ_n denote a primitive n^{th} root of unity, set $K = \mathbf{Q}(\zeta_n)$ as a subfield of $\mathbf{C}$, and let $K^+ = K \cap \mathbf{R}$. Prove that $K^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$. **Hint:** The element ζ_n satisfies a quadratic equation over $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$, so $[K : \mathbf{Q}(\zeta_n + \zeta_n^{-1})] = 2$.
17. Suppose F is a field of characteristic 0, and K a finite extension of F contained in some extension M/F that is Galois. Let L be the Galois closure of K in M . Prove that L is the compositum of the fields $\sigma(K)$ for $\sigma \in \text{Gal}(M/F)$.
18. Suppose F is a field of characteristic 0, $a, b \in F$, $K_0 = F(\sqrt{b})$ is a quadratic extension of F , and $K = F(\sqrt{a + \sqrt{b}})$ is a quadratic extension of K_0 . That is, we are assuming
- $b \in F^\times$, but not in $(F^\times)^2$
 - $a + \sqrt{b} \in K_0^\times$ but not in $(K_0^\times)^2$.

Let M be some Galois extension of F containing K . Define $K' = F(\sqrt{a - \sqrt{b}})$, and let L be the Galois closure of K in M . Observe that $K' \subseteq M$, and verify that L is the compositum of K and K' . Suppose now that $K \neq K'$. Let $H = \text{Gal}(L/K_0)$ and $T = \text{Gal}(L/F)$. Then H is isomorphic to $C_2 \times C_2$, the Klein 4 group, $T/H \simeq C_2$, and the induced action of C_2 on H is switching the factors. The only group with this structure is the dihedral group D_8 of order 8, so deduce that $T \simeq D_8$.

19. Let the notation be as in the previous problem, and again assume that $K \neq K'$. Let $\alpha = \sqrt{a + \sqrt{b}}$, $\alpha' = \sqrt{a - \sqrt{b}}$, and $f(x) = (x - \alpha)(x + \alpha)(x - \alpha')(x + \alpha')$.
- (a) The polynomial $f(x)$ above is $f(x) = (x^2 - a)^2 - b$. Prove that $f(x) \in F[x]$ is irreducible. **Hint:** In the notation of the previous problem, simply observe that T permutes the roots of $f(x)$ transitively.
 - (b) Suppose $F = \mathbf{Q}$ and $a^2 < b$. Check that $K \neq K'$ in this case, and so all the above facts apply.
 - (c) In fact, check that if $b \notin (F^\times)^2$, and $a + \sqrt{b} \notin (K_0^\times)^2$, then $f(x) = (x^2 - a)^2 - b$ is irreducible, even if $K = K'$. **Hint:** Prove that $\sqrt{a + \sqrt{b}}$ is primitive for K/F .
 - (d) Suppose again that $F = \mathbf{Q}$, and $a = 2 = b$. Prove that, in this case $K = K'$, so $L = \mathbf{Q}(\sqrt{2 + \sqrt{2}})$ is Galois over $\mathbf{Q}$. In this case, it turns out that $\text{Gal}(L/\mathbf{Q}) \simeq C_4$; see Example 16.9.2(b) in the text.
20. Generalize the results of questions 13 and 14 to C_p extensions of $\mathbf{Q}$, where p is a prime number.