

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.

Proof. Suppose F is a field of characteristic 0, $p(x) \in F[x]$ is irreducible, K, K_1, K_2 are Galois extensions of F , and F' is an extension field of F , and E is a splitting field over F . We assume that all these fields are contained in one larger field M , so that we can talk about intersections and compositums.

- (a) If $p(x)$ contains one root in E , then $p(x)$ splits in E .
- (b) The maps $V \mapsto \text{Aut}(K/V)$ and $H \mapsto K^H$ define inverse bijections between intermediate fields V between F and K , and subgroups H of $\text{Aut}(K/F)$. This bijection is inclusion reversing. In it, V is Galois over F if and only if H is normal in $\text{Aut}(K/F)$.
- (c) The Galois group of $\mathbf{Q}(\mu_n)$ over $\mathbf{Q}$ is identified with $(\mathbf{Z}/n)^\times$. The class of $[a]$ takes $\zeta \mapsto \zeta^a$, if $\zeta \in \mu_n$.
- (d) If F contains μ_n , then:
 - i. There is a bijection between finite subgroups Δ of $F^\times/(F^\times)^n$ and finite Galois extensions L/F that are abelian of exponent n . In this bijection, $L \mapsto \Delta(L/F) = ((L^\times)^n \cap F^\times)/(F^\times)^n$ and $\Delta \mapsto F(t^{1/n} : t \in \Delta)$, and these are inverse maps.
 - ii. In the above bijection, the pairing $\text{Gal}(L/F) \times \Delta \rightarrow \mu_n$ given by $(g, [t]) \mapsto g(t^{1/n})/t^{1/n}$ identifies $\text{Gal}(L/F)$ with $\widehat{\Delta}$ and Δ with $\widehat{\text{Gal}(L/F)}$.
 - iii. In particular, if L/F is cyclic of degree n , then there exists $v \in F^\times$ so that $L = F(v^{1/n})$ and v generates a group of order n in $F^\times/(F^\times)^n$.
- (e) Going back to the general case.

- i. Let L be the compositum of K and F' . Then L is Galois over F' , and the restriction map defines an isomorphism $\text{Aut}(L/F') \simeq \text{Aut}(K/K \cap F')$.
 - ii. Let now L be the compositum of K_1 and K_2 . Then L is Galois over F , and the restriction map defines an isomorphism $\text{Gal}(L/F) \simeq H$, where H is the subgroup of $\text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$ consisting of pairs (σ, τ) that have the same restriction to $K_1 \cap K_2$.
- (f) If $\gamma \in K$, then the irreducible polynomial for γ is given as $f(x) = \prod_{\gamma_j} (x - \gamma_j)$, where the γ_j are the elements of $\text{Gal}(K/F)$ -orbit of γ .

□

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.)

Proof. Every intermediate extension is Galois over F , because every subgroup of an abelian group is normal. If $n > 2$, then only one root of $x^n - p$ is in $\mathbf{Q}(p^{1/n})$, so this field cannot be Galois over $\mathbf{Q}$. □

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 $K_2 = F(v^{1/q})$.

Proof. Because $(p, q) = 1$, $K_1 \cap K_2 = F$, so $\text{Gal}(L/F) \simeq C_p \times C_q \simeq C_{pq}$. By Kummer theory, $L = F(v^{1/(pq)})$ for some $v \in F^\times$, which generates a group of order pq in $F^\times / (F^\times)^{pq}$. It follows that $K'_1 = F(v^{1/p})$ and $K'_2 = F(v^{1/q})$ are intermediate extensions between F and L , with $[L : K_1] = q$ and $[L : K_2] = p$. By the correspondence theorem, $K'_1 = K_1$ and $K'_2 = K_2$, because C_{pq} has unique subgroups of order q and p . □

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 .

Proof. Set $F = \mathbf{Q}$, $F_1 = F(q^{1/p})$, $F_2 = F(\mu_p)$. Then $[F_1 : F] = p$ by Eisenstein, and $[F_2 : F] = p - 1$. These degrees are relatively prime, so K is a degree p extension of F_2 , and a degree $p - 1$ extension of F_1 . Because K is Galois over F , it is also Galois over the F_j . We have $\text{Gal}(K/F_2) = C_p$ and, by the theorem on Galois groups of composit extensions, $\text{Gal}(K/F_1) \simeq (\mathbf{Z}/p)^\times =: A$. We claim that $G = C_p A$. Indeed, if $g \in G$, then by considering the action of g on F_2/F , we can find $a \in A$ so that ga^{-1} fixes F_2 and is thus in C_p . Since C_p is normal in G , we obtain $G \simeq C_p \rtimes A$.

Finally, using that $K = F_2(q^{1/p})$, one easily checks (e.g., using Kummer theory), that the action of A on C_p in this semidirect product is the usual one. □

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 $\text{Gal}(L/\mathbf{Q}) \simeq C_n \rtimes (\mathbf{Z}/n\mathbf{Z})^\times$.

Proof. We have

- (a) Set $E_1 = \mathbf{Q}(a^{1/d})$. Then clearly $[K : E_1] \leq n/d$ (because $(a^{1/n})^{n/d} = a^{1/d} \in E_1$) and $[E_1 : \mathbf{Q}] \leq d$ (by the same argument.). Thus both inequalities are equalities by the multiplicativity of field degrees.
- (b) On the one hand, $N_{K/E}(a^{1/n}) = \prod_{\tau} \tau(a^{1/n})$. But $\tau(a^{1/n}) = \zeta_{\tau} a^{1/n}$ for some $\zeta_{\tau} \in \mu_n$. There are n/d such τ 's, so $N_{K/E}(a^{1/n})$ is equal to $a^{1/d}$ times a root of unity. But it is also a real number, so this root of unity is ± 1 , proving the claim.
- (c) By the previous two parts, we have $E_1 \subseteq E$, but both have the same degree over $\mathbf{Q}$, so $E_1 = E$.
- (d) Because n is odd, d is also odd, so E_1 is not Galois. Thus $E_1 = E$ is not contained in $F := \mathbf{Q}(\mu_n)$ for any $d > 1$. Hence $K \cap F = \mathbf{Q}$. Because F is Galois over $\mathbf{Q}$ of degree $\varphi(n)$, with Galois group $(\mathbf{Z}/n\mathbf{Z})^\times =: A$, we get that L has degree $n\varphi(n)$ over $\mathbf{Q}$, and that $\text{Gal}(L/K) \simeq A$. Moreover, $L = F(a^{1/n})$ has degree n over F , so by Kummer theory, $\text{Gal}(L/F) = C_n$ is cyclic of order n . By similar arguments as in a previous problem, $\text{Gal}(L/\mathbf{Q}) \simeq C_n \rtimes A$, and one can calculate the A action on C_n is the usual one.

□

6. Give an example of Galois extensions K/F and L/K so that L/F is not Galois.

Proof. For example, $F = \mathbf{Q}$, $L = F(2^{1/4})$, $K = F(2^{1/2})$. Then K/F and L/K are each quadratic, so Galois, but L/F is not Galois because it does not contain the other roots of $x^4 - 2$. □

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 .

Proof. Set $K = \mathbf{Q}(\alpha)$, where α is the real root of $f(x)$. Then K has degree 3 over $\mathbf{Q}$, and is not Galois because $K \subseteq \mathbf{R}$ so K does not contain the other roots of $f(x)$. The Galois group of $f(x)$ is thus a subgroup of S_3 that has size bigger than 3, so it is all of 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.

Proof. One can argue as follows:

- (a) Let $\Delta \subseteq F^\times/(F^\times)^n$ be the subgroup generated by v . If the order of Δ is $d < n$, then $(v^{1/n})^d \in F^\times$ so that L has degree at most d over F .
(b) We have $\Delta \subseteq \Delta(L/F)$. But by Kummer theory, $\Delta(L/F)$ has the size $[L : F] = n$. Hence $\Delta = \Delta(L/F)$.

□

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.

Proof. F is a degree $p-1$ extension of $\mathbf{Q}$, and $\mathbf{Q}(q^{1/p})$ is a degree p extension of $\mathbf{Q}$. By inspecting degrees, or lots of other methods (as in previous problems), we get that L_1 is a degree p Galois extension of F . Then, arguing as in the hint, suppose $L_1 = L_2$ so that $q = r^m v^p$ for some integer $m = 1, 2, 3, \dots, p-1$ and $v \in F^\times$. Taking norms to $\mathbf{Q}$ gives $q^{p-1} = r^{m(p-1)} N(v)^p$ in $\mathbf{Q}^\times$, which contradicts unique factorization. □

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 $\alpha \in \bigcap_j F_j$. But this intersection is Galois over $\mathbf{Q}$

Proof.because if $\sigma \in \text{Gal}(L/\mathbf{Q})$, σ permutes the F_j so stabilizes the intersection. Thus this intersection contains the Galois closure of L , a contradiction. □

11. Determine the Galois group of $(x^3 - 2)(x^3 - 3) \in \mathbf{Q}[x]$.

Proof. The Galois group is the subgroup H of $S_3 \times S_3$ consisting of elements (σ, τ) with $\text{sgn}(\sigma) = \text{sgn}(\tau)$. Indeed, set $F_0 = \mathbf{Q}$, $F = \mathbf{Q}(\mu_3)$, $K_1 = F(2^{1/3})$, and $K_2 = F(3^{1/3})$. By a previous problem, $K_1 \neq K_2$ so their intersection contains F , and is a proper subfield that is Galois over F_0 , and thus the intersection is F . The claim follows. □

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 $\mathbf{Q}(\mu_3)$?

Proof. In the notation of the previous problem, the subfields are K , K_1 , K_2 and $F = \mathbf{Q}(\mu_3)$. This follows from the correspondence theorem. Indeed, the subgroup of H corresponding to F is $C_3 \times C_3$, which has exactly 4 subgroups, so the four fields above are all of them. To see that the subgroup of H corresponding to F is $C_3 \times C_3$, one just has to remember that the maps $\text{Gal}(K_j/F_0) \simeq S_3 \rightarrow \text{Gal}(F/F_0) \simeq \pm 1$ is the sign map. $\square$

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 $N(v) \equiv 1 \pmod{(F^\times)^3}$.

Proof. Hopefully you noticed while doing this problem that we need to assume that v is not in $(F^\times)^3$. We assume this going forward.

The field L is Galois over $\mathbf{Q}$ by a homework question, because $\bar{v} \in \langle v \rangle \subseteq F^\times / (F^\times)^3$. Let G be the Galois group of $L/\mathbf{Q}$. Because complex conjugation c defines a $C_2 = \langle c \rangle$ subgroup of G , and we have a normal C_3 subgroup of G coming from $\text{Gal}(L/F)$, we know from very similar questions above that $G \simeq C_3 \rtimes C_2$. However, when one computes the action of C_2 on C_3 , one gets that the action is trivial, exactly using that $\bar{v} \equiv v^2 \pmod{(F^\times)^3}$. Thus $G \simeq C_3 \times C_2$, a usual direct product. Now $K = L^{C_2}$ is the fixed field under complex conjugation, so $K/\mathbf{Q}$ has Galois group C_3 . The last part is easy. $\square$

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 $\bar{v} \equiv v^2 \pmod{(F^\times)^3}$.

Proof. Here is the proof:

- (a) Let γ be a primitive element for $K/\mathbf{Q}$, and $f(x) \in \mathbf{Q}[x]$ its irreducible polynomial. Every real cubic has either one real root or three real roots. If $f(x)$ has one real root, then the splitting field of $f(x)$, which is K , has Galois group S_3 , not C_3 . Thus $f(x)$ has three real roots, so that γ must be real so $K \subseteq \mathbf{R}$.
- (b) This part follows directly from our general analysis of Galois groups of composit extensions, because $K \cap F = \mathbf{Q}$.
- (c) That $L = F(v^{1/3})$ follows from Kummer theory. We have computed the C_2 action on C_3 in this Kummer theory situation, so the second part follows. Here is a direct argument: Let $v^{1/3}$ be our fixed cube root of v , and $\bar{v}^{1/3}$ denote the cube root of $\bar{v}$ that

is the complex conjugate of $v^{1/3}$. If σ denotes the generator of the C_3 , and c is complex conjugation, then $\sigma(\bar{v}^{1/3}) = c\sigma(v^{1/3}) = c(\zeta_3 v^{1/3}) = \zeta_3^2 \bar{v}^{1/3}$. But $\sigma(v^{2/3}) = \zeta_3^2 v^{2/3}$, so $\bar{v}^{1/3}/v^{2/3} \in F^\times$, giving the claim. □

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.

Proof. Part (a) follows as in your homework question. For part (b), note that each K_j is a splitting field, so it is easy to see that L is a splitting field. The restriction map $\text{Gal}(L/F) \rightarrow G_1 \times \cdots \times G_n$ is an injection, by using part (a). The third part follows immediately, because a subgroup of an abelian group is 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 $[K : \mathbf{Q}(\zeta_n + \zeta_n^{-1})] = 2$.

Proof. Set $K_0 = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$. We clearly have $K_0 \subseteq K^+ \subseteq K$. But clearly $K \neq K^+$, and from the hint $[K : K_0] = 2$, so $K_0 = K^+$. Note also that we could have used that K^+ is the fixed field of a subgroup of order 2 (generated by complex conjugation), so $[K : K^+] = 2$. □

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 $\sigma \in \text{Gal}(M/F)$.

Proof. Let L_0 be the compositum of the fields $\sigma(K)$. Then each $K \subseteq L$ so $L = \sigma(L) \supseteq \sigma(K)$ so L contains L_0 . But L_0 is Galois over F , because $\tau(L_0) \subseteq L_0$ for every $\tau \in \text{Gal}(M/F)$, because these τ 's permute the $\sigma(K)$. Thus $L \subseteq L_0$ by the definition of Galois closure, finishing the proof. □

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 $T \simeq D_8$.

Proof. The fact that L is the compositum of K, K' follows from the previous problem. That $H \simeq C_2 \times C_2$ follows from the general computation of the Galois group of composite extensions. Suppose now $\sigma \in T$ induces the nontrivial automorphism on K_0/F , and $h \in H$ induces the nontrivial automorphism on K/K_0 . Then

$$\sigma h \sigma^{-1}(\sqrt{a - \sqrt{b}}) = \sigma(h\epsilon\sqrt{a + \sqrt{b}}) = \sigma(-\epsilon\sqrt{a + \sqrt{b}}) = -\sqrt{a - \sqrt{b}}$$

for some $\epsilon = \pm 1$. A similar computation with K' replaced by K proves that the T/H conjugation on H exchanges the C_2 factors. $\square$

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.

Proof. We argue as follows.

- (a) This follows quickly from the hint.
- (b) If $a^2 < b$, then $a + \sqrt{b} > 0$ but $a - \sqrt{b} < 0$, so K is contained in $\mathbf{R}$ while K' is not, so $K \neq K'$.
- (c) Indeed, as suggested by the hint, we observe that $\gamma := \sqrt{a + \sqrt{b}}$ is primitive for K/F : $\gamma^2 = a + \sqrt{b}$, so $K_0 \subseteq F(\gamma)$, and $K = K_0(\gamma)$, so $K \subseteq F(\gamma)$. Because $[K : K_0] = 2$ and $[K_0 : F] = 2$, $[K : F] = 4$ so the degree of γ over F is 4, proving that $f(x)$ must be irreducible.
- (d) To see that $K = K'$, observe that $\alpha\alpha' = \sqrt{2 + \sqrt{2}}\sqrt{2 - \sqrt{2}} = \sqrt{2}$, so $\alpha' \in K$.

$\square$

20. Generalize the results of questions 13 and 14 to C_p extensions of $\mathbf{Q}$, where p is a prime number.

Proof. Feel free to talk to me about this in office hours. □