Cyclic cubic extensions of $\mathbb{Q}$, after Brian Lawrence

Guiding Question

In the case of quadratic extensions, we know every quadratic extension is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer d. Together with the fact that $\mathbb{Q}(\sqrt{p})$ is a subfield of $\mathbb{Q}(\zeta_{4p})$ for p odd, and that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$, this allows us to explicitly construct a field of the form $\mathbb{Q}(\zeta)$ containing $\mathbb{Q}(\sqrt{d})$ in accordance with the Kronecker-Weber Theorem.

Consider now the degree 3 case. Could we do a similar thing? Could we make a list of algebraic numbers α_i (or, more likely, their minimal polynomials) so that $\mathbb{Q}(\alpha_i)$ is cyclic cubic, every field listed is distinct, and every cyclic cubic extension is enumerated somewhere? Perhaps having done so, it will be easy to then find that these fields all lie in some $\mathbb{Q}(\zeta)$.

Preliminary Questions

For these first questions on quadratic extensions, do *not* appeal to the quadratic formula.

Question 1. Let K be an arbitrary field, and let L/K be a quadratic extension.

(a) Show that L is a normal extension.

(b) What more do you need to know to conclude that L/K is Galois?

Question 2. Let K be a field, and let V be a finite dimensional vector space over K. Suppose $T\colon V \to V$ is a linear transformation, and suppose $\lambda \in K$ is a root of the characteristic polynomial of T. Which of the following possibilities is true:

(i) T must have an eigenvector $v \in V$ of eigenvalue λ.

(ii) T will never have an eigenvector $v \in V$ of eigenvalue λ.

(iii) T may or may not have an eigenvector $v \in V$ of eigenvalue λ.

Prove your claim.

Question 3. Let K, V, T be as above, and suppose $T^2 = \mathrm{id}$.

(a) What are the possibilities for the minimal polynomial of T?

(b) What are the possible eigenvalues of T?

(c) Given an eigenvalue λ, can we guarantee that T will have an eigenvector of eigenvalue λ?

Question 4. Let K be a field, and let L/K be a separable quadratic extension. By Question 1, L is Galois, so let $\sigma \in \mathrm{Gal}(L/K)$ be the nontrivial automorphism.

(a) We can view σ as an K-linear map $L \to L$. Prove that σ has an eigenvector of eigenvalue -1.

(b) Suppose $\alpha \in L$ is such an eigenvector of σ. Prove that $\alpha^2 \in K$.

(c) Now take $K = \mathbb{Q}$. Explain why we can choose α so that α^2 is a squarefree integer.

Question 5. The preceding questions together establish that any quadratic extension of $\mathbb{Q}$ must be of the form $\mathbb{Q}(\sqrt{d})$ for a squarefree $d \in \mathbb{Z}$. Importantly, they do so *without* relying on the quadratic formula, so they have a chance of generalizing to higher degree extensions.

(a) Suppose $L/\mathbb{Q}$ is a Galois extension with Galois group $\mathbb{Z}/n\mathbb{Z}$. We know that L is not necessarily of the form $\mathbb{Q}(\sqrt[n]{d})$ for an integer d; in fact, $\mathbb{Q}(\sqrt[n]{d})$ probably isn't even a Galois extension. So, the argument we used in the quadratic case must fail somewhere. Where does it fail?

(b) Is there a simple condition we could place on a field K to guarantee that every Galois extension L/K with Galois group $\mathbb{Z}/n\mathbb{Z}$ is of the form $K(\sqrt[n]{\mu})$ for some $\mu \in K$? That is, what would we need in order to repair the gap in the argument above when $K = \mathbb{Q}$?

In what follows, it may be useful to keep in mind the following fact, which is a special case of Proposition 13.27 in Dummit and Foote.

Fact. Let K be a field and let L/K be a normal extension (i.e. any polynomial with a root in L factors completely). If $\sigma\colon K \to K$ is an automorphism, then there is an automorphism $\sigma'\colon L \to L$ extending σ to all of L.

If this sounds unfamiliar to you, the next question gives a consequence of this fact which may ring a bell. However, it will be useful to know the fact in this level of generality.

Question 6. Suppose L and K are as above, and suppose that they are both Galois extensions of some third field F. Since K is Galois, any automorphism $\tau\colon L \to L$ satisfies $\tau(K) = K$. So, define a function $\mathrm{res} : \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ by $\mathrm{res}(\tau) = \tau|_K$.

(a) Show that res is in fact a homomorphism.

(b) Use the fact above to show that res is surjective.

(c) What is $\ker \mathrm{res}$? How does this relate to a Galois theory fact you already know?

Finding cyclic cubic extensions

Our classification procedure is going to make use of Kummer's theorem, which the preceding questions aimed to give an understanding of.

Theorem (Kummer's Theorem)**.** Suppose K is a field containing all nth roots of unity. Then any cyclic degree n extension L/K is of the form $K(\sqrt[n]{\mu})$ for some $\mu \in K$.

The idea of what is called "Kummer theory" is to analyze cyclic n-extensions of an arbitrary K by first adjoining the nth roots of unity ζ_n, then determining which cyclic n-extensions of $K(\zeta_n)$ come from (or "descend to") cyclic n-extensions of $\mathbb{Q}$. From here on, let ω be a primitive third root of unity, and let $K = \mathbb{Q}(\omega)$. Note that $K/\mathbb{Q}$ is Galois and its Galois group is generated by complex conjugation, which we will denote τ.

Question 7. Fix an algebraic closure of $\mathbb{Q}$ so that we may freely speak of intersections of fields and composite fields.

(a) Suppose $L/\mathbb{Q}$ is a cyclic cubic extension, i.e. a Galois cubic extension with cyclic Galois group (of order 3). Show that $L \cap K = \mathbb{Q}$.

(b) Let M be the composite field KL. What is $[M : \mathbb{Q}]$?

(c) Show that M is Galois over $\mathbb{Q}$ by finding $[M : \mathbb{Q}]$-many automorphisms.

(d) What is $\mathrm{Gal}(M/\mathbb{Q})$? What is $\mathrm{Gal}(M/K)$?

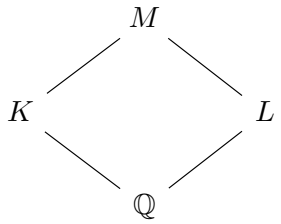
(e) The Galois correspondence says that subfields of M correspond to subgroups $H \subset \mathrm{Gal}(M/\mathbb{Q})$ by taking the fixed field of H, M^H. What subgroup H corresponds to L under this correspondence?

What we would like to do is to go the other way around. That is, we would like to be able to start with the field $M = K(\sqrt[3]{\mu})$ and take the fixed field $L = M^H$ (where H is the subgroup you found in the previous problem), which will be a degree 3 extension of $\mathbb{Q}$. We hope that under some conditions on μ, we can guarantee that the field we construct this way will end up being Galois. In order for this strategy to work, we need M to be Galois over $\mathbb{Q}$.

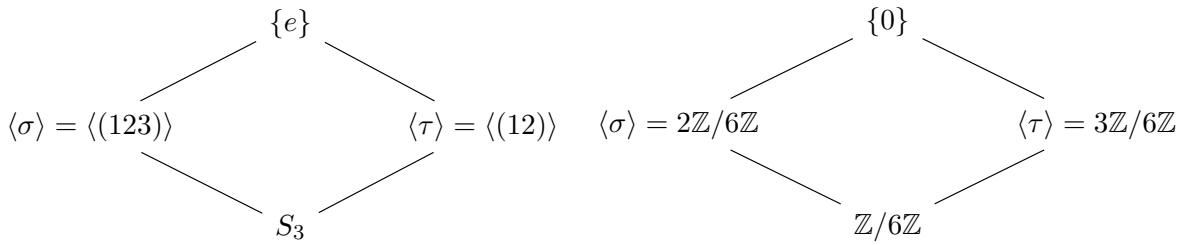
In what follows, we will start with the assumption that $M/\mathbb{Q}$ is Galois, and find that we do not encounter any obstacles. The next question invites you to think about whether we need to make this assumption, or if it follows from other facts about the situation; it is not an essential exercise for the rest of the section.

Question 8. (Not essential) Let M/K be a cyclic cubic extension. Do you think there are any examples of M which are *not* Galois over $\mathbb{Q}$? If yes, try to find a counterexample, and if no, try to prove it.

So, supposing that M is Galois over $\mathbb{Q}$, let's make a diagram of the situation.



By the fact at the end of the Preparatory Questions, the Galois group $G = \mathrm{Gal}(M/\mathbb{Q})$ will be generated by a generator $\sigma \in \mathrm{Gal}(M/K)$ and a lift of $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ (which we have said is complex conjugation). Further, let us choose σ so that $\sigma(\sqrt[3]{\mu}) = \omega\sqrt[3]{\mu}$. There are two possible groups G could be: S_3 and $\mathbb{Z}/6\mathbb{Z}$. When we look at the subgroup lattice of G, we will be in one of the following situations:



Question 9. Explain why $L/\mathbb{Q}$ will be Galois only in the latter situation. So, a sufficient and necessary condition for $L/\mathbb{Q}$ to be Galois is for σ and τ to commute.

Question 10. Consider σ as a map of K-vector spaces $M \to M$. What are the eigenvalues of σ? What are eigenvectors for each eigenvalue?

Question 11. Since $M = \mathbb{Q}(\omega, \sqrt[3]{\mu})$, we can check if σ and τ commute by checking that $\sigma \circ \tau(\omega) = \tau \circ \sigma(\omega)$ and $\sigma \circ \tau(\sqrt[3]{\mu}) = \tau \circ \sigma(\sqrt[3]{\mu})$.

(a) Check that $\sigma \circ \tau(\omega) = \tau \circ \sigma(\omega)$ always.

(b) Check that $\tau(\sqrt[3]{\mu})$ is a cube root of $\tau(\mu)$.

(c) Show that $\sigma \circ \tau(\sqrt[3]{\mu}) = \tau \circ \sigma(\sqrt[3]{\mu})$ implies that $\tau(\sqrt[3]{\mu})$ lies in a particular eigenspace of σ.

(d) Using the eigenvectors you found in Question 9, the previous part implies that $\tau(\sqrt[3]{\mu})$ is a K-scalar multiple of one of them. Find which one, and use this to conclude a certain function of μ must have a cube root in K.

The last part of the preceding question gives us an explicit condition on μ in order for $L/\mathbb{Q}$ to be Galois. In order to actually compute minimal polynomials, it now becomes important to know some things about the structure of the integers in K.

Question 12.

(a) What is $\mathcal{O}_K$?

(b) Show that $\mathcal{O}_K$ is a PID.

(c) What is the discriminant of $\mathcal{O}_K$? What primes ramify?

(d) What primes split in $\mathcal{O}_K$? What primes are inert?

Question 13.

(a) Check that changing μ by multiplying it by an element of $(K^\times)^3$ (the group of cubes in $K^\times$) does not change the extenstion M. Therefore, μ gives a well-defined element in the quotient group $K^\times/(K^\times)^3$.

(b) Check that any element in $K^\times/(K^\times)^3$ can be represented by a cube-free element of $\mathcal{O}_K$.

(c) Let $\mu \in \mathcal{O}_K$ be cube-free. Write down a factorization of μ as a product of primes. What must be true about that factorization in order for μ to satisfy the condition of Question 11(d)?

Question 14.

(a) Suppose μ is as in the previous question. Find a τ-invariant element $\alpha \in M \setminus \mathbb{Q}$.

(b) Find the trace and norm of your α. (In terms of the factorization of μ.)

(c) Find the minimal polynomial of your α.

Question 15. Let $\alpha_1, \alpha_2, \alpha_3$ be the three elements of least norm produced by this process you've described. Find the minimal polynomials of each of the α_i.

Proving Kronecker-Weber

So far, we have found how to construct cyclic cubic extensions of $\mathbb{Q}$. By design, all cyclic cubic extensions of $\mathbb{Q}$ arise from our construction, and we can tell almost exactly where one of the fields we construct will be ramified.

Question 16.

(a) Let $M/K/\mathbb{Q}$ be any tower of field extensions with $[M:K] = m$ and $[K:\mathbb{Q}] = n$. Prove or look up that $\mathrm{Disc}(M/\mathbb{Q}) = N_{\mathbb{Q}}^K(\mathrm{Disc}(M/K))\,\mathrm{Disc}(K/\mathbb{Q})^m$. Unless I got the formula wrong, in which case find the right formula.

(b) Show that when we perform the process from the previous section, we can decide which primes divide $\mathrm{Disc}(L/\mathbb{Q})$ except perhaps $p = 3$.

To rephrase this a bit: if S is any finite set of primes which includes 3 and such that any $p \in S$ satisfies $p \equiv 0, 1 \pmod 3$, then our construction can build all of the cyclic cubic extensions of $\mathbb{Q}$ unramified at primes outside of S. The set of such extensions is finite, and the virtue of our construction is that it lets us actually count how many different fields there are in there.

Question 17. Fix some set S of rational primes satisfying the above conditions. Let U_S be the subgroup of $K^\times/(K^\times)^3$ generated by ω and the primes lying over primes $p \equiv 1 \pmod 3$ in S.

(a) What is the size of U_S?

(b) Show that for $\mu \in U_S$, μ and μ^2 give the same extension of K.

(c) Every element of U_S has order dividing 3, so we can think of U_S as a vector space over $\mathbb{F}_3$, where vector "addition" is multiplication and "scalar multiplication" is exponentiation. Interpret the above as saying that the different extensions M/K are in bijection with lines in this vector space. Use this to count the different extensions M.

This gives us a route to proving Kronecker-Weber in the degree 3 case. Given a set S as above, if we can count how many cyclic cubic extensions unramified outside of S arise as subfields of cyclotomic fields, and it turns out to be the same number as before, then that means every cyclic cubic extension of $\mathbb{Q}$ is contained in a cyclotomic extensions.

Question 18.

(a) Show that Φ_p is separable for any $\ell \neq p$.

(b) What primes ramify in $\mathbb{Q}(\zeta_p)$?

(c) For which p does $\mathbb{Q}(\zeta_{p^k})$ contain a cyclic cubic subfield? Does increasing k change the subfield found?

(d) Given a set S as above, how many cyclic cubic extensions of $\mathbb{Q}$ can you find that are subfields of a cyclotomic field? (Remember you can take composites!)

(e) Prove the Kronecker-Weber theorem for degree 3 extensions of $\mathbb{Q}$.